V. A. Kopyttsev, V. G. Mikhailov, Poisson type theorems for the number of solutions of random inclusions, *Mat. Vopr. Kriptogr.*, 2010, Volume 1, Issue 4, 63–84

DOI: 10.4213/mvk21

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2010 Т. 1 № 4 С. 63–84

УДК: 519.212.2

Теоремы пуассоновского типа для числа решений случайных включений

В. А. Копытцев, В. Г. Михайлов

Академия криптографии Российской Федерации
Математический институт им. В. А. Стеклова РАН

Получено 20.IV.2010

Пусть F — случайное отображение n-мерного пространства V^n над конечным полем $GF(q)$ в T-мерное пространство V^T над тем же полем, и $D \subset V^n$, $B \subset V^T$. Выведены достаточные условия сходимости при $n, T \to \infty$ распределения числа решений системы включений $x \in D$, $F(x) \in B$ к распределениям пуассоновского типа.

Ключевые слова: случайные включения, случайные системы уравнений, число решений, предельная теорема Пуассона

Poisson type theorems for the number of solutions of random inclusions

V. A. Kopytcev, V. G. Mikhailov

Academy of Cryptography of Russian Federation
Steklov Mathematical Institute of RAS

Abstract. Let F be a random mapping of n-dimensional space V^n over the finite field $GF(q)$ into T-dimensional space V^T over the same field, and $D \subset V^n$, $B \subset V^T$. For systems of inclusions $x \in D$, $F(x) \in B$ sufficient conditions for the weak convergence of the number of solutions to the Poisson type laws as $n, T \to \infty$ are obtained.

Key words: random inclusions, random equations systems, number of solutions, Poisson limit theorem

Citation: *Mathematical Aspects of Cryptography*, 2010, vol. 1, no. 4, pp. 63–84 (Russian).

1. Введение

Включением (над полем $K = GF(q)$) размерности T относительно n-мерного вектора $x = (x_1, \ldots, x_n)$ мы называем запись $F(x) \in B$, где $F(x) = (F_1(x), \ldots, F_T(x))\colon V^n \to V^T$ — отображение пространства n-мерных векторов V^n над конечным полем K в пространство V^T над тем же полем, а $B \subset V^T$. В случае, когда множество B состоит из единственного вектора $B = \{b = (b_1, \ldots, b_T)\}$, включение $F(x) \in B$ представляет собой систему из T уравнений

$$F_t(x_1, \ldots, x_n) = b_t, \quad t = 1, \ldots, T,$$

относительно n неизвестных.

Рассмотрим в качестве $F(x)$ случайное отображение $AG(x)\colon V^n \to V^T$, где $G(x) = (g_1(x), \ldots, g_m(x))$ — детерминированное отображение V^n в V^m, а A — случайная матрица размера $T \times m$. Пусть $D \subseteq V^n$. Обозначим $\xi(D, AG, B)$ число решений системы включений $x \in D$, $AG(x) \in B$.

В работе [1] был изучен случай, когда $m = n$, а $G(x) = x$, т. е. отображение AG линейно. Были выведены условия сходимости при $n, T \to \infty$ распределения числа решений системы $x \in D$, $Ax \in B$ к распределениям пуассоновского типа. В настоящей работе эти результаты распространяются на широкий класс включений $AG(x) \in B$ с нелинейными отображениями G. Наш подход опирается на следующее соображение. В случае, когда ограничение отображения G на множество D обратимо, число решений системы $x \in D$, $AG(x) \in B$ совпадает с числом решений системы линейных включений $y \in G(D)$, $Ay \in B$. Это обстоятельство позволяет применить для описания свойств распределения случайной величины $\xi(D, AG, B)$ результаты работы [1].

В предыдущих работах авторов решения включения $Ax \in B$ (или системы $Ax = b$), удовлетворяющие условию $x \in D$, $D \subset V^n$, были названы *специальными*. Этот термин естественно использовать и для нелинейных включений. В работах [2] и [3] в качестве множеств специальных решений рассматривались шары и сферы относительно метрики Хемминга в пространстве V^n. В работе [4] была описана связь между числом специальных решений системы случайных однородных линейных уравнений $Ax = 0$ и числом решений специально построенного случайного линейного включения $A'y \in B'$. В упомянутых работах были найдены достаточные условия сходимости распределений исследуемых чисел решений к распределениям пуассоновского типа. Итог этим исследованиям был подведен в работе [1].

Сформулируем результаты настоящей работы. Отметим, что далее рассматривается схема, в которой от параметров n, T зависят числа $m = m(n, T)$,

функции $G(x) = G(x; n, T)$, матрицы $A = A(n, T)$ размера $T \times n$ и множества $B = B(T) \subset V^T$ и $D = D(n) \subset V^n$.

Знаком $\oplus$ будем обозначать операцию сложения в поле и в линейных пространствах над этим полем. Обозначим через $N(a_1, a_2, a_3, d, B)$, где $a_1, a_2, a_3 \in K \setminus \{0\}$, $d \in V^T$, число решений уравнения $a_1 u^1 \oplus a_2 u^2 \oplus a_3 u^3 = d$ относительно тройки векторов $(u^1, u^2, u^3) \in B^3$. Пусть

$$N(B) = \max_{a_1,a_2,a_3,d} N(a_1, a_2, a_3, d, B), \quad \rho(B) = N(B)/|B|^2. \tag{1}$$

Очевидно, что $0 \le \rho(B) \le 1$. Для линейных и аффинных подпространств эта величина принимает максимально возможное значение $\rho(B) = 1$.

Из соотношения $\rho(B(T)) \to 0$ при $T \to \infty$ следует, что вероятность того, что любая линейная комбинация любого заданного числа наугад выбранных элементов множества $B(T)$ попадет в $B(T)$, с ростом размерности пространства стремиться к нулю (см. [1]). Этим свойством обладают, например, последовательности шаров и сфер в пространствах V^T относительно метрики Хемминга, если их радиусы $r(T)$ при $T \to \infty$ удовлетворяет неравенствам $1 \le r(T)$, $r(T)T^{-1} \le \mu$, где $\mu < (q-1)/q$. При $q \ge 3$ еще один пример дает последовательность множеств тех векторов пространств V^T, в записи которых отсутствует заданный элемент поля.

Пусть элементы случайной матрицы $A = \|a_{i,j}\|$ независимы в совокупности и

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

где $\sum_{k \in K} \Delta_{i,j}(k) = 0$, $i = 1, \ldots, T$, $j = 1, \ldots, m$. Положим

$$\Delta = \Delta(A) = \max_{i,j,k} |\Delta_{i,j}(k)| < 1. \tag{2}$$

Отметим, что свойство $\Delta(A) \to 0$ означает сближение распределения элементов матрицы A с равномерным.

Зададим множество $D = D(n) \subset V^n$ и набор попарно не пересекающихся множеств $B_1 = B_1(T), \ldots, B_s = B_s(T) \subset V^T$. Положим $B = B_1 \cup \ldots \cup B_s$. Напомним, что векторы z и z' считаются *подобными*, если $z' = cz$, $c \in K \setminus \{0\}$. Будем говорить, что отображение G множества V^n в некоторое множество U *обратимо на множестве* $D \subseteq V^n$, если все элементы $G(x)$, $x \in D$, различны.

