V. A. Kopytcev, V. G. Mikhailov, Conditions of convergence to the Poisson distribution for the number of solutions of random inclusions, *Mat. Vopr. Kriptogr.*, 2012, Volume 3, Issue 3, 35–55

DOI: 10.4213/mvk60

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2012 Т. 3 № 3 С. 35–55

УДК: 519.212.2+519.214.5

Условия сходимости к распределению Пуассона для чисел решений случайных включений

В. А. Копытцев[1], **В. Г. Михайлов**[2]

[1]Академия криптографии Российской Федерации, Москва
[2]Математический институт им. В. А. Стеклова РАН, Москва

Получено 20.V.2011

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 новые достаточные условия сходимости при $n, T \to \infty$ распределения числа решений системы включений $x \in D$, $F(x) \in B$ к распределению Пуассона.

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

Conditions of convergence to the Poisson distribution for the number of solutions of random inclusions

V. A. Kopytcev[1], **V. G. Mikhailov**[2]

[1]*Academy of Cryptography of the Russian Federation, Moscow*
[2]*Steklov Mathematical Institute of RAS, Moscow*

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; let $D \subset V^n$, $B \subset V^T$. For the number of solutions of random inclusions $x \in D$, $F(x) \in B$ we find new sufficient conditions of weak convergence to the Poisson law as $n, T \to \infty$.

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

Citation: *Mathematical Aspects of Cryptography*, 2012, vol. 3, no. 3, pp. 35–55 (Russian).

§ 1. Введение

В работе исследуется распределение числа $\xi(D, F, B)$ решений системы включений

$$x \in D, \quad F(x) \in B, \tag{1.1}$$

где $F(x) = (F_1(x), \ldots, F_T(x))\colon V^n \to V^T$ — случайное отображение пространства n-мерных векторов V^n над полем $K = GF(q)$ в пространство V^T, а D и B — некоторые множества n-мерных и T-мерных векторов над полем K.

Рассмотрим класс включений вида (1.1) с функцией

$$F(x) = A_1 x + A_2 f(x) + S(x), \tag{1.2}$$

где A_1 и A_2 — независимые случайные матрицы (над полем K) размеров $T \times n$ и $T \times m$ соответственно, $f(x) = (f_1(x), \ldots, f_m(x))$ — заданное отображение, удовлетворяющее условию $f(0^n) = 0^m$, а $S(x) = (S_1(x), \ldots, S_T(x))$ — случайное отображение, не зависящее от матриц A_1, A_2. Случай, когда $S(x) \equiv 0^T$, был исследован ранее в работах [1, 2].

Нетрудно заметить, что класс включений с функцией $F(x)$ вида (1.2) с $S(x) \not\equiv 0^T$ содержит системы полиномиальных уравнений над полем $K = GF(q)$ вида

$$\sum_{\substack{d_1,\ldots,d_n \in \{0,\ldots,q-1\} \\ 1 \le d_1+\ldots+d_n \le g_t}} a^{(t)}_{d_1 \ldots d_n} x_1^{d_1} \ldots x_n^{d_n} = b_t, \quad t = 1, \ldots, T, \tag{1.3}$$

где $a^{(t)}_{d_1 \ldots d_n}$ — независимые в совокупности случайные величины, а параметры g_t зависят от номеров уравнений и удовлетворяют условиям $2 \le g_t \le n(q-1)$, $t = 1, \ldots, T$. Возможность исследования случайных систем из полиномиальных уравнений разных степеней является главным отличием нынешней постановки задачи от [1, 2].

Сформулируем результаты работы. Далее предполагаем, что от параметров n, T зависят числа $m = m(n)$, множества $D = D(n)$, $B = B(T)$, матрицы $A_s = A_s(n, T)$, $s = 1, 2$, и отображения $f(x)$, $S(x)$.

Всюду далее элементы случайной матрицы $A = (A_1, A_2)$ независимы в совокупности и

$$\mathbf{P}\{a_{t,j} = k\} = \frac{1 + \Delta_{t,j}(k)}{q}, \quad k \in K, \tag{1.4}$$

где $\sum_{k \in K} \Delta_{t,j}(k) = 0$, $t = 1, \ldots, T$, $j = 1, \ldots, n + m$. Пусть

$$\Delta = \max_{t,j,k} |\Delta_{t,j}(k)| < 1. \tag{1.5}$$

Обозначим через $N(k_1, k_2, k_3, c, D)$ число решений уравнения $k_1u^1 + k_2u^2 + k_3u^3 = c$ относительно тройки векторов $(u^1, u^2, u^3) \in D^3$, где $k_1, k_2, k_3 \in K\backslash\{0\}$, $c \in V^n$. Пусть

$$N(D) = \max_{k_1,k_2,k_3,c} N(k_1, k_2, k_3, c, D), \quad \rho(D) = N(D)/|D|^2. \tag{1.6}$$

Очевидно, что $\rho(D) \le 1$. Так как уравнение $k_1u^1 + k_2u^2 + k_3u^3 = c$ при $c \in D$ и $k_1 = k_2 = 1$, $k_3 = -1$ имеет решения $(u^1, u^2, u^3) = (c, u, u)$, то

$$|D|^{-1} \le \rho(D) \le 1. \tag{1.7}$$

Ниже будет играть важную роль условие $\rho(D(n)) \to 0$ при $n \to \infty$ (заметим, что тогда $|D(n)| \to \infty$).

Сначала обратимся к случаю, когда отображение $f(x) \equiv 0^T$, и исследуем предельное поведение числа решений системы

$$x \in D, \quad Ax + S(x) \in B, \tag{1.8}$$

где A — случайная матрица размера $T \times n$, а $S(x)$ — случайное отображение, не зависящее от матрицы A.

Векторы x и cx, $c \ne 0$, будем называть *подобными*.

Теорема 1. *Пусть $D \subseteq V^n\backslash\{0^n\}$, причем в этом множестве нет подобных векторов, $F(x) = Ax + S(x)$ и выполнены условия $n, T \to \infty$, $T\Delta \to 0$, $|D| \to \infty$,*

$$\rho(D) \to 0, \quad \frac{\ln|B|}{\ln\rho(D)} \to 0, \tag{1.9}$$

$$q^{-T}|D||B| \to \lambda, \quad 0 \le \lambda < \infty. \tag{1.10}$$

Тогда распределение случайной величины $\xi(D, F, B)$ сходится к распределению Пуассона с параметром λ.

Теперь перейдем к системам общего вида

$$x \in D, \quad A_1x + A_2f(x) + S(x) \in B. \tag{1.11}$$

Заменой переменных

$$y = (x, f(x)) = \big(y_1 = x_1, \dots, y_n = x_n, y_{n+1} = f_1(x), \dots, y_{n+m} = f_m(x)\big)$$

эта система сводится к системе

$$y \in D_f, \quad Ay + S^*(y) \in B, \tag{1.12}$$

где $S^*(y) = S(y_1, \ldots, y_n)$,

$$D_f = \{(x, f(x)) | x \in D\} \subseteq V^{n+m},$$

а матрица $A = (A_1, A_2)$ получена объединением столбцов матриц A_1 и A_2. Число решений системы (1.11) совпадает с числом решений системы (1.12). Используя этот факт, мы выведем из теоремы 1 следующее утверждение.

