Math-Net.Ru

Общероссийский математический портал

В. А. Копытцев, Предельные теоремы о нормальном распределении для числа решений нелинейных включений, *Матем. вопр. криптогр.*, 2020, том 11, выпуск 4, 77–96

DOI: <https://doi.org/10.4213/mvk340>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 52.6.47.48

26 апреля 2023 г., 04:56:45

Предельные теоремы о нормальном распределении для числа решений нелинейных включений

В. А. Копытцев

Академия криптографии Российской Федерации, Москва

Получено 12.II.2020

Аннотация. При заданном множестве B векторного пространства K^T размерности T над полем $K = GF(2)$ изучается распределение числа ξ решений системы включений $A_1x + A_2f(x) \in B$, $x \in K^n \setminus \{0^n\}$, где A_1 и A_2 — случайные матрицы над полем K размерностей $T \times n$ и $T \times m$ с независимыми элементами, а $f(x) = (f_1(x), \dots, f_m(x)) : K^n \rightarrow K^m$ — заданное нелинейное отображение. Указаны условия сходимости распределения случайной величины ξ к стандартному нормальному распределению.

Ключевые слова: случайные включения, число решений, асимптотическая нормальность

Limit theorems on the normal distribution for the number of solutions of nonlinear inclusions

V. A. Kopytcev

Academy of Cryptography of the Russian Federation, Moscow

Abstract. For a given subset B of linear space K^T over the field $K = GF(2)$ we study the distribution of the number ξ of solutions of the system formed by inclusions $A_1x + A_2f(x) \in B$, $x \in K^n \setminus \{0^n\}$, where A_1 and A_2 are random $T \times n$ and $T \times m$ matrices over K with independent elements and $f(x) = (f_1(x), \dots, f_m(x)) : K^n \rightarrow K^m$ is a given nonlinear mapping. Sufficient conditions for the convergence of distribution of ξ to the standard normal distribution are obtained.

Keywords: random inclusions, number of solutions, asymptotic normality

1. Введение и формулировка результата

Изучается распределение числа решений системы включений

$$A_1x + A_2f(x) \in B, \quad x \in K^n \setminus \{0^n\},$$

где:

K^n — линейное пространство размерности n над полем $K = GF(2)$,

B — множество T -мерных векторов над K ,

A_1 и A_2 — случайные матрицы над K размеров $T \times n$ и $T \times m$ соответственно,

$f(x) = (f_1(x), \dots, f_m(x)) : K^n \rightarrow K^m$ — заданное нелинейное отображение.

Здесь и далее полагаем, что x и $f(x)$ — вектор-столбцы и запись вида $(x, f(x))$ понимаем как вектор-столбец $\begin{pmatrix} x \\ f(x) \end{pmatrix}$. Положим

$$F(x) = A_1x + A_2f(x)$$

и обозначим через $\xi = \xi(K^n \setminus \{0^n\}, F, B)$ число решений данной системы включений. Условия сходимости распределения случайной величины $\xi(K^n \setminus \{0^n\}, F, B)$ к распределению Пуассона приведены в теореме 3 и следствии 5 работы [1]. Здесь исследуются условия сходимости распределения этой величины к стандартному нормальному распределению.

Пусть множество координатных функций отображения $f(x)$ состоит из всех мономов со степенями от 2 до целого числа g включительно и определяется формулой

$$\{f_1(x), \dots, f_m(x)\} = \bigcup_{t=2}^g \bigcup_{\substack{d_1, \dots, d_n \in \{0,1\} \\ d_1 + \dots + d_n = t}} \{x_1^{d_1} \dots x_n^{d_n}\}, \quad (1)$$

где $m = \sum_{t=2}^g C_n^t$. Будем полагать, что элементы случайной матрицы $A = (A_1, A_2) = (a_{i,j})$ независимы в совокупности и

$$\mathbf{P}\{a_{i,j} = k\} = \frac{1 + \Delta_{i,j}(k)}{2}, \quad k \in K. \quad (2)$$

Пусть

$$0 \leq \max_{i,j,k} |\Delta_{i,j}(k)| \leq \Delta < 1. \quad (3)$$

Величина Δ является постоянной (не зависит от параметров n, T). Положим

$$\Lambda_{n,T} = (2^n - 1)|B| \cdot 2^{-T}. \quad (4)$$

Теорема 1. Пусть $K = GF(2)$, выполнено условие (1), где $g = g(n) \geq \log_2 n$, и условия (2), (3), $n, T \rightarrow \infty$,

$$\ln |B| = o(n), \quad (5)$$

$$\Lambda_{n,T} \rightarrow \infty, \quad (6)$$

$$\ln \Lambda_{n,T} = o(n). \quad (7)$$

Тогда распределение случайной величины $(\xi(K^n \setminus \{0^n\}, F, B) - \Lambda_{n,T}) / \Lambda_{n,T}^{1/2}$ сходится к нормальному распределению с нулевым средним и дисперсией 1.