Теорема 1. *Пусть отображение G обратимо на множестве D, причем $0 \notin G(D)$, множество $G(D) \times B$ не содержит подобных векторов,*

выполнены условия $n, T \to \infty$, $T\Delta \to 0$, $|D| \to \infty$ *и соотношения*

$$\rho(G(D))\rho(B) \to 0, \tag{3}$$

$$q^{-T}|D| \cdot |B_k| \to \lambda_k,\ 0 < \lambda_k < \infty,\ k = 1, \ldots, s. \tag{4}$$

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

Рассмотрим теперь некоторое множество $B = B(T) \subset V^T$. Разобьем множество $G(D) \times B$ на классы подобных векторов $(G(D)B)_1, \ldots, (G(D)B)_M$, где M — общее число таких классов. Положим

$$l_r(G(D), B) = |\{k \in \{1, \ldots, M\}\colon |(G(D)B)_k| = r\}|, \quad r = 1, \ldots, q-1.$$

Пусть $\pi_1(\lambda_1), \ldots, \pi_{q-1}(\lambda_{q-1})$ — независимые в совокупности случайные величины, распределенные по закону Пуассона с параметрами $\lambda_1, \ldots, \lambda_{q-1}$ соответственно.

Теорема 2. *Пусть отображение* G *обратимо на множестве* D, *причем* $0 \notin G(D)$, *выполнены условия* $n, T \to \infty$, $T\Delta \to 0$, $|D| \to \infty$ *и соотношения*

$$\rho(G(D))\rho(B) \to 0, \tag{5}$$

$$q^{-T} l_r(G(D), B) \to \lambda_r,\ 0 \le \lambda_r < \infty,\ r = 1, \ldots, q-1,$$

$$\exists r \in \{1, \ldots, q-1\}\colon \lambda_r > 0. \tag{6}$$

Тогда распределение величины $\xi(D, AG, B)$ *сходится к распределению случайной величины*

$$\pi(\lambda_1, \ldots, \lambda_{q-1}) = \pi_1(\lambda_1) + 2\pi_2(\lambda_2) + \ldots + (q-1)\pi_{q-1}(\lambda_{q-1}).$$

Замечание 1. Если в условиях теорем 1 и 2 множество $G(D)$ заменить множеством D, то утверждения этих теорем будут относиться к числу решений системы $x \in D$, $Ax \in B$, а сами теоремы обратятся в теоремы 2 и 3 работы [1]. Утверждения теорем 1 и 2 вытекают непосредственно из теорем 1 и 3 работы [1].

Пусть $G(x) = (x, f(x))$ и $F(x) = AG(x) = A_1 x + A_2 f(x)$ при случайных матрицах A_1 и A_2 размерностей $T \times n$ и $T \times (m-n)$ соответственно с независимыми в совокупности случайными элементами и заданном отображении $f(x) = (f_{n+1}(x), \ldots, f_m(x))\colon V^n \to V^{m-n}$ таком, что $f(0^n) = 0^{m-n}$ (через 0^n

обозначаем нулевой вектор пространства V^n). Класс включений с таким отображением F представляет особый интерес, поскольку в него входят системы нелинейных уравнений

$$\sum_{\substack{d_1,\dots,d_n\in\{0,\dots,q-1\},\\ 1\le d_1+\dots+d_n\le d}} a^{(t)}_{d_1,\dots,d_n} x_1^{d_1}\dots x_n^{d_n} = b_t, \quad t=1,\dots,T. \tag{7}$$

Если случайные величины $a^{(t)}_{d_1,\dots,d_n}$ распределены равномерно на множестве элементов поля K и независимы в совокупности, то левые части уравнений системы (7) независимы и имеют равномерные распределения на множестве всех функций степени не выше $d = d(n)$.

Замечание 2. Отображение $G(x) = (x, f(x))$ является обратимым отображением множества V^n во множество V^m. Поэтому условие обратимости в теореме 1 выполнено при любом $D \subseteq V^n$. Кроме того, при $G(x) = (x, f(x))$ из $\rho(D) \to 0$ следует, что $\rho(G(D)) \to 0$.

Изучим асимптотическое поведение распределения общего числа ненулевых решений случайного включения $A_1x + A_2f(x) \in B$ при $n, T \to \infty$ (в наших обозначениях это $\xi(V^n \setminus \{0^n\}, F, B)$). Введем обозначение

$$H_f = G(V^n \setminus \{0^n\}) = \{(x, f(x))\colon x \in V^n \setminus \{0^n\}\}.$$

Снова зададим набор попарно не пересекающихся множеств $B_1 = B_1(T), \dots, B_s = B_s(T) \subset V^T$. Положим $B = B_1 \cup \dots \cup B_s$. Пусть величина $\Delta = \Delta(A_1, A_2)$ задается формулой (2) где A — матрица размера $T \times m$, образованная объединением столбцов матриц A_1 и A_2.

Теорема 3. *Пусть множество $H_f \times B$ не содержит подобных векторов, выполнены условия $n, T \to \infty$, $\Delta \to 0$,*

$$\rho(H_f)\rho(B) \to 0, \tag{8}$$

$$q^{n-T} \cdot |B_k| \to \lambda_k,\ 0 < \lambda_k < \infty,\ k = 1, \dots, s, \tag{9}$$

$$|B| \le q^{\delta T} \quad (0 < \delta < 1). \tag{10}$$

Тогда случайные величины $\xi(V^n \setminus \{0^n\}, F, B_k)$ асимптотически независимы, а их распределения сходятся к распределениям Пуассона с параметрами λ_k соответственно.

Теорема 4. *Пусть $n, T \to \infty$, выполнены условия $\Delta \to 0$, (8),*

$$q^{-T} l_r(H_f, B) \to \lambda_r,\ 0 \le \lambda_r < \infty\ (r = 1, \dots, q-1),\ \exists r\colon \lambda_r > 0, \tag{11}$$

$$|B| \le q^{\delta T} \quad (0 < \delta < 1). \tag{12}$$

Тогда распределение случайной величины $\xi(V^n \setminus \{0^n\}, F, B)$ *сходится к распределению величины* $\pi(\lambda_1, \ldots, \lambda_{q-1})$.

Замечание 3. Условие (12) выполнено, например, для шаров радиуса r в метрике Хемминга, если $r \geq 1$ и $rT^{-1} \leq \mu < (q-1)q^{-1}$.

Для широкого класса отображений f множество H_f при переходе к пределу удовлетворяет соотношению $\rho(H_f) \to 0$, и для таких отображений условие (8) в теоремах 3–4 выполнено «автоматически».

Пример 1. Рассмотрим отображение $f(x) = (f_1(x), \ldots, f_{m-n}(x))$, в качестве части координатных функций которого выступают все произведения вида $x_1^{d_1} \ldots x_n^{d_n}$, для которых $2 \leq d_1 + \ldots + d_n \leq d$. Здесь $d = d(n) \leq (q-1)n -$ заданное число, а

$$m = m(n) \geq m(n, d) = \sum_{r=1}^{d} C_n^r.$$

Отображения такого вида изучались А. М. Зубковым в 70-х–80-х годах прошлого века. Из его результатов следует, что при $K = GF(2)$, равномерных распределениях матриц A_1, A_2, фиксированном параметре d и при $n, T \to \infty$, $n - T = r$ распределение числа ненулевых решений системы

$$A_1 x \oplus A_2 f(x) = b$$

сходится к распределению Пуассона с параметром 2^r.