Обозначим через D'_f множество всех векторов из D_f, не имеющих в D_f подобных себе векторов.

Теорема 2. *Пусть* $D \subseteq V^n \backslash \{0^n\}$, $F(x) = A_1 x + A_2 f(x) + S(x)$ *и выполнены условия* $n, T \to \infty$, $T\Delta \to 0$, $|D| \to \infty$,

$$\frac{|D'_f|}{|D|} \to 1, \tag{1.13}$$

$$\rho(D_f) \to 0, \quad \frac{\ln |B|}{\ln \rho(D_f)} \to 0, \tag{1.14}$$

а также условие (1.10). *Тогда распределение случайной величины* $\xi(D, F, B)$ *сходится к распределению Пуассона с параметром* λ.

Замечание 1. В работе [1] было показано (см. доказательства следствий 4 и 2 в [1]), что условие (1.13) выполнено, если $D = V^n \setminus \{0^n\}$, а для множества $Q(f) = \{f_1(x), \ldots, f_m(x)\}$ справедливо хотя бы одно из условий $Q(f) \supseteq Q_n^{(2)}$ и $Q(f) \supseteq Q_n^{(t_1)} \cup Q_n^{(t_2)}$, где

$$Q_n^{(t)} = \bigcup_{\substack{d_1, \ldots, d_n \in \{0, \ldots, q-1\} \\ d_1 + \ldots + d_n = t}} \{x_1^{d_1} \ldots x_n^{d_n}\}$$

и $2 < t_1 < t_2$, НОД$(t_1 - 1, t_2 - 1) = 1$.

Пусть мощность множества $D \subseteq V^n \backslash \{0^n\}$ при переходе к пределу сравнима с мощностью пространства V^n. В этом случае условие $T\Delta \to 0$, использованное в теоремах 1 и 2, можно заменить менее ограничительным условием $\Delta \to 0$.

Теорема 3. *Пусть* $F(x) = A_1 x + A_2 f(x) + S(x)$, $D \subseteq V^n \backslash \{0^n\}$, $q^{-n}|D| \geq c > 0$ *и выполнены условия теоремы 2 с заменой условия* $T\Delta \to 0$ *условием* $\Delta \to 0$. *Тогда распределение случайной величины* $\xi(D, F, B)$ *сходится к распределению Пуассона с параметром* λ.

Замечание 2. Если $K = GF(2)$, то в V^n нет подобных векторов. Поэтому $D'_f = D_f$, а условие (1.13) в теоремах 2 и 3 можно опустить.

Дальнейший порядок изложения материала в статье следующий. Теоремы 1–3 доказываются в параграфах 2–4. В параграфе 5 теоремы 2 и 3 используются для исследования асимптотических свойств распределения числа решений систем включений из специального класса, содержащего заведомо совместные системы. В параграфе 6 рассматривается случай $K = GF(2)$. Здесь для $\xi(D, F, B)$ доказывается предельная теорема Пуассона, условия которой допускают асимптотическое вырождение распределений элементов матрицы A. Она распространяет теорему 3 работы [1] на случай $S(x) \not\equiv 0^T$.

§ 2. Доказательство теоремы 1

Доказательство теоремы 1 проведем по схеме доказательства теоремы 6 в [3]. Мы рассматриваем случай, когда $F(x) = Ax + S(x)$. Пусть $I\{E\}$ обозначает индикатор случайного события E, а $J = D \times B$. Тогда

$$\xi(D, F, B) = \sum_{(x,b)\in J} I\{F(x) = b\}. \tag{2.1}$$

В отличие от доказательства теоремы 6 в [3], которая доказывалась с помощью «многомерной» версии теоремы Б. А. Севастьянова о предельном распределении Пуассона суммы зависимых индикаторов (см. [4]), мы воспользуемся традиционной («одномерной») версией этой теоремы (см. [5, 6]). Для ее применения потребуется ряд определений. Как и в [3], введем множества

$$D_{k,j} = \{(x^1, \ldots, x^k) \in D^k\colon \operatorname{rank}\left(x^1, \ldots, x^k\right) = j\},$$
$$D_k = \bigcup\nolimits_{j=1}^{k-1} D_{k,j}\,.$$

Отметим, что

$$|D_{k,j}| \le C_k^j q^{j(k-j)} |D|^j. \tag{2.2}$$

Положим

$$J_k = \left\{((x^1, b^1), \ldots, (x^k, b^k)) \in J^k\colon (x^\alpha, b^\alpha) \ne (x^\beta, b^\beta)\ (\alpha \ne \beta)\right\}.$$

Определим исключительные множества $I_k \subset J_k$ равенством

$$I_k = \left\{((x^1, b^1), \ldots, (x^k, b^k)) \in J_k\colon (x^1, \ldots, x^k) \in D_k\right\}. \tag{2.3}$$

Для доказательства теоремы достаточно проверить выполнение условий (они отличаются от аналогичных условий в [3] лишь заменой Ax на $F(x)$)

$$\sum_{(x,b)\in J} \mathbf{P}\{F(x) = b\} \to \lambda, \tag{2.4}$$

$$\max_{(x,b)\in J} \mathbf{P}\{F(x) = b\} \to 0, \tag{2.5}$$

и при всех $k = 2, 3, \ldots$ (далее для краткости используем обозначение $v^i = (x^i, b^i)$)

$$\max_{(v^1,\ldots,v^k)\in J_k\setminus I_k} \left| \frac{\mathbf{P}\left\{F(x^1) = b^1, \ldots, F(x^k) = b^k\right\}}{\mathbf{P}\left\{F(x^1) = b^1\right\} \cdot \ldots \cdot \mathbf{P}\left\{F(x^k) = b^k\right\}} - 1 \right| \to 0, \tag{2.6}$$

$$\sum_{(v^1,\ldots,v^k)\in I_k} \prod_{i=1}^{k} \mathbf{P}\left\{F(x^i) = b^i\right\} \to 0, \tag{2.7}$$

$$\sum_{(v^1,\ldots,v^k)\in I_k} \mathbf{P}\left\{F(x^1) = b^1, \ldots, F(x^k) = b^k\right\} \to 0. \tag{2.8}$$

Проверка аналогов условий (2.4)–(2.8) в [3] опиралась на следующее утверждение (лемма 1 в [3]).