В этой теореме рассмотрен общий случай, когда распределения элементов матрицы $A = (A_1, A_2)$ могут быть различными. Пусть теперь все элементы матрицы $A = (A_1, A_2)$ имеют равновероятное распределение.

Теорема 2. Пусть $K = GF(2)$, выполнено условие (1), где $g = g(n) \geq 2$, а также условия $\Delta = \max_{i,j,k} |\Delta_{i,j}(k)| = 0$, $n, T \rightarrow \infty$, (5), (6), (7).

Тогда распределение случайной величины $(\xi(K^n \setminus \{0^n\}, F, B) - \Lambda_{n,T}) / \Lambda_{n,T}^{1/2}$ сходится к нормальному распределению с нулевым средним и дисперсией 1.

Замечание 1. Условие (5) не требует обязательного стремления величины $|B|$ к бесконечности, величина $|B|$ может быть ограниченной и в случае нелинейной системы уравнений принимать значение 1.

2. Доказательства

Доказательство теоремы 1. Положим

$$D = K^n \setminus \{0^n\}. \quad (8)$$

Разобьем множество D на два непересекающихся подмножества:

$$\dot{D} = \{x \in D : \|x\| > \ln n\}, \quad (9)$$

$$\ddot{D} = \{x \in D : \|x\| \leq \ln n\}, \quad (10)$$

где $\|x\|$ — количество ненулевых элементов вектора x . Имеем

$$\xi(D, F, B) = \dot{\xi} + \ddot{\xi}, \quad (11)$$

где $\dot{\xi}$ — число решений системы включений

$$y \in \{(x, f(x)) : x \in \dot{D}\}, \quad Ay \in B;$$

$\ddot{\xi}$ — число решений системы включений

$$y \in \{(x, f(x)) : x \in \ddot{D}\}, \quad Ay \in B.$$

Введем обозначение

$$G(x) = (x, f(x)). \quad (12)$$

Пусть

$$\dot{D}_{k,j} = \{(x^1, \dots, x^k) \in \dot{D}^k : \text{rank}\langle G(x^1), \dots, G(x^k) \rangle = j\}, \quad (13)$$

$$\dot{D}_k = \bigcup_{j=1}^{k-1} \dot{D}_{k,j}. \quad (14)$$

Отметим, что

$$|\dot{D}_{k,j}| \leq \sum_{s=1}^j |\{(x^1, \dots, x^k) \in D^k : \text{rank}\langle x^1, \dots, x^k \rangle = s\}|.$$

Следовательно,

$$|\dot{D}_{k,j}| \leq \sum_{s=1}^j C_k^s 2^{s(k-s)} |D|^s. \quad (15)$$

Далее потребуется следующее утверждение. Пусть

$$L_j(n) = n2^{-j+1} - 1. \quad (16)$$

Лемма 1. Пусть $K = GF(2)$, выполнено условие (1), где $g \geq \log_2 n$, условия (2), (3), $(x^1, \dots, x^k) \in \dot{D}_{k,j}$, $b^1, \dots, b^k \in K^T$. Тогда при всех $k = 1, 2, \dots$

$$\mathbf{P}\{F(x^1) = b^1, \dots, F(x^k) = b^k\} \leq \left(\frac{1 + \Delta_{L_j(n)}}{2} \right)^{jT}, \quad (17)$$

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

$$\left(\frac{1 - \Delta_{L_k(n)}}{2} \right)^{kT} \leq \mathbf{P}\{F(x^1) = b^1, \dots, F(x^k) = b^k\} \leq \left(\frac{1 + \Delta_{L_k(n)}}{2} \right)^{kT}. \quad (18)$$

Лемма 1 следует из леммы 1 в [1], где в качестве показателей степеней величины Δ вместо (16) используются числа

$$l_j(r, g) = \sum_{i=1}^{\min(r-j+1, g-j+1)} C_{r-j+1}^i.$$

Положим $r = g$, тогда $l_j(g, g) = 2^{g-j+1} - 1$. При $g \geq \log_2 n$ имеем:

$$l_j(g, g) \geq 2^{(\log_2 n) - j + 1} - 1 = L_j(n). \quad (19)$$

Используя лемму 1 из [1] и неравенство (19), получаем лемму 1 настоящей работы.

Из леммы 1 при $j = k = 1$ с учетом (16) получаем следствие 1.

Следствие 1. Пусть $K = GF(2)$, выполнено условие (1), где $g \geq \log_2 n$, и условия (2), (3), $x \in \dot{D} = D_{1,1}$, $b \in K^T$. Тогда

$$\left(\frac{1 - \Delta^{n-1}}{2} \right)^T \leq \mathbf{P}\{F(x) = b\} \leq \left(\frac{1 + \Delta^{n-1}}{2} \right)^T. \quad (20)$$

К следствию 1 добавим, что при любых векторах $x \in D = K^n \setminus \{0^n\}$ и $b \in K^T$ справедливы неравенства

$$\left(\frac{1 - \Delta}{2} \right)^T \leq \mathbf{P}\{F(x) = b\} \leq \left(\frac{1 + \Delta}{2} \right)^T. \quad (21)$$