Теорема 5. *Пусть отображение* $f(x)$ *принадлежит классу, описанному в примере* 1, *и* $n \to \infty$. *Тогда* $\rho(H_f) \to 0$.

Теорема 5 вместе с теоремами 1–4 дает достаточные условия сходимости распределения числа ненулевых решений случайного включения $A_1 x \oplus A_2 f(x) \in B$ с отображением $f(x)$ указанного вида к распределениям пуассоновского типа. В качестве примера приведем предельную теорему Пуассона для числа ненулевых решений включения, левая часть которого совпадает с левой частью системы (7).

Следствие 1. *Пусть при каждых* n *и* T *отображение* $F(x)$ *выбирается случайно и равновероятно из множества всех отображений из* V^n *в* V^T *с координатными функциями степени не выше* $d = d(n) \geq 2$, $B \subset V^T$, $n, T \to \infty$ *и* $q^{n-T} \cdot |B| \to \lambda$, $0 < \lambda < \infty$. *Тогда распределение числа ненулевых решений включения* $F(x) \in B$ *сходится к распределению Пуассона с параметром* λ *соответственно.*

Теоремы 3 и 4 доказываются в разделе 2. Раздел 3 посвящен доказательству теоремы 5 и следствия 1.

2. Доказательства теорем 3 и 4

Напомним, что в данном случае $F(x) = AG(x) = A_1x + A_2f(x)$ при случайных матрицах A_1 и A_2 размерностей $T \times n$ и $T \times (m-n)$ соответственно с независимыми в совокупности случайными элементами, где отображение G имеет вид $G(x) = (x, f(x))$, $f(x) = (f_{n+1}(x), \dots, f_m(x))\colon V^n \to V^{m-n}$, что $f(0^n) = 0^{m-n}$.

Рассмотрим множества

$$J = (V^n \setminus \{0^n\}) \times B, \quad J^f = \{(x, f(x), b)\colon (x, b) \in J\}. \tag{13}$$

Пусть задан набор $R_1, \dots, R_s$ непересекающихся подмножеств множества J. Положим

$$\xi_u = \sum_{(x,b)\in R_u} I\{F(x) = b\}, \quad u = 1, \dots, s. \tag{14}$$

Теорема 6. *Пусть множество $H_f \times B$ не содержит подобных векторов, $n, t \to \infty$, выполнены условия $\Delta = \Delta(A_1, A_2) \to 0$,* (8), (10) *и условия*

$$q^{n-T}|B| = O(1), \tag{15}$$

$$q^{-T} \cdot |R_k| \to \lambda'_k,\ 0 < \lambda'_k < \infty,\ k = 1, \dots, s. \tag{16}$$

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.

Доказательство. Воспользуемся многомерной версией известной теоремы Б. А. Севастьянова об условиях сходимости распределений сумм зависимых индикаторов к распределению Пуассона (см. [5]). Ее условия используют понятие исключительных множеств. Для построения этих множеств в нашем случае потребуется ряд новых определений. Положим

$$D^f_{k,j} = \left\{(x^1, \dots, x^k) \in (V^n \setminus \{0^n\})^k\colon \operatorname{rank}(G(x^1), \dots, G(x^k)) = j\right\}, \tag{17}$$

$$D^f_k = \bigcup_{j=1}^{k-1} D^f_{k,j}. \tag{18}$$

Отметим, что

$$|D^f_{k,j}| \le \sum_{s=1}^{j} \left|\left\{(x^1, \dots, x^k) \in (V^n \setminus \{0^n\})^k\colon \operatorname{rank}(x^1, \dots, x^k) = s\right\}\right|.$$

Следовательно,

$$|D^f_{k,j}| < \sum_{s=1}^{j} C^s_k q^{s(k-s)} q^{ns}. \tag{19}$$

При всех $(x^1, \ldots, x^k) \in (V^n \setminus \{0^n\})^k$, $k \geq 2$ и $\alpha = 1, \ldots, k$ положим

$$\eta^\alpha(x^1, \ldots, x^k) = \sum_{i=1}^{n} \eta^\alpha_i(x^1, \ldots, x^k), \tag{20}$$

где

$$\eta^\alpha_i(x^1, \ldots, x^k) = 1, \quad \text{если } x^\alpha_i \neq 0 \text{ и } x^\beta_i = 0 \text{ при всех } \beta = 1, \ldots, k,\ \beta \neq \alpha,$$
$$\eta^\alpha_i(x^1, \ldots, x^k) = 0 \text{ — в противном случае.}$$

При $k = 1$ положим $\eta^1(x^1) = \|x^1\|$ (напомним, что $\|x\|$ — число ненулевых элементов вектора x). При $0 \leq l \leq n$ определим множество

$$D^f_{k,j}(l) = \{(x^1, \ldots, x^k) \in D^f_{k,j}:$$
$$\exists s_1, \ldots, s_j \in \{1, \ldots, k\}, \quad s_\alpha \neq s_\beta\ (\alpha \neq \beta),$$
$$\eta^s(x^{s_1}, \ldots, x^{s_j}) \geq l \quad \forall s \in \{s_1, \ldots, s_j\}\}. \tag{21}$$

Замечание 4. Множество $D^f_{k,j}(l)$ образовано теми наборами $(x^1, \ldots, x^k)$ из $D^f_{k,j}$, в которых найдутся j векторов, каждый из которых имеет не менее l отличных от нуля элементов на тех местах, где остальные $j - 1$ векторов имеют нули.

Введем обозначение $v^i = (x^i, b^i)$ и положим

$$J_k = \{(v^1, \ldots, v^k) \in J^k : v^\alpha \neq v^\beta\ (\alpha \neq \beta)\}.$$

Определим исключительные множества $I_k \subset J_k$ равенством

$$I_k = \left\{(v^1, \ldots, v^k) \in J_k : (x^1, \ldots, x^k) \in D^f_k \cup \left(D^f_{k,k} \setminus D^f_{k,k}(\ln n)\right)\right\}. \tag{22}$$

Согласно этому определению в исключительное множество I_k вошли все наборы $(v^1, \ldots, v^k) \in J_k$, для которых набор $(x^1, \ldots, x^k)$ имеет ранг $j < k$, а в случае полного ранга $j = k$ все составляющие этот набор векторы имеют относительно мало ненулевых элементов на тех местах, где остальные $k - 1$ векторов имеют нули.

Согласно многомерной версии теоремы Б. А. Севастьянова утверждение теоремы 6 будет доказано, если убедиться, что выполнены условия

$$\max_{(x,b)\in J} \mathbf{P}\{F(x) = b\} \to 0, \tag{23}$$

$$\sum_{(x,b)\in R_u} \mathbf{P}\{F(x) = b\} \to \lambda'_u, \quad u = 1, \dots, k, \tag{24}$$

и при всех k=2,3,...

$$\max_{(v^1,\dots,v^k)\in I_k\setminus I_k} \left| \frac{\mathbf{P}\{F(x^1) = b^1, \dots, F(x^k) = b^k\}}{\mathbf{P}\{F(x^1) = b^1\} \dots \{F(x^k) = b^k\}} - 1 \right| \to 0, \tag{25}$$

$$\sum_{(v^1,\dots,v^k)\in I_k} \prod_{j=1}^{k} \mathbf{P}\{F(x^j) = b^j\} \to 0, \tag{26}$$

$$\sum_{(v^1,\dots,v^k)\in I_k} \mathbf{P}\{F(x^1) = b^1, \dots, F(x^k) = b^k\} \to 0. \tag{27}$$

Перед проверкой условий (23)–(27) докажем леммы, которые понадобятся при выводе этих соотношений.