Лемма 1. *Пусть* $(x^1, \ldots, x^k) \in D_{k,j}$, $b^1, \ldots, b^k \in V^T$ *и выполнено условие* (1.5). *Тогда при всех* $k = 1, 2, \ldots$

$$\mathbf{P}\{Ax^1 = b^1, \ldots, Ax^k = b^k\} \le \left(\frac{1+\Delta}{q}\right)^{jT}, \tag{2.9}$$

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

$$\left(\frac{1-\Delta}{q}\right)^{kT} \le \mathbf{P}\{Ax^1 = b^1, \ldots, Ax^k = b^k\} \le \left(\frac{1+\Delta}{q}\right)^{kT}. \tag{2.10}$$

Мы будем использовать лемму 1а — следствие леммы 1 и независимости случайного отображения S и случайной матрицы A.

Лемма 1а. *Пусть* $F(x) = Ax + S(x)$ (*или* $F(x) = A_1x + A_2f(x) + S(x)$), $(x^1, \ldots, x^k) \in D_{k,j}$, $b^1, \ldots, b^k \in V^T$ *и выполнено условие* (1.5). *Тогда при всех* $k = 1, 2, \ldots$

$$\mathbf{P}\{F(x^1) = b^1, \ldots, F(x^k) = b^k\} \le \left(\frac{1+\Delta}{q}\right)^{jT}, \tag{2.11}$$

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

$$\left(\frac{1-\Delta}{q}\right)^{kT} \le \mathbf{P}\{F(x^1) = b^1, \dots, F(x^k) = b^k\} \le \left(\frac{1+\Delta}{q}\right)^{kT}. \qquad (2.12)$$

Соотношения (2.4)– (2.7) можно доказать, повторяя соответствующие рассуждения работы [3] с заменой Ax на $F(x)$ и используя лемму 1а вместо леммы 1. Эти выкладки мы не приводим.

Проверка же условия (2.8) требует использования нового хода рассуждений и нового условия (см. (1.9)), поскольку из-за наличия слагаемого S в отображении F некоторые леммы, использованные при доказательстве аналога (2.8) в [3], не применимы.

Итак, проверим соотношение (2.8). Введем множества

$$\overline{D}_{k,j} = \{(x^1, \dots, x^k) \in D_{k,j} \colon x^\alpha \ne x^\beta (\alpha \ne \beta)\}. \qquad (2.13)$$

Заметим, что $\overline{D}_{k,1} = \varnothing$, $k = 2, 3, \dots$ Положим $\overline{D}_k = \bigcup_{j=2}^{k-1} \overline{D}_{k,j}$. Тогда

$$I_k \subseteq \{(v^1, \dots, v^k) \colon (x^1, \dots, x^k) \in \overline{D}_k,\ b^1, \dots, b^k \in B\}. \qquad (2.14)$$

Так как $\overline{D}_2 = \overline{D}_{2,1} = \varnothing$, то $I_2 = \varnothing$. При $k \ge 3$, используя (2.14), получаем:

$$\begin{aligned} &\sum_{(v^1,\dots,v^k)\in I_k} \mathbf{P}\left\{F(x^1) = b^1, \dots, F(x^k) = b^k\right\} = \\ &\le \sum_{j=2}^{k-1} \sum_{(x^1,\dots,x^k)\in \overline{D}_{k,j}} \sum_{(b^1,\dots,b^k)\in B^k} \mathbf{P}\left\{F(x^1) = b^1, \dots, F(x^k) = b^k\right\}. \end{aligned} \qquad (2.15)$$

К выражению в правой части (2.15) применим оценку (2.9). Получим

$$\begin{aligned} &\sum_{(v^1,\dots,v^k)\in I_k} \mathbf{P}\left\{F(x^1) = b^1, \dots, F(x^k) = b^k\right\} \le \\ &\le \sum_{j=2}^{k-1} \sum_{(x^1,\dots,x^k)\in \overline{D}_{k,j}} |B|^k \left(\frac{1+\Delta}{q}\right)^{jT} \le \\ &\le \sum_{j=2}^{k-1} \frac{|\overline{D}_{k,j}|}{|D|^j} |B|^{k-j} \sum_{j=2}^{k-1} \left(\frac{(1+\Delta)^T |D||B|}{q^T}\right)^j. \end{aligned} \qquad (2.16)$$

Так как в D нет подобных векторов, то из (2.14) следует равенство

$$\overline{D}_{k,j} = \{(x^1, \ldots, x^k) \in D_{k,j} \colon x^\alpha \neq cx^\beta (c \in K \backslash \{0\}, \alpha \neq \beta)\}. \tag{2.17}$$

В [3] (см. лемму 6 и текст после нее) было показано, что для множества, указанного в правой части (2.17), выполнено неравенство

$$|\overline{D}_{k,j}| \cdot |D|^{-j} \leq q^{k(k-j)} \rho(D). \tag{2.18}$$

Из этой оценки, условий (1.9), (1.10) и $T\Delta \to \infty$ следует, что выражение в правой части цепочки неравенств (2.16) стремится к нулю. Значит, условие (2.8) тоже выполнено. Теорема 1 доказана.

§ 3. Доказательство теоремы 2

Теперь $F(x) = A_1 x + A_2 f(x) + S(x)$, а $\xi(D, F, B)$ — число решений системы (1.11). Как мы уже отмечали, это число совпадает с числом решений системы (1.12).

Обратившись к определению функции $\rho(D)$, нетрудно проверить, что из равенства $|D_f| = |D|$, условий $\rho(D_f) \to 0$ и $|D'_f| = |D|(1 + o(1))$ следует соотношение $\rho(D'_f) \to 0$. Поэтому из теоремы 1 и условий теоремы 2 выводим, что распределение числа решений $\xi(D'_f, Ay + S^*(y), B)$ системы

$$y \in D'_f, \quad Ay + S^*(y) \in B, \tag{3.1}$$

сходится к распределению Пуассона с параметром λ.

Осталось показать, что $\mathbf{P}\{\xi(D'_f, Ay + S^*(y), B) = \xi(D, F, B)\} \to 1$. Учитывая, что по лемме 1а для любых $y \in V^{n+m} \backslash \{0^{n+m}\}$ и $b \in B$ выполнено неравенство $\mathbf{P}\{Ay + S^*(y) = b\} \leq ((1 + \Delta)/q)^T$, а $|D_f| = |D|$, получаем

$$\begin{aligned} &\mathbf{E}\xi(D, F, B) - \mathbf{E}\xi(D'_f, Ay + S^*(y), B) = \\ &= \mathbf{E}\xi(D_f, Ay + S^*(y), B) - \mathbf{E}\xi(D'_f, Ay + S^*(y), B) \leq \\ &\leq q^{-T} |B||D| \left(1 - \frac{|D'_f|}{|D|}\right) (1 + \Delta)^T. \end{aligned} \tag{3.2}$$

Согласно условиям (1.13), (1.14), $T\Delta \to 0$ правая часть в цепочке соотношений (3.2) стремится к нулю. Так как

$$\mathbf{P}\{\xi(D, F, B) \geq \xi(D'_f, Ay + S^*(y), B)\} = 1,$$

то из (3.2) следует, что

$$\mathbf{P}\{\xi(D'_f, Ay + S^*(y), B) \neq \xi(D, F, B)\} \to 0.$$

Теорема 2 доказана.

§ 4. Доказательство теоремы 3

По условию $F(x) = A_1 x + A_2 f(x) + S(x)$. Пусть

$$D' = \{x \in D\colon (x, f(x)) \in D'_f\},$$

а J и J' обозначают множества $D \times B$ и $D' \times B$ соответственно. Тогда

$$\xi(D, F, B) = \sum_{(x,b)\in J} I\{F(x) = b\}, \quad \xi(D', F, B) = \sum_{(x,b)\in J'} I\{F(x) = b\}. \tag{4.1}$$

Доказательство проведем по схеме доказательства теорем 1 и 2 с использованием некоторых вспомогательных результатов из работы [2].

Сначала покажем, что

$$\mathbf{P}\{\xi(D', F, B) = \xi(D, F, B)\} \to 1. \tag{4.2}$$

Введем множества

$$D_{k,j} = \{(x^1, \dots, x^k) \in (D)^k\colon \operatorname{rank}\Big((x^1, f(x^1)), \dots, (x^k, f(x^k))\Big) = j\},$$
$$D'_{k,j} = D_{k,j} \cap \{(x^1, \dots, x^k) \in (D')^k\}.$$

Для величин $|D'_{k,j}|$ выполнены оценки, аналогичные оценкам (2.2):

$$\left|D'_{k,j}\right| \le \left|D_{k,j}\right| \le \sum\nolimits_{s=1}^{j} C_k^s q^{s(k-s)} |D|^s < \sum\nolimits_{s=1}^{j} C_k^s q^{s(k-s)} q^{ns}. \tag{4.3}$$

Положим

$$D'_k = \bigcup\nolimits_{j=1}^{k-1} D'_{k,j}\,.$$

Для $x^1, \dots, x^k \in D$, $k \ge 2$, $\alpha = 1, \dots, k$, введем величины

$$\eta^{\alpha}(x^1,\dots,x^k) = \sum_{i=1}^{n} \eta_i^{\alpha}(x^1,\dots,x^k),$$

где

$$\eta_i^{\alpha}(x^1,\dots,x^k) = \begin{cases} 1, & \text{если } x_i^{\alpha} \ne 0 \text{ и } x_i^{\beta} = 0 \text{ при всех } \beta \in \{1, \dots, k\}\backslash\{\alpha\}, \\ 0 & \text{в противном случае.} \end{cases}$$

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

$$D_{k,j}(l) = \{(x^1, \dots, x^k) \in D_{k,j}\colon \exists s_1, \dots, s_j \in \{1, \dots, k\},\ s_\alpha \ne s_\beta\ (\alpha \ne \beta),$$
$$\eta^s(x^{s_1}, \dots, x^{s_j}) \ge l\ \ \forall s \in \{s_1, \dots, s_j\}\}.$$

Пусть

$$D'_{k,j}(l) = D_{k,j}(l) \cap D'_{k,j}.$$

Положим

$$J'_k = \left\{((x^1, b^1), \ldots, (x^k, b^k)) \in (J')^k \colon (x^\alpha, b^\alpha) \neq (x^\beta, b^\beta)\ (\alpha \neq \beta)\right\}.$$

Сформулируем два вспомогательных утверждения.

Лемма 2. *Пусть* $(x^1, \ldots, x^k) \in D_{k,j}(l)$, $0 \leq l \leq n$, $b^1, \ldots, b^k \in V^T$, *и выполнено условие* (1.5). *Тогда при всех* $k = 1, 2, \ldots$

$$\mathbf{P}\{F(x^1) = b^1, \ldots, F(x^k) = b^k\} \leq \left(\frac{1 + \Delta^l}{q}\right)^{jT}, \tag{4.4}$$

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

$$\left(\frac{1 - \Delta^l}{q}\right)^{kT} \leq \mathbf{P}\{F(x^1) = b^1, \ldots, F(x^k) = b^k\} \leq \left(\frac{1 + \Delta^l}{q}\right)^{kT}. \tag{4.5}$$

Доказательство. Согласно лемме 1 из [2] соотношения (4.4), (4.5) выполнены (при указанных выше условиях и при любых $b^1, \ldots, b^k \in V^T$), если $S(x) \equiv 0^T$ и отображение $F(x)$ задано равенством $F(x) = A_1 x + A_2 f(x)$. В силу независимости отображений $A_1 x + A_2 f(x)$ и $S(x)$ лемма 2 вытекает из леммы 1 работы [2].

Лемма 3. *Существует такая функция* $\varepsilon(n) \to 0$, $n \to \infty$, *что при всех* $j = 1, \ldots, k$ *выполнено неравенство*

$$|D_{k,j} \backslash D_{k,j}(\ln n)| \leq q^{jn} \exp\left\{n\left(\ln\left(1 - \frac{q-1}{q^j}\right) + \varepsilon(n)\right)\right\}. \tag{4.6}$$

Лемма 3 является следствием леммы 2 из [2], в которой оценка (4.6) была доказана для $D = V^n \backslash \{0^n\}$.

Из (4.1) следует, что

$$\mathbf{E}(\xi(D, F, B) - \xi(D', F, B)) = \sum_{(x,b) \in J \backslash J^1} \mathbf{P}\{F(x) = b\}. \tag{4.7}$$

Разобьем сумму в правой части на две суммы:

$$\sum_{(x,b) \in J \backslash J'} \mathbf{P}\{F(x) = b\} = \Sigma_1 + \Sigma_2, \tag{4.8}$$

где

$$\Sigma_1 = \sum_{(x,b)\in J\setminus J',\ \|x\|\geq \ln n} \mathbf{P}\{F(x) = b\},$$
$$\Sigma_2 = \sum_{(x,b)\in J\setminus J',\ \|x\|< \ln n} \mathbf{P}\{F(x) = b\}.$$

Используя оценку (4.5) (где $k = 1$), получаем

$$\begin{aligned}\Sigma_1 &\leq |D\setminus D'||B|\left(\frac{1+\Delta^{\ln n}}{q}\right)^T = \\ &= \left(1-\frac{|D'|}{|D|}\right)\frac{|D||B|}{q^T}\left(1+\Delta^{\ln n}\right)^T.\end{aligned} \tag{4.9}$$

Из условий (1.10), (1.14), неравенств $q^{-n}|D| \geq c > 0$ и $\rho(D_{\hat{f}}) \geq q^{-n}$ (см. (1.7)) следует, что при $n \to \infty$ выполнена оценка

$$T = n(1 + o(1)), \tag{4.10}$$

а из оценки (4.10) и условия $\Delta \to 0$ следует, что

$$T\Delta^{\ln n} \to 0. \tag{4.11}$$

Из (4.9), (1.13), (1.10) и соотношения (4.11) получаем, что $\Sigma_1 = o(1)$.