Лемма 1. *Пусть* $x^1, \dots, x^k \in D^{\dagger}_{k,j}(l)$, $1 \le l \le n$, $b^1, \dots, b^k \in V^T$ *и выполнено условие* (2). *Тогда при всех* $k = 1, 2, \dots$

$$\mathbf{P}\{F(x^1) = b^1, \dots, F(x^k) = b^k\} \le \left(\frac{1+\Delta^l}{q}\right)^{jT}, \tag{28}$$

если $j \le k-1$, *а если* $j = k$, *то*

$$\left(\frac{1-\Delta^l}{q}\right)^{kT} \le \mathbf{P}\{F(x^1) = b^1, \dots, F(x^k) = b^k\} \le \left(\frac{1+\Delta^l}{q}\right)^{kT}. \tag{29}$$

Замечание 5. Это утверждение является аналогом леммы 4.1 работы [1], которая также будет использована нами. Приведем формулировку этой леммы.

Лемма 1а. *Пусть* $x^1, \dots, x^k \in D^{\dagger}_{k,j}$, $b^1, \dots, b^k \in V^T$ *и выполнено условие* (2). *Тогда при всех* $k = 1, 2, \dots$

$$\mathbf{P}\{F(x^1) = b^1, \dots, F(x^k) = b^k\} \le \left(\frac{1+\Delta}{q}\right)^{jT}, \tag{28}$$

если $j \le k-1$, *а если* $j = k$, *то*

$$\left(\frac{1-\Delta}{q}\right)^{kT} \le \mathbf{P}\{F(x^1) = b^1, \ldots, F(x^k) = b^k\} \le \left(\frac{1+\Delta}{q}\right)^{kT}. \qquad (29)$$

Доказательство леммы 1. Соотношение $F(x^s) = b^s$ представляет собой систему $Ay = b^s$ из T линейных уравнений относительно вектора $y = G(x^s)$ со случайной матрицей A, образованной объединением столбцов матриц A_1 и A_2. Пусть вектор y имеет l ненулевых координат $y_{u_1}, \ldots, y_{u_l}$. Тогда, используя равенства $\Delta_{i,u}(k) = q\mathbf{P}\{a_{i,u} = k\} - 1$ и $\sum_{k\in K} \Delta_{i,u}(k) = 0$ (см. раздел 1), получаем

$$\mathbf{P}\{a_{i,u_1} y_{u_1} \oplus \ldots \oplus a_{i,u_l} y_{u_l} = c\} = \sum \prod_{w=1}^{l} \mathbf{P}\{a_{i,u_w} = c_w\} =$$
$$= \frac{1}{q} + \frac{1}{q^l} \sum \Delta_{i,u_1}(c_1) \cdot \ldots \cdot \Delta_{i,u_l}(c_l),$$

где $c \in K$, а оба суммирования проводятся по всем $c_1, \ldots, c_l \in K$, для которых выполнено равенство $c_1 y_{u_1} \oplus \ldots \oplus c_l y_{u_l} = c$. Значит,

$$\frac{1-\Delta^l}{q} \le \mathbf{P}\{a_{i,u_1} y_{u_1} \oplus \ldots \oplus a_{i,u_l} y_{u_l} = c\} \le \frac{1+\Delta^l}{q}.$$

Следовательно,

$$\left(\frac{1-\Delta^l}{q}\right)^{T} \le \mathbf{P}\{Ay = b|E\} \le \left(\frac{1+\Delta^l}{q}\right)^{T} \qquad (30)$$

для любого события E, которое не зависит от совокупности случайных элементов, стоящих в столбцах матрицы A с номерами $u_1, \ldots, u_l$.

Выберем в наборе $x^1, \ldots, x^k$ векторы $x^{s_1}, \ldots, x^{s_j}$, о которых шла речь в замечании 4. Для каждого $s \in \{s^1, \ldots, s^j\}$ введем множество M_s столбцов матрицы A, отвечающих таким ненулевым координатам вектора y^s, в которых остальные векторы из набора $y^{s_1}, \ldots, y^{s_j}$ имеют только нулевые координаты. Тогда согласно замечанию 4 множества M_{s_u} попарно не пересекаются и $|M_{s_u}| \ge l$, $u = 1, \ldots, j$. Поэтому по аналогии с (30) получаем неравенства

$$\left(\frac{1-\Delta^l}{q}\right)^{jT} \le \mathbf{P}\{Ay^{s_1} = b^{s_1}, \ldots, Ay^{s_j} = b^{s_j} \mid E\} \le \left(\frac{1+\Delta^l}{q}\right)^{jT}$$

для любого события E, не зависящего от элементов столбцов матрицы A из множества $\bigcup_{u=1}^{j} M_{s_u}$. Кроме того,

$$\mathbf{P}\{F(x^1) = b^1, \ldots, F(x^k) = b^k\} \le \mathbf{P}\{F(x^{s_1}) = b^{s_1}, \ldots, F(x^{s_j}) = b^{s_j}\} = \\ = \mathbf{P}\{Ay^{s_1} = b^{s_1}, \ldots, Ay^{s_j} = b^{s_j}\}. \tag{31}$$

Из приведенных соотношений вытекают неравенства (28) и (29). Во втором случае следует воспользоваться тем, что неравенство (31) при $j = k$ обращается в равенство. Лемма доказана.

Лемма 2. *При всех $j = 1, \ldots, k$ выполнено неравенство*

$$|D_{k,j}^{f} \setminus D_{k,j}^{f}(\ln n)| \le q^{jn} \exp\{n(\ln(1 - p(j)) + \varepsilon(n))\}, \tag{32}$$

где $p(j) = (q-1)q^{-j}$ и $\varepsilon(n) \to 0$ при $n \to 0$.

Доказательство. Пусть $(x^1, \ldots, x^k) \in D_{k,j}^{f} \setminus D_{k,j}^{f}(\ln n)$. Тогда

$$\operatorname{rank}(x^1, \ldots, x^k) \le \operatorname{rank}(G(x^1), \ldots, G(x^k)) = j$$

и найдется такой набор векторов $x^{s_1}, \ldots, x^{s_j}$, что $\operatorname{rank}(x^{s_1}, \ldots, x^{s_j}) = \operatorname{rank}(x^1, \ldots, x^k)$ и $\eta^s(x^{s_1}, \ldots, x^{s_j}) < \ln n$ при некотором числе $s \in \{s_1, \ldots, s_j\}$. Поэтому

$$|D_{k,j}^{f} \setminus D_{k,j}^{f}(\ln n)| \le \tag{33}$$

$$\le C_k^j q^{j(k-j)} \left| \left\{ (x^1, \ldots, x^j) \in (V^n)^j : \exists \alpha \in \{1, \ldots, j\} : \eta^{\alpha}(x^1, \ldots, x^j) < \ln n \right\} \right| \le$$

$$\le C_k^j q^{j(k-j)} \sum_{\alpha=1}^{j} \left| \left\{ (x^1, \ldots, x^j) \in (V^n)^j : \eta^{\alpha}(x^1, \ldots, x^j) < \ln n \right\} \right|. \tag{34}$$

Все слагаемые суммы в правой части (34) одинаковы и равны числу матриц (над полем $GF(q)$) размера $j \times n$, в которых имеется менее $\ln n$ столбцов с ненулевым элементом в заданной строке и нулями в остальных позициях. При равновероятном случайном выборе матрицы число таких столбцов имеет биномиальное распределение с параметрами n и $((q-1)/q)(1/q)^{j-1} = p(j)$. Поэтому

$$\left| \left\{ (x^1, \ldots, x^j) \in (V^n)^j : \eta^{\alpha}(x^1, \ldots, x^j) < \ln n \right\} \right| =$$

$$= q^{jn} \sum_{0 \le i < \ln n} C_n^i p^i(j)(1 - p(j))^{n-i} = q^{jn}(1 - p(j))^n \sum_{0 \le i < \ln n} C_n^i \left(\frac{p(j)}{1 - p(j)} \right)^i =$$

$$= q^{jn} \exp\{n(\ln(1 - p(j)) + o(1)\}. \tag{35}$$

Из (34) и (35) следует соотношение (32). Лемма 2 доказана.