Вместе с этим, используя теперь оценку (2.10) (где $k = 1$) и соотношения (4.10), $\Delta \to 0$, получаем

$$\begin{aligned}\Sigma_2 &\leq \sum_{0\leq i<\ln n} C_n^i(q-1)^i\cdot|B|\left(\frac{1+\Delta}{q}\right)^T = \\ &= O\left((n(q-1))^{\ln n}|B|\right)\left(\frac{1+\Delta}{q}\right)^T = \\ &= \exp\{-n\ln q + T\ln(1+\Delta) + O(\ln^2 n)\} = \\ &= \exp\{-n\ln q(1+o(1))\} = o(1).\end{aligned}$$

Так как $\mathbf{P}\{\xi(D,F,B) \geq \xi(D',F,B)\} = 1$, то, подставив в (4.8) и (4.7) выведенные соотношения для Σ_1 и Σ_2, получим:

$$\mathbf{P}\{\xi(D',F,B) \neq \xi(D,F,B)\} \leq \mathbf{E}(\xi(D,F,B) - \xi(D',F,B)) \to 0. \tag{4.12}$$

Итак, соотношение (4.2) доказано.

Теперь докажем предельную теорему Пуассона для случайной величины $\xi(D', F, B)$ (см. (4.1)), что и завершит доказательство теоремы 3. Для этого опять воспользуемся теоремой Б. А. Севастьянова. Определим исключительные множества $I'_k \subset J'_k$ равенством

$$I'_k = \left\{((x^1, b^1), \ldots, (x^k, b^k)) \in J'_k \colon (x^1, \ldots, x^k) \in D'_k \cup \left(D'_{k,k} \backslash D'_{k,k}(\ln n)\right)\right\}.$$

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 $j = k$ — те наборы, в которых хотя бы один из векторов $x^1, \ldots, x^k$ имеет относительно мало ненулевых элементов на тех местах, где остальные $k - 1$ векторов имеют нули.

Отметим сразу, что

$$I'_k \subseteq \left\{(x^1, \ldots, x^k) \in D'_k \cup \left(D'_{k,k} \backslash D'_{k,k}(\ln n)\right)\right\} \cap \left\{b^1, \ldots, b^k \in B\right\}, \qquad (4.13)$$

а

$$D'_k \cup \left(D'_{k,k} \backslash D'_{k,k}(\ln n)\right) = D'_k(\ln n) \cup \left(D'_k \backslash D'_k(\ln n)) \cup (D'_{k,k} \backslash D'_{k,k}(\ln n))\right). \quad (4.14)$$

Предельная теорема Пуассона для случайной величины $\xi(D', F, B)$ (см. (4.1)) будет доказана, если убедиться, что выполнены условия (2.4)–(2.8) для рассматриваемых в этом разделе отображения F и множеств I'_k). Приступим к проверке этих условий.

Соотношение (2.4) следует из (1.10) и (4.12), а соотношение (2.5) — из оценки (2.10) и условия $\Delta \to 0$. Соотношение (2.6) вытекает из определения исключительных множеств и неравенств (4.5).

Проверим соотношение (2.7) при $k \geq 2$. Из (4.14) следует равенство

$$\sum_{(v^1, \ldots, v^k) \in I'_k} \prod_{i=1}^{k} \mathbf{P}\left\{F(x^i) = b^i\right\} = S_1 + S_2, \qquad (4.15)$$

где

$$S_1 = \sum_{\substack{(v^1, \ldots, v^k) \in J'_k \\ (x^1, \ldots, x^k) \in D'_k(\ln n)}} \prod_{i=1}^{k} \mathbf{P}\left\{F(x^i) = b^i\right\},$$

$$S_2 = \sum_{\substack{(v^1, \ldots, v^k) \in J'_k \\ (x^1, \ldots, x^k) \in (D'_k \backslash D'_k(\ln n)) \cup (D'_{k,k} \backslash D'_{k,k}(\ln n))}} \prod_{i=1}^{k} \mathbf{P}\left\{F(x^i) = b^i\right\}.$$

Используя условие $q^{-n}|D| \geq c > 0$ и оценки (4.3), (4.4) (при $k = 1$), (4.13), получаем

$$S_1 \leq |B|^k \sum_{j=1}^{k-1} |D'_{k,j}| \left(\frac{1+\Delta^{\ln n}}{q}\right)^{kT} \leq$$

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

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

Поэтому из (1.10), (4.11) и соотношения

$$\frac{1}{q^{nk}} \sum_{j=1}^{k-1} \sum_{s=1}^{j} C_k^s q^{s(n+k-s)} \to 0, \quad n \to \infty,$$

следует, что $S_1 \to 0$.

Аналогичным образом с помощью соотношений $D'_{k,j} \backslash D'_{k,j}(\ln n) \subseteq D_{k,j} \backslash D_{k,j}(\ln n)$, (2.12) (в нем надо положить $k = 1$ и взять $F(x) = A_1 x + A_2 f(x) + S(x)$) и (4.6) получаем оценки

$$S_2 \leq \left(\frac{|D||B|}{q^T}\right)^k (1+\Delta)^{kT} \frac{1}{|D|^k} \sum_{j=1}^{k} |D_{k,j} \backslash D_{k,j}(\ln n)| \leq$$

$$= \frac{1}{(cq^n)^k} \sum_{j=1}^{k} q^{nj} \exp\left\{ n \ln\left(1 - \frac{q-1}{q^j}\right) + kT \ln(1+\Delta) + \varepsilon(n) \right\} = o(1). \tag{4.16}$$

Подставив в (4.15) выведенные соотношения для S_1 и S_2, получим (2.7).

Проверим соотношение (2.8). Опять $k \geq 2$. Введем множества

$$\overline{D}'_{k,j} = \{(x^1, \ldots, x^k) \in D'_{k,j} \colon x^\alpha \neq x^\beta (\alpha \neq \beta)\},$$
$$\overline{D}'_{k,j}(\ln n) = \{(x^1, \ldots, x^k) \in D'_{k,j}(\ln n) \colon x^\alpha \neq x^\beta (\alpha \neq \beta)\}.$$

Заметим, что $\overline{D}'_{k,1} = \varnothing$, $k = 2, 3, \ldots$, и положим

$$\overline{D}'_k = \bigcup_{j=2}^{k-1} \overline{D}'_{k,j}, \quad \overline{D}'_k(\ln n) = \bigcup_{j=2}^{k-1} \overline{D}'_{k,j}(\ln n).$$

Так как $\overline{D}'_2 = \overline{D}'_{2,1} = \varnothing$, то $I'_k = \varnothing$. Далее полагаем $k \geq 3$.

Из (4.14) следует равенство

$$\sum_{(v^1,\ldots,v^k)\in I'_k} \mathbf{P}\left\{F(x^1) = b^1, \ldots, F(x^k) = b^k\right\} = \overline{S}_1 + \overline{S}_2, \tag{4.17}$$

где

$$\overline{S}_1 = \sum_{\substack{(v^1,\ldots,v^k)\in I'_k \\ (x^1,\ldots,x^k)\in \overline{D}'_k(\ln n)}} \mathbf{P}\left\{F(x^1) = b^1, \ldots, F(x^k) = b^k\right\},$$

$$\overline{S}_2 = \sum_{\substack{(v^1,\ldots,v^k)\in I'_k \\ (x^1,\ldots,x^k)\in (\overline{D}'_k \setminus \overline{D}'_k(\ln n))\cup (D'_{k,k}\setminus D'_{k,k}(\ln n))}} \mathbf{P}\left\{F(x^1) = b^1, \ldots, F(x^k) = b^k\right\}.$$

Применим оценки (4.4) (при $l = \ln n$) к сумме $\overline{S}_1$. Получим

$$\begin{aligned}\overline{S}_1 &= \sum_{j=2}^{k-1} \sum_{(x^1,\ldots,x^k)\in \overline{D}'_{k,j}(\ln n)} \sum_{(b^1,\ldots,b^k)\in B^k} \mathbf{P}\left\{F(x^1) = b^1, \ldots, F(x^k) = b^k\right\} \leq \\ &\leq \sum_{j=2}^{k-1} |\overline{D}'_{k,j}||B|^k \left(\frac{1+\Delta^{\ln n}}{q}\right)^{jT} \leq |B|^k \sum_{j=2}^{k-1} \left|D^*_{k,j}\right| \left(\frac{1+\Delta^{\ln n}}{q}\right)^{jT},\end{aligned} \tag{4.18}$$

где мы воспользовались отсутствием подобных векторов в D'_f и вытекающими из этого свойства соотношениями $\overline{D}'_{k,j} \subseteq D^*_{k,j}$,

$$D^*_{k,j} = \left\{(x^1,\ldots,x^k) \in D_{k,j} : (x^\alpha, f(x^\alpha)) \neq (cx^\beta, cf(x^\beta)), c \in K, \alpha \neq \beta\right\}.$$

Применив (2.18) (в данном случае в (2.18) в качестве D рассматривается D_f), получаем $|D^*_{k,j}| \leq q^{k(k-j)}\rho(D_f)|D|^j$. Используя эту оценку, условия теоремы и (4.11), от (4.18) приходим к соотношениям

$$\begin{aligned}\overline{S}_1 &\leq \rho(D_f)|B|^k \sum_{j=2}^{k-1} q^{k(k-j)}|D|^j \left(\frac{1+\Delta^{\ln n}}{q}\right)^{jT} = \\ &= \rho(D_f)|B|^k \sum_{j=2}^{k-1} q^{k(k-j)} \left(\frac{|D|(1+\Delta^{\ln n})^T}{q^T}\right)^j = O(\rho(D_f)|B|^k) \to 0.\end{aligned} \tag{4.19}$$

Аналогичным образом с помощью леммы 1 (см. (2.10)) и соотношений $\overline{D}'_{k,j}\backslash\overline{D}'_{k,j}(\ln n) \subseteq D_{k,j}\backslash D_{k,j}(\ln n)$ получаем

$$\overline{S}_2 \le |B|^k \sum_{j=2}^{k} |D_{k,j}\backslash D_{k,j}(\ln n)| \left(\frac{(1+\Delta)^T}{q^T}\right)^j.$$

Используя оценку $\ln|B| = o(n)$ (она вытекает из (1.7), (1.14) и условия $q^{-n}|D| \ge c > 0$), (4.6) и (4.10), приходим к выводу, что $\overline{S}_2 = o(1)$. Подставив в (4.17) выведенные соотношения для $\overline{S}_1$ и $\overline{S}_2$, получим (2.8).

Таким образом, сходимость распределения случайной величины $\xi(D', F, B)$ к распределению Пуассона с параметром λ доказана. Значит, доказана и теорема 3.

§ 5. Класс включений, содержащий заведомо совместные системы

В этом параграфе рассматривается распределение случайной величины $\xi(D, F, B \mid x^0)$, $x^0 \in V^n$, равной количеству решений системы включений

$$x \in D, \quad F(x) \in F(x^0) + B. \tag{5.1}$$

В случае, когда $D = V^n$ и $B = \{0^T\}$, система включений (5.1) с $F(x) = (F_1(x), \ldots, F_T(x))$ представляет собой заведомо совместную систему уравнений

$$F_j(x) = F_j(x^0), \quad j = 1, \ldots, T,$$

относительно $x \in V^n$.

Заменой переменных $u = x - x^0$ включения (5.1) приводятся к виду (1.1):

$$u \in D - x^0, \quad F^{(x^0)}(u) \in B, \tag{5.2}$$

где $F^{(x^0)}(u) = F(u + x^0) - F(x^0)$. Поэтому между случайными величинами $\xi(D, F, B|x^0)$ и $\xi(D, F, B)$ существует связь, выраженная равенствами

$$\xi(D, F, B|x^0) = \xi(D - x^0, F^{(x^0)}, B). \tag{5.3}$$

При этом $\xi(D, F, B|0^n) = \xi(D, F, B)$, если $F(0^n) = 0^T$.

Далее $F(x) = A_1 x + A_2 f(x) + S(x)$, где A_1 и A_2 — случайные матрицы (над полем K) размеров $T \times n$ и $T \times m$ соответственно, $f(x) = (f_1(x), \ldots, f_m(x))$ — заданное отображение, удовлетворяющее условию

$f(0^n) = 0^m$, а $S(x) = (S_1(x), \ldots, S_T(x))$ — случайное отображение, не зависящее от матриц A_1, A_2. Пусть матрица $A = (A_1, A_2)$ размера $T \times (n+m)$ получена объединением матриц A_1, A_2; далее считается, что $\Delta = \Delta(A)$ удовлетворяет условию (1.5).

Определим отображение $f^{(x^0)}\colon V^n \to V^m$ равенством $f^{(x^0)}(x) = f(x + x^0) - f(x^0)$, $x \in V^n$, и множество

$$(D - x^0)_{f^{(x^0)}} = \{(x, f^{(x^0)}(x)) | x \in D - x^0\} \subseteq V^{n+m}.$$

Заметим, что $|(D - x^0)_{f^{(x^0)}}| = |D|$. Построим множество $(D - x^0)'_{f^{(x^0)}} \subseteq (D - x^0)_{f^{(x^0)}}$ по такому же правилу, по какому для теоремы 2 из множества D_f строилось множество D'_f. Будем предполагать, что вектор $x^0 = x^0(n)$ зависит от параметра n.