Приступим к проверке условий (23)–(27). Соотношение (23) следует из (29) и условия $\Delta \to 0$.

Проверим условие (24). Имеем

$$\sum_{(x,b)\in R_u} \mathbf{P}\{F(x) = b\} = \Sigma_{u,1} + \Sigma_{u,2}, \tag{36}$$

где

$$\Sigma_{u,1} = \sum_{(x,b)\in R_u,\ \|x\|\geq \ln n} \mathbf{P}\{F(x) = b\},$$

$$\Sigma_{u,2} = \sum_{(x,b)\in R_u,\ \|x\|< \ln n} \mathbf{P}\{F(x) = b\}.$$

Используя неравенства (29) (где $k = 1$, $l = \|x\| > \ln n$), получаем

$$\left(\frac{1-\Delta^{\ln n}}{q}\right)^T \leq \frac{\Sigma_{u,1}}{|\{(x,b)\in R_u\colon \|x\| > \ln n\}|} \leq \left(\frac{1+\Delta^{\ln n}}{q}\right)^T. \tag{37}$$

Далее мы воспользуемся условиями (16), (10) и $\Delta \to 0$, из которых следует, что

$$T = O(n), \quad T\Delta^{\ln n} \to 0. \tag{38}$$

Поэтому аналогично (35) получаем, что

$$\begin{aligned} |\{(x,b)\in R_u\colon \|x\| \leq \ln n\}| &\leq |\{x\in V^n\colon \|x\| \leq \ln n\}|\cdot|B| = \\ &= |B|\cdot q^n \sum_{0\leq i<\ln n} C_n^i((q-1)/q)^i(1/q)^{n-i} = \\ &= |B|\cdot \sum_{0\leq i<\ln n} C_n^i(q-1)^i = O((n(q-1))^{\ln n}|B|). \end{aligned} \tag{39}$$

Из (15) и (39) следует, что

$$|\{(x,b)\in R_u\colon \|x\| > \ln n\}| = |R_u|(1+o(1)).$$

Поэтому из (37) и (38) получаем, что $\Sigma_{u,1} \to \lambda'_u$.

Используя оценки (29) при $k = l = 1$ и соотношения (15), (38), (39) и $\Delta \to 0$, получаем

$$\Sigma_{u,2} \leq |\{(x,b)\in R_u\colon \|x\| \leq \ln n\}| \left(\frac{1+\Delta}{q}\right)^T =$$

$$= O\left((n(q-1))^{\ln n}|B|\right)\left(\frac{1+\Delta}{q}\right)^T =$$

$$= \exp\left\{-n\ln q + T\ln(1+\Delta) + O(\ln^2 n)\right\} =$$

$$= \exp\{-n\ln q(1+o(1))\} = o(1).$$

Подставив в (36) выведенные соотношения для $\Sigma_{u,1}$ и $\Sigma_{u,2}$, получим (24).

Проверим выполнение условия (25). Согласно определениям множество $J_k \setminus I_k$ образуют наборы $((x^1, b^1), \dots, (x^k, b^k))$, в которых $(x^1, \dots, x^k) \in \in D^{\hat{f}}_{k,k}(\ln n)$. Из неравенств (29) вытекает, что для них

$$\left(\frac{1-\Delta^{\ln n}}{1+\Delta^{\ln n}}\right)^{kT} \le \frac{\mathbf{P}\{F(x^1)=b^1,\dots,F(x^k)=b^k\}}{\mathbf{P}\{F(x^1)=b^1\}\dots\{F(x^k)=b^k\}} \le \left(\frac{1+\Delta^{\ln n}}{1-\Delta^{\ln n}}\right)^{kT}.$$

Поэтому из (38) следует (25).

Проверим соотношение (26) при $k \ge 2$. Из определений и равенства

$$D^{\hat{f}}_k \cup \left(D^{\hat{f}}_{k,k} \setminus D^{\hat{f}}_{k,k}(\ln n)\right) = \left(\bigcup_{j=1}^{k-1} D^{\hat{f}}_{k,j}(\ln n)\right) \cup \left(\bigcup_{j=1}^{k} D^{\hat{f}}_{k,j} \setminus D^{\hat{f}}_{k,j}(\ln n)\right) \quad (40)$$

следует, что

$$\sum_{(v^1,\dots,v^k)\in I_k} \prod_{j=1}^{k} \mathbf{P}\{F(x^j)=b^j\} \le S_1 + S_2, \quad (41)$$

где

$$S_1 = \sum_{j=1}^{k-1} \sum_{b^1,\dots,b^k\in B} \sum_{(x^1,\dots,x^k)\in D^{\hat{f}}_{k,j}(\ln n)} \prod_{j=1}^{k} \mathbf{P}\{F(x^j)=b^j\},$$

$$S_2 = \sum_{j=1}^{k} \sum_{b^1,\dots,b^k\in B} \sum_{(x^1,\dots,x^k)\in D^{\hat{f}}_{k,j}\setminus D^{\hat{f}}_{k,j}(\ln n)} \prod_{j=1}^{k} \mathbf{P}\{F(x^j)=b^j\}.$$

Используя оценки (29) (при $k = 1$) и (19), получаем

$$S_1 \le |B|^k \sum_{j=1}^{k-1} \sum_{(x^1,\dots,x^k)\in D^f_{k,j}(\ln n)} \left(\frac{1+\Delta^{\ln n}}{q}\right)^{jT} <$$

$$< |B|^k \sum_{j=1}^{k-1} |D^f_{k,j}| \left(\frac{1+\Delta^{\ln n}}{q}\right)^{jT} \le$$

$$\le |B|^k \left(\frac{1+\Delta^{\ln n}}{q}\right)^{kT} \sum_{j=1}^{k-1}\sum_{s=1}^{j} C_k^s q^{s(k-s)} q^{ns} =$$

$$= \left(q^{n-T}|B|\right)^k (1+\Delta^{\ln n})^{kT} \frac{1}{q^{nk}} \sum_{j=1}^{k-1}\sum_{s=1}^{j} C_k^s q^{s(n+k-s)}.$$

С учетом условий (15) и соотношений (38) получаем, что $S_1 \to 0$.

Аналогичным способом, используя также лемму 2, получаем оценки

$$S_2 \le \left(q^{n-T}|B|\right)^k (1+\Delta)^{kT} \frac{1}{q^{nk}} \sum_{j=1}^{k} |D^f_{k,j} \setminus D^f_{k,j}(\ln n)| =$$

$$= \frac{1}{q^{nk}} \sum_{j=1}^{k} q^{nj} \exp\{n\ln(1-p(j)) + kT\ln(1+\Delta) + o(n)\} = o(1). \qquad (42)$$

Подставив в (41) выведенные соотношения для S_1 и S_2, получим (26).