Теорема 2а. *Пусть $D \subseteq V^n \backslash \{x^0\}$, $F(x) = A_1 x + A_2 f(x) + S(x)$ и выполнены условия $n, T \to \infty$, $|D| \to \infty$, $T\Delta \to 0$, (1.10),*

$$\frac{|(D - x^0)'_{f^{(x^0)}}|}{|D|} \to 1, \tag{5.4}$$

$$\rho\left((D - x^0)_{f^{(x^0)}}\right) \to 0, \quad \frac{\ln |B|}{\ln \rho\left((D - x^0)_{f^{(x^0)}}\right)} \to 0. \tag{5.5}$$

Тогда распределение случайной величины $\xi(D, F, B | x^0)$ сходится к распределению Пуассона с параметром λ.

Теорема 2а следует из теоремы 2, равенств (5.3) и

$$F^{(x^0)}(x) = F(x + x^0) - F(x^0) = A_1 x + A_2 f^{(x^0)}(x) + S^{(x^0)}(x), \tag{5.6}$$

где $S^{(x^0)}(x) = S(x + x^0) - S(x^0)$.

С помощью равенств (5.3) и (5.6) из теоремы 3 получается теорема 3а.

Теорема 3а. *Пусть $F(x) = A_1 x + A_2 f(x) + S(x)$, $D \subseteq V^n \backslash \{x^0\}$, $q^{-n}|D| \geq c > 0$ и выполнены условия теоремы 2а с заменой условия $T\Delta \to 0$ условием $\Delta \to 0$. Тогда распределение случайной величины $\xi(D, F, B | x^0)$ сходится к распределению Пуассона с параметром λ.*

Сразу приведем условия для множества координатных функций $\{f_1(x), \dots, f_m(x)\}$ отображения f, которые влекут условие $\rho\left((D - x^0)_{f(x^0)}\right) \to$ $\to 0$ теорем 2а и 3а при $D = V^n \backslash \{x^0\}$. Пусть $||z||$ — число ненулевых элементов вектора z. Рассмотрим набор $d^s = (d_1^s, \dots, d_n^s) \in \{0,1\}^n$, $s = 1, \dots, l$, где

$$||d^s|| \geq 2, \quad s = 1, \dots, l, \tag{5.7}$$

$$||(d_1^{s_1} d_1^{s_2}, \dots, d_n^{s_1} d_n^{s_2})|| = 0, \quad 1 \leq s_1 < s_2 \leq l, \tag{5.8}$$

и введем при $l = 2, 3, \dots$ множество функций

$$Q_n(d^1, \dots, d^l) = \bigcup_{s=1}^{l} \{x_1^{d_1^s} \dots x_n^{d_n^s}\}. \tag{5.9}$$

Отметим, что множество $Q_n(d^1, \dots, d^l)$ состоит из мономов $\varphi_s(x) = x_1^{d_1^s} \dots x_n^{d_n^s}$, $s = 1, \dots, l$, содержащих только первые степени переменных. Согласно условию (5.7), степени самих мономов $\varphi_s(x)$ больше единицы, а условие (5.8) означает, что множества существенных переменных мономов из набора $Q_n(d^1, \dots, d^l)$ попарно не пересекаются.

Условия, при которых $\rho\left((D - x^0)_{f(x^0)}\right) \to 0$, дает следующее утверждение, вытекающее непосредственно из оценки (3.10) в [1], полученной там при доказательстве теоремы 2.

Теорема А. *Пусть* $\{f_1(x), \dots, f_m(x)\} \supseteq Q_n(d^1, \dots, d^l)$, $l \leq m$. *Тогда при* $D = V^n \backslash \{x^0\}$ *для всех* $x^0 \in V^n$

$$\rho\left((D - x^0)_{f(x^0)}\right) \leq 4 \prod_{s=1}^{l} \left(1 - q^{-2\|d_s\|}\right).$$

Эта теорема позволяет нам доказать следующее утверждение. Рассмотрим множество функций (см. замечание 1)

$$Q_n^{(2)} = \bigcup_{\substack{d_1, \dots, d_n \in \{0, \dots, q-1\} \\ d_1 + \dots + d_n = 2}} \{x_1^{d_1} \dots x_n^{d_n}\},$$

которое состоит из всех мономов степени 2.

Следствие 1. *Пусть* $\{f_1(x), \dots, f_m(x)\} \supseteq Q_n^{(2)}$, $S(0^n) = 0^T$, *выполнены условия* $n, T \to \infty$, (1.10), $\Delta \to 0$,

$$|B| \le q^{\delta T}, \quad \delta = \delta(n) = o(1). \tag{5.10}$$

Тогда распределение случайной величины $\xi(V^n \backslash \{x^0\}, F, B|x^0)$ (*и в том числе распределение величины* $\xi(V^n \backslash \{0^n\}, F, B)$) *сходится к распределению Пуассона с параметром* λ *равномерно относительно векторов* $x^0 \in V^n$.

Замечание 3. Класс случайных включений $F(x) \in F(x^0) + B$, где $F(x) = A_1 x + A_2 f(x) + S(x)$ и множество $\{f_1(x), \dots, f_m(x)\}$ удовлетворяет условию теоремы А, содержит «заведомо совместные» системы уравнений, в левых частях которых стоят полиномы степеней g_t, где $2 \le g_t \le n(q-1)$, $t = 1, \dots, T$ (см. (1.3)). Предельное распределение числа решений таких систем в случае, когда $K = GF(2)$, исследовалось в работе [7]. Предельная теорема Пуассона доказана в [7] при более слабых, чем у нас, условиях для параметра Δ, но при дополнительных ограничениях на вес $\|x^0\|$ вектора x^0 (не допускаются векторы, имеющие при $n \to \infty$ «малый» вес, в частности, не допускается вектор $x^0 = 0^n$). В связи с этим отметим, что в следствии 1 сходимость к предельному распределению выполняется равномерно относительно всех векторов $x^0 \in V^n$ (и в предположении, что K — произвольное конечное поле). Для числа решений системы уравнений (1.3) эта сходимость равномерна и относительно величин $2 \le g_t \le n(q-1)$, $t = 1, \dots, T$.

Доказательство следствия 1. Проверим, что условия (5.4) и (5.5) теоремы 2а выполнены равномерно по $x^0 \in V^n$. Положим $\varphi_{i,j}(x) = x_i x_j$, где $1 \le i < j \le n$. Тогда

$$\varphi_{i,j}^{(x^0)}(x) = \varphi_{i,j}(x + x^0) - \varphi_{i,j}(x^0) = x_i x_j + x_j^0 x_i + x_i^0 x_j.$$

Пусть $x_i, x_j \in K \backslash \{0\}$ и $k \in K \backslash \{0\}$. При этом условии равенство $\varphi_{i,j}^{(x^0)}(kx) = k\varphi_{i,j}^{(x^0)}(x)$ выполнено только в том случае, когда k — единица поля K. Из условия $\{f_1(x), \dots, f_m(x)\} \supseteq Q_n^{(2)}$ следует, что множество $\{f_1(x), \dots, f_m(x)\}$ содержит все функции $\varphi_{i,j}(x)$, $1 \le i < j \le n$. Значит, $D'_{f(x^0)} \supseteq \{x \in V^n : ||x|| \ge 2\}$ при всех $x^0 \in V^n$. Следовательно, при $n \to \infty$ соотношение (5.4) выполнено равномерно относительно векторов $x^0 \in V^n$.