Наконец, проверим соотношение (27). Пусть $k \ge 2$. Из определений следует равенство

$$\sum_{(v^1,\dots,v^k)\in I_k} \mathbf{P}\{F(x^1) = b^1, \dots, F(x^k) = b^k\} =$$

$$= \sum_{(v^1,\dots,v^k)\in I_k,\ (x^1,\dots,x^k)\in D^f_k \cup \left(D^f_{k,k}\setminus D^f_{k,k}(\ln n)\right)} \mathbf{P}\{F(x^1) = b^1, \dots, F(x^k) = b^k\}. \qquad (43)$$

Введем множества

$$\overline{D}^f_{k,j} = D^f_{k,j} \cap \left\{(x^1,\dots,x^k) \in (V^n \setminus \{0^n\})^k \colon G(x^\alpha) \ne cG(x^\beta),\ c\in K,\ \alpha\ne\beta\right\}.$$

Заметим, что $\overline{D}^f_{k,1} = \varnothing$, k=2,3,..., и положим $\overline{D}^f_2 = \varnothing$, $\overline{D}^f_k = \bigcup_{j=2}^{k-1} \overline{D}^f_{k,j}$.

Лемма 3. *Пусть множество $H_f \times B$ не содержит подобных векторов, $(x^1, \dots, x^k) \in D_k^f \setminus \overline{D}_k^f$ и $((x^1, b^1), \dots, (x^k, b^k)) \in J_k$. Тогда*

$$\mathbf{P}\{F(x^1) = b^1, \dots, F(x^k) = b^k\} = 0.$$

Доказательство леммы 3 повторяет доказательство леммы 4.2 работы [1], и мы его не приводим.

Из (43) и леммы 3 следует, что

$$\sum_{(v^1,\dots,v^k)\in I_k} \mathbf{P}\{F(x^1) = b^1, \dots, F(x^k) = b^k\} =$$

$$= \sum_{(v^1,\dots,v^k)\in J_k,\ (x^1,\dots,x^k)\in\overline{D}_k^f\cup\left(D_{k,k}^f\setminus D_{k,k}^f(\ln n)\right)} \mathbf{P}\{F(x^1) = b^1, \dots, F(x^k) = b^k\}. \quad (44)$$

Теперь рассмотрим произвольный набор векторов $x^1, \dots, x^k \in V^n$. Ему соответствует (возможно пустая) система $L_G(x^1, \dots, x^k)$ уравнений над полем $GF(q)$ вида

$$\alpha_1 G(x^1) \oplus \dots \oplus \alpha_k G(x^k) = 0,$$

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

Лемма 4. *Пусть $(b^1, \dots, b^k) \notin B(x^1, \dots, x^k)$, $(x^1, \dots, x^k) \in \overline{D}_k^f$. Тогда* $\mathbf{P}\{F(x^1) = b^1, \dots, F(x^k) = b^k\} = 0$.

Доказательство леммы 4 повторяет доказательство леммы работы [1], и мы его опускаем.

Из (44) и леммы 4 следует, что

$$\sum_{(v^1,\dots,v^k)\in J_k,\ (x^1,\dots,x^k)\in\overline{D}_k^f\cup\left(D_{k,k}^f\setminus D_{k,k}^f(\ln n)\right)} \mathbf{P}\{F(x^1) = b^1, \dots, F(x^k) = b^k\} =$$

$$= \sum_{j=2}^{k-1} \sum_{(x^1,\dots,x^k)\in\overline{D}_{k,j}^f} \sum_{(b^1,\dots,b^k)\in B(x^1,\dots,x^k)} \mathbf{P}\{F(x^1) = b^1, \dots, F(x^k) = b^k\} +$$

$$+ \sum_{(x^1,\dots,x^k)\in D_{k,k}^f\setminus D_{k,k}^f(\ln n)} \sum_{(b^1,\dots,b^k)\in B^k} \mathbf{P}\{F(x^1) = b^1, \dots, F(x^k) = b^k\}. \quad (45)$$

Здесь нам понадобится оценка мощности множества $B(x^1, \dots, x^k)$.

Лемма 5. *Пусть* $2 \le j \le k-1$ *и* $(x^1, \dots, x^k) \in \overline{D}^f_{k,j}$. *Тогда*

$$|B(x^1, \dots, x^k)| \le \rho(B)|B|^j.$$

Лемма 5 повторяет (с некоторыми отличиями в обозначениях) лемму 4.4 работы [1]. Поэтому ее доказательство мы не приводим.

Введем при $1 \le l \le n$ множества

$$\overline{D}^f_{k,j}(l) = D^f_{k,j}(l) \cap$$
$$\cap \left\{(x^1, \dots, x^k) \in (V^n \setminus \{0^n\})^k \colon G(x^\alpha) \ne cG(x^\beta),\ c \in K,\ \alpha \ne \beta\right\}.$$

Используя эти обозначения, можно записать

$$\sum_{j=2}^{k-1} \sum_{(x^1,\dots,x^k)\in\overline{D}^f_{k,j}} \sum_{(b^1,\dots,b^k)\in B(x^1,\dots,x^k)} \mathbf{P}\{F(x^1) = b^1, \dots, F(x^k) = b^k\} =$$
$$= \sum_{j=2}^{k-1} \sum_{(x^1,\dots,x^k)\in\overline{D}^f_{k,j}(\ln n)} \sum_{(b^1,\dots,b^k)\in B(x^1,\dots,x^k)} \mathbf{P}\{F(x^1) = b^1, \dots, F(x^k) = b^k\} +$$
$$+ \sum_{j=2}^{k-1} \sum_{(x^1,\dots,x^k)\in\overline{D}^f_{k,j}\setminus\overline{D}^f_{k,j}(\ln n)} \sum_{(b^1,\dots,b^k)\in B(x^1,\dots,x^k)} \mathbf{P}\{F(x^1) = b^1, \dots, F(x^k) = b^k\}. \tag{46}$$

Применим лемму 5 и оценку (28) (при $l = \ln n$) к первому слагаемому в правой части равенства (46). Получим

$$\sum_{j=2}^{k-1} \sum_{(x^1,\dots,x^k)\in\overline{D}^f_{k,j}(\ln n)} \sum_{(b^1,\dots,b^k)\in B(x^1,\dots,x^k)} \mathbf{P}\{F(x^1) = b^1, \dots, F(x^k) = b^k\} \le$$
$$\le \sum_{j=2}^{k-1} \sum_{(x^1,\dots,x^k)\in\overline{D}^f_{k,j}(\ln n)} |B(x^1, \dots, x^k)| \left(\frac{1+\Delta^{\ln n}}{q}\right)^{jT} \le$$
$$\le \rho(B) \sum_{j=2}^{k-1} \sum_{(x^1,\dots,x^k)\in\overline{D}^f_{k,j}(\ln n)} |B|^j \left(\frac{1+\Delta^{\ln n}}{q}\right)^{jT} \le$$

$$\leq \rho(B)\sum_{j=2}^{k-1}|\overline{D}^f_{k,j}|\cdot|B|^j\left(\frac{1+\Delta^{\ln n}}{q}\right)^{jT}\leq$$

$$\leq \rho(B)\sum_{j=2}^{k-1}\frac{|\overline{D}^f_{k,j}|}{q^{jn}}\sum_{j=2}^{k-1}\left(q^{n-T}|B|(1+\Delta^{\ln n})^T\right)^j. \tag{47}$$

Согласно (15) и (38) имеет место соотношение

$$\sum_{j=2}^{k-1}\left(q^{n-T}|B|(1+\Delta^{\ln n})^T\right)^j = O(1). \tag{48}$$

Лемма 6. *Пусть* $2\leq j\leq k-1$, $n\to\infty$, *а множество* H_f *меняется так, что* $\rho(H_f)\to 0$. *Тогда* $q^{-jn}|\overline{D}^f_{k,j}|\to 0$.

Эта лемма является частным случаем леммы 4.5 работы [1]. Поэтому ее доказательство мы не приводим.

Учитывая условие (8), соотношения (47), (48), лемму 6 и (48), приходим к выводу, что первое слагаемое в правой части (46) стремится к нулю.

Аналогичным образом с помощью лемм 1а и 5 оцениваем второе слагаемое в правой части (46):

$$\sum_{j=2}^{k-1}\sum_{(x^1,\ldots,x^k)\in\overline{D}^f_{k,j}\setminus\overline{D}^f_{k,j}(\ln n)}\sum_{(b^1,\ldots,b^k)\in B^k}\mathbf{P}\{F(x^1)=b^1,\ldots,F(x^k)=b^k\}\leq$$

$$\leq\sum_{j=2}^{k-1}\sum_{(x^1,\ldots,x^k)\in\overline{D}^f_{k,j}\setminus\overline{D}^f_{k,j}(\ln n)}|B(x^1,\ldots,x^k)|\left(\frac{1+\Delta}{q}\right)^{jT}\leq$$

$$\leq\rho(B)\sum_{j=2}^{k-1}\sum_{(x^1,\ldots,x^k)\in\overline{D}^f_{k,j}\setminus\overline{D}^f_{k,j}(\ln n)}|B|^j\left(\frac{1+\Delta}{q}\right)^{jT}=$$

$$=\rho(B)\sum_{j=2}^{k-1}\left|\overline{D}^f_{k,j}\setminus\overline{D}^f_{k,j}(\ln n)\right|\cdot|B|^j\left(\frac{1+\Delta}{q}\right)^{jT}. \tag{49}$$

Аналогично оцениваем второе слагаемое в (45):

$$\sum_{(x^1,\ldots,x^k)\in D^f_{k,k}\setminus D^f_{k,k}(\ln n)}\sum_{(b^1,\ldots,b^k)\in B^k}\mathbf{P}\{F(x^1)=b^1,\ldots,F(x^k)=b^k\}\leq$$

$$\leq|B|^k\left|D^f_{k,k}\setminus D^f_{k,k}(\ln n)\right|\left(\frac{1+\Delta}{q}\right)^{kT}. \tag{50}$$

Мы уже убедились в (42), что суммы в правых частях (49) и (50) при переходе к пределу стремятся к нулю. Значит, вторые слагаемые в правых частях (49) и (50) тоже стремятся к нулю. Вместе с (44) это влечет (27). Теорема 6 доказана.

Доказательство теоремы 3. Заметим, что условия теоремы 6 повторяют условия теоремы 3 применительно к подмножествам $R_1, \ldots, R_s$ множества $J \subseteq D \times B$. Возьмем $J = D \times B$, $R_j = D \times B_j$, $j = 1, \ldots, s$, $B = B_1 \cup \ldots \cup B_s$. Тогда $\lambda'_j = \lambda_j$, $j = 1, \ldots, s$. Используя теорему 6, получаем утверждение теоремы 3.

Доказательство теоремы 4 проведем для случая, когда все $\lambda_k > 0$. Ее вывод для общего случая из этого частного проводится стандартными рассуждениями, которые мы опускаем.

Напомним, что

$$l_r(G(D), B) = |\{k \in \{1, \ldots, M\} : |(G(D)B)_k| = r\}|, \quad r = 1, \ldots, q-1,$$

где $(G(D)B)_1, \ldots, (G(D)B)_M$ — разбиение множества $G(D) \times B$ на классы подобных векторов; M — общее число таких классов. Выберем из каждого класса $(G(D)B)_k$ по одному произвольному вектору $d^k \in (G(D)B)_k$ и положим

$$J = \left\{d^1, \ldots, d^M\right\} \subseteq H_f \times B.$$

Построим разбиение этого множества на непересекающиеся множества $R_1, \ldots, R_{q-1}$ по правилу

$$R_r = \{d^s : s \in \{1, \ldots, M\},\ |(G(D)B)_s| = r\}, \quad r = 1, \ldots, q-1, \tag{51}$$

и введем случайные величины

$$\xi_r = \sum_{(x,b) \in R_r} I\{F(x) = b\}, \quad r = 1, \ldots, q-1, \tag{52}$$

с множествами $R_1, \ldots, R_{q-1}$ из (51). Тогда

$$\xi(V^n \setminus \{0^n\}, F, B) = \xi_1 + 2\xi_2 + \ldots + (q-1)\xi_{q-1}. \tag{53}$$

Используя предположения теоремы 4, нетрудно убедиться, что для случайных величин (52) выполнены условия теоремы 6, причем $\lambda'_j = \lambda_j$, $j = 1, \ldots, q-1$. Поэтому согласно теореме 6 распределение вектора $(\xi_1, \ldots, \xi_{q-1})$ сходится к распределению вектора $(\pi_1, \ldots, \pi_{q-1})$, компоненты которого являются независимыми в совокупности случайными величинами, распределенными по закону Пуассона с параметрами $\lambda_1, \ldots, \lambda_{q-1}$ соответственно. Осталось воспользоваться равенством (53). Теорема 4 доказана.

Замечание 6. Использованные в доказательствах теорем 3, 4 и 6 методы можно применить и при исследовании асимптотических свойств числа специальных решений заведомо совместных систем нелиненйных уравнений. Изучению таких свойств заведомо совместного варианта системы (7) при $K = GF(2)$ посвящены работы [6] и [7]. В этих работах указаны достаточные условия сходимости и оценки скорости сходимости распределения числа решений такой системы к распределению Пуассона.

3. Доказательства теоремы 5 и следствия 1

Доказательство теоремы 5. Напомним, что рассматривается отображение $f(x) = (f_1(x), \ldots, f_{m-n}(x))$, в качестве части координатных функций которого выступают все произведения вида $x_1^{d_1} \ldots x_n^{d_n}$, $n \geq 2$, для которых $2 \leq d_1 + \ldots + d_n \leq d$. Здесь $d = d(n) \leq (q-1)n$ — заданное число, и $m = m(n) \geq m(n,d) = \sum_{r=1}^{d} C_n^r$.

Чтобы оценить величину $\rho(H_f)$, обратимся к определению функции ρ, приведенному в разделе 1. Согласно этому определению

$$\rho(H_f) = \frac{N_f}{|H_f|^2}, \tag{54}$$

где N_f — максимально возможное при $a_1, a_2, a_3 \in K \setminus \{0\}$, $d \in V^T$ число решений уравнения

$$a_1 y^1 \oplus a_2 y^2 \oplus a_3 y^3 = d \tag{55}$$

относительно тройки векторов $(y^1, y^2, y^3) \in (H_f)^3$. Здесь, очевидно, можно положить $a_1 = 1$.