Проверим соотношения (5.5). Выберем в качестве $Q(d^1, \dots, d^l)$ (см. (5.7)) множество функций $\varphi_s(x) = x_{2s-1} x_{2s}$, $s = 1, \dots, l$, где $l = [n/2]$ —

целая часть числа $n/2$. Для такого множества

$$\prod_{s=1}^{l}\left(1-q^{-2\|d_s\|}\right)=\left(1-q^{-4}\right)^{[n/2]}\to 0$$

при $n\to\infty$, и по теореме А выполнено первое из соотношений (5.5) (равномерно относительно $x^0\in V^n$). Кроме этого, отсюда и из теоремы А получаем, что

$$\left|\ln\left(\rho\left((D-x^0)_{\hat{f}(x^0)}\right)\right)\right|\geq -\ln\left(4\left(1-q^{-4}\right)^{[n/2]}\right)\geq cn \tag{5.11}$$

при некотором $c>0$. В свою очередь из условий (1.10) и (5.10) следует, что

$$\ln|B|=o(T),\quad T=n(1+o(1)). \tag{5.12}$$

Из (5.11) и (5.12) вытекает, что второе соотношение в (5.5) выполнено равномерно относительно векторов $x^0\in V^n$. Таким образом, следствие 1 доказано.

§ 6. Случай $K=GF(2)$

Пусть

$$\overline{Q}_n^{(g)}=\bigcup_{t=2}^{g}\bigcup_{\substack{d_1,\dots,d_n\in\{0,1\}\\ d_1+\dots+d_n=t}}\{x_1^{d_1}\dots x_n^{d_n}\}. \tag{6.1}$$

Для натуральных чисел r и g положим

$$l(r,g)=\sum_{i=1}^{\min(r,g)}C_r^i. \tag{6.2}$$

Далее предполагаем, что числа $r=r(n)$, $g=g(n)$ зависят от параметра n.

Теорема 4. *Пусть* $K=GF(2)$, $F(x)=A_1x+A_2\hat{f}(x)+S(x)$, $D\subseteq V^n\backslash\{0^n\}$, $\{f_1(x),\dots,f_m(x)\}\supseteq\overline{Q}_n^{(g)}$ *и выполнены условия* $n,T\to\infty$, $r,g\to\infty$, $|D|\to\infty$, $\rho(D_{\hat{f}})\to 0$,

$$\frac{\ln|B|}{\ln\rho(D_{\hat{f}})}\to 0, \tag{6.3}$$

$$2^{-T}|D||B|\to\lambda,\quad 0<\lambda<\infty, \tag{6.4}$$

$$\frac{(1+\Delta)^T\,|\{x\in D\colon\|x\|<r\}|}{|D|}\to 0, \tag{6.5}$$

$$T\Delta^{l(r-j,g-j)}\to 0,\quad j=0,1,\dots. \tag{6.6}$$

Тогда распределение случайной величины $\xi(D, F, B)$ сходится к распределению Пуассона с параметром λ.

Следствие 2. *Пусть $K = GF(2)$, $F(x) = A_1 x + A_2 f(x) + S(x)$, $\{f_1(x), \ldots, f_m(x)\} \supseteq \overline{Q}_n^{(g)}$, $\log_2 n \le g \le n$, и выполнены условия $n, T \to \infty$,*

$$2^{n-T}|B| \to \lambda, \quad 0 < \lambda < \infty, \tag{6.7}$$

$$|B| \le 2^{\delta T}, \tag{6.8}$$

$$0 \le \Delta \le \left(2\left(1 - n^{-1}\psi(n)\right)\right)^{1-\delta} - 1, \tag{6.9}$$

где $0 \le \delta = \delta(n) = o(1)$, $0 < \psi(n) = o(n)$ и

$$\frac{\ln^2 n}{\psi(n)} = o(1), \ n \to \infty. \tag{6.10}$$

Тогда распределение случайной величины $\xi(V^n \backslash \{0^n\}, F, B)$ сходится к распределению Пуассона с параметром λ.

Замечание 4. При выполнении условий (6.7), (6.8) и (6.10) следствия 2 правая часть в (6.9) стремится к единице, что означает возможность асимптотического вырождения распределений (1.4) элементов матрицы $A = (A_1, A_2)$.

Немного о доказательстве теоремы 4. Вспомним, что при выводе теоремы 3 для проверки большинства условий теоремы Б. А. Севастьянова мы использовали схему и фрагменты доказательства теоремы 3 работы [2], добавив к ним новую выкладку для проверки условия (2.8). Для теоремы 4 все делается аналогично. Только теперь вместо теоремы 3 из [2] используется теорема 3 из [1]. Проверка же условия (2.8) здесь проводится точно так же, как для теоремы 3. Поэтому мы доказательство теоремы 4 не приводим.

Доказательство следствия 2 сводится к проверке условий $\rho(D_{\hat{f}}) \to 0$, (6.3), (6.5) и (6.6) теоремы 4 в случае, когда $D = V^n \backslash \{0^n\}$. Проверка условий $\rho(D_{\hat{f}}) \to 0$ и (6.3) повторяет проверку (5.5) в доказательстве следствия 1 (см. раздел 4). Проверка условий (6.5) и (6.6) приведена в доказательстве следствия 5 работы [1]. Поэтому эти выкладки мы опускаем.

Авторы благодарны А. М. Зубкову за полезные замечания.

Список литературы

1. *Копытцев В. А., Михайлов В. Г.* О распределении чисел решений случайных включений // Математические вопросы криптографии. — 2011. — Т. 2. Вып. 2. — С. 55–80.
2. *Копытцев В. А., Михайлов В. Г.* Теоремы пуассоновского типа для числа решений случайных включений // Математические вопросы криптографии. — 2010. — Т. 1. Вып. 4. — С. 63–84.
3. *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.
4. *Михайлов В. Г.* О предельной теореме Б. А. Севастьянова для сумм зависимых случайных индикаторов // Обозрение прикладной и промышленной математики. — 2003. — Т. 10. Вып. 3. — С. 571–578.
5. *Колчин В. Ф., Севастьянов Б. А., Чистяков В. П.* Случайные размещения. — М.: Наука, 1976. — 224 с.
6. *Севастьянов Б. А.* Предельный закон Пуассона в схеме сумм зависимых случайных величин // Теория вероятностей и ее применения. — 1972. — Т. 17. Вып. 4. — С. 733–738.
7. *Масол В. И.* Теорема о предельном распределении числа ложных решений системы нелинейных случайных уравнений // Теория вероятностей и ее применения. — 1998. — Т. 43. Вып. 1. — С. 41–56.