Уравнение (55) является системой из m уравнений относительно неизвестных $x_1, \ldots, x_n$, которую можно разбить на три частных системы. Первая система состоит из n линейных уравнений

$$x_i^1 \oplus a_2 x_i^2 \oplus a_3 x_i^3 = d_i, \quad i = 1, \ldots, n. \tag{56}$$

Вторая система состоит из $[n/2]$ уравнений

$$x_i^1 x_{i+1}^1 \oplus a_2 x_i^2 x_{i+1}^2 \oplus a_3 x_i^3 x_{i+1}^3 = d_{i,i+1}, \quad i = 1, 3, \ldots, 2[n/2] - 1. \tag{57}$$

Третья система содержит все остальные уравнения.

Пусть $N_f^{(56)(57)}$ — число решений системы (56)–(57) относительно тройки $(y^1, y^2, y^3) \in (V^T)^3$. Тогда $N_f^{(56)(57)} \geq N_f$, а $N_f^{(56)(57)}$ совпадает с числом $N_f^{(59)}$ решений системы

$$(d_i \ominus a_2 x_i^2 \ominus a_3 x_i^3)(d_{i+1} \ominus a_2 x_{i+1}^2 \ominus a_3 x_{i+1}^3) \oplus a_2 x_i^2 x_{i+1}^2 \oplus a_3 x_i^3 x_{i+1}^3 = d_{i,i+1}, \tag{58}$$

$$i = 1, 3, \ldots, 2[n/2] - 1, \tag{59}$$

получаемой подстановкой уравнений системы (56) в уравнения системы (57).

В случае, когда все члены с неизвестными в некотором уравнении системы (59) сокращаются, это уравнение имеет либо q^4 решений, либо не имеет их вовсе. В остальных случаях число решений этого уравнения $N_f^{(59)}(i)$ удовлетворяет неравенству

$$N_f^{((59)}(i) \leq q^4 - 1. \tag{60}$$

Покажем, что для системы (59) осуществляется только этот последний случай.

Пусть $d_i \neq 0$ или $d_{i+1} \neq 0$. Тогда i-е уравнение системы (59) обязательно имеет несократимый линейный член. Следовательно, выполняется (60).

Пусть $d_i = d_{i+1} = 0$. Тогда i-е уравнение системы (59) преобразуется к виду

$$2a_2 x_i^2 x_{i+1}^2 \oplus a_2 x_i^2 a_3 x_{i+1}^3 \oplus a_3 x_i^3 a_2 x_{i+1}^2 \oplus 2a_3 x_i^3 x_{i+1}^3 = d_{i,i+1}.$$

Коэффициенты второго и третьего слагаемых левой части этого уравнения отличны от нуля. Значит, опять выполнено неравенство (60).

Осталось заметить, что уравнения системы (59) зависят от разных неизвестных. Поэтому, используя (60), получаем

$$N_f^{(3.5)} = \prod_{i=1}^{[n/2]} N_f^{(3.5)}(i) \leq \left(q^4 - 1\right)^{[n/2]}.$$

Подставив эту оценку в (54) и вспомнив, что $|H_f| = q^n - 1$, получим неравенство

$$\rho(H_f) \leq \left(\frac{q^n}{q^n - 1}\right)^2 \left(1 - q^{-4}\right)^{[n/2]},$$

из которого следует, что $\rho(H_f) \to 0$ при $n \to \infty$. Теорема 5 доказана.

Доказательство следствия 1. При изучении числа $\xi(V^n \setminus \{0^n\}, F, B)$ ненулевых решений включения $Fx \in B$ со случайно и равновероятно выбранным отображением F (из указанного в формулировке следствия множества отображений) мы воспользуемся теоремой 2. Проверим выполнение ее условий.

Рассматривается случай $n, T \to \infty$, причем $|D| = q^n - 1 \to \infty$. Из равновероятности отображения $F(x) = A_1 x + A_2 f(x)$ следует, что матрица $A = (A_1, A_2)$ распределена на множестве матриц соответствующего размера равномерно. Значит, $\Delta = 0$ и выполнено условие $T\Delta \to 0$ теоремы 2. Согласно теореме 5 имеет место соотношение $\rho(H_f) \to 0$, и, значит, выполнено условие (5) (в данном случае $G(D) = H_f$). Таким образом, условия теоремы 2 выполнены, и осталось определить значения параметров предельного распределения, задаваемые соотношениями (6).

Подобные векторы в H_f обязательно имеют единичный вес и образуют классы

$$(H_f)_k = \{y \in H_f : \|y\| = 1,\ y_k \neq 0\}, \quad k = 1, \ldots, n.$$

Остальные векторы в H_f не имеют подобных. Они образуют классы $(H_f)_k$, $k = 1 + n, \ldots, q^n - 1$, по одному вектору в каждом классе.

Так как $|(H_f)_k| = q - 1$, $k = 1, \ldots, n$ и $|(H_f)_k| = 1$, $k = 1 + n, \ldots, q^n - 1$, то подобные векторы множества $H_f \times B$ образуют не более $n|B|$ классов мощности $q - 1$ и не менее $(q^n - 1)|B|$ единичных классов. Поэтому

$$\sum_{r=2}^{q-1} l_r(G(D), B) \leq n(q-1)|B|, \tag{61}$$

$$(q^n - 1 - n(q-1))\,|B| \leq l_1(G(D), B) \leq (q^n - 1)|B|. \tag{62}$$

Осталось воспользоваться условием $q^{n-T} \cdot |B| \to \lambda$. Из него и (61), (62) следует, что $\lambda_1 = \lambda$, а $\lambda_2 = \ldots = \lambda_{q-1} = 0$. Поэтому согласно теореме 2 предельное распределение случайной величины является распределением Пуассона с параметром λ. Следствие 1 доказано.

Авторы признательны А. М. Зубкову за полезные замечания.

Список литературы

1. *Копытцев В. А., Михайлов В. Г.* Теоремы пуассоновского типа для числа специальных решений случайного линейного включения. — Дискретная математика, 2010, т. 22, вып. 2, с. 3–21.

2. *Копытцев В. А.* О числе решений систем линейных булевых уравнений в множестве векторов, обладающих заданным числом единиц. — Дискретная математика, 2002, т. 14, вып. 4, с. 87–109.
3. *Копытцев В. А.* О числе решений системы случайных линейных уравнений. — Дискретная математика, 2006, т. 18, вып. 1, с. 40–62.
4. *Михайлов В. Г.* Предельные теоремы для числа решений системы случайных линейных уравнений, попавших в заданное множество. — Дискретная математика. 2007, т. 19, вып. 1, с. 17–26.
5. *Михайлов В. Г.* О предельной теореме Б. А. Севастьянова для сумм зависимых случайных индикаторов. — Обозрение прикл. и промышл. математики, 2003, т. 10, вып. 3, с. 571–578.
6. *Масол В. И.* Теорема о предельном распределении числа ложных решений системы нелинейных случайных булевых уравнений. — Теория вероятностей и ее применения, 1998, т. 43, вып. 1, с. 41–56.
7. *Masol V., Slobodian M.* Estimation of the rate convergence to the limit distribution of the number of false solution of the system of nonlinear random Boolean equations that has a linear part. — Theory Stoch. Process., 2007, v. 13(29), № 1–2, p. 132–143.