Приведем асимптотические соотношения, которыми будем пользоваться в дальнейшем: из равенства (4) и условий (5), (7) следует, что

$$T = n + \frac{\ln(1 - 2^{-n})}{\ln 2} + \frac{\ln |B|}{\ln 2} - \frac{\ln \Lambda_{n,T}}{\ln 2} = n(1 + o(1)), \quad (22)$$

поэтому при любом заданном j и $n \rightarrow \infty$

$$(1 \pm \Delta^{L_j(n)})^{jT} = \exp \{ \pm jT \Delta^{L_j(n)} (1 + o(1)) \} = 1 + O(n \exp \{n \ln \Delta\}). \quad (23)$$

Воспользуемся разложением $\xi(D, F, B) = \dot{\xi} + \ddot{\xi}$ (см. (11)) и покажем, что для доказательства теоремы 1 достаточно доказать асимптотическую нормальность величины $(\dot{\xi} - \mathbf{E}\dot{\xi})/\sqrt{\mathbf{E}\dot{\xi}}$.

Согласно верхней оценке (21) имеем

$$\mathbf{E}\ddot{\xi} = \sum_{(x,b) \in \dot{D} \times B} \mathbf{P}\{F(x) = b\} \leq |\dot{D}| |B| \left(\frac{1 + \Delta}{2} \right)^T. \quad (24)$$

При этом (здесь пользуемся известным неравенством, см. лемму 2 в [2])

$$\begin{aligned} |\ddot{D}| &= \sum_{k=1}^{\lfloor \ln n \rfloor} C_n^k \leq C_n^{\lfloor \ln n \rfloor} \frac{n - \lfloor \ln n \rfloor}{n - 2\lfloor \ln n \rfloor} \leq n^{\lfloor \ln n \rfloor} \frac{n - \lfloor \ln n \rfloor}{n - 2\lfloor \ln n \rfloor} \\ &= \exp\{\ln^2 n + o(1)\}. \end{aligned} \quad (25)$$

Используя (5), (22), (24), (25), получаем

$$\begin{aligned} \mathbf{E}\ddot{\xi} &\leq \exp\left\{(\ln^2 n)(1 + o(1)) + n \ln \frac{1 + \Delta}{2} + o(n)\right\} \\ &= \exp\left\{n \ln \frac{1 + \Delta}{2}(1 + o(1))\right\} = o(1), \end{aligned} \quad (26)$$

так как $(1 + \Delta)/2 < 1$. Отсюда следует, что

$$\mathbf{P}\{\ddot{\xi} > 0\} = o(1). \quad (27)$$

Положим

$$\hat{\Lambda}_{n,T} = \mathbf{E}\dot{\xi} = \sum_{(x,b) \in \dot{D} \times B} \mathbf{P}\{F(x) = b\}.$$

С учетом (22), (23) получаем

$$\begin{aligned} \Lambda_{n,T} - \hat{\Lambda}_{n,T} &= \left(|\ddot{D}| + |\dot{D}|\right) |B|2^{-T} - |\dot{D}||B|2^{-T} (1 + O(n \exp\{n \ln \Delta\})) \\ &= |\ddot{D}||B|2^{-T} + |\dot{D}||B|2^{-T} \times O(n \exp\{n \ln \Delta\}) \\ &\leq \mathbf{E}\ddot{\xi} + O(n \exp\{n \ln \Delta + \ln \Lambda_{n,T}\}) = o(1) \end{aligned} \quad (28)$$

согласно оценке (26) и условию (7) для $\ln \Lambda_{n,T}$. Вместе с этим

$$\Lambda_{n,T} = \hat{\Lambda}_{n,T}(1 + o(1)). \quad (29)$$

Из (27), (28), (29) следует, что

$$\begin{aligned} \mathbf{P}\left\{\frac{\xi(D, F, B) - \Lambda_{n,T}}{\Lambda_{n,T}^{1/2}} < x\right\} &= \mathbf{P}\left\{\frac{\dot{\xi} - \Lambda_{n,T}}{\Lambda_{n,T}^{1/2}} < x\right\} + \varepsilon_{n,T} \\ &= \mathbf{P}\left\{\frac{\dot{\xi} - \hat{\Lambda}_{n,T}}{\hat{\Lambda}_{n,T}^{1/2}} < x + \varepsilon'_{n,T}\right\} + \varepsilon_{n,T}, \end{aligned} \quad (30)$$

где $\varepsilon_{n,T} = o(1)$ (согласно (27)) и $\varepsilon'_{n,T} = o(1)$ (согласно (28), (29)). Поэтому для доказательства теоремы 1 достаточно доказать асимптотическую нормальность случайной величины $(\dot{\xi} - \hat{\Lambda}_{n,T})/\hat{\Lambda}_{n,T}^{1/2}$.

Воспользуемся следующим утверждением. В нем мы применяем обозначения, не связанные с ранее использованными. Пусть в схеме серий

$$\xi = \eta_1 + \eta_2 + \dots + \eta_n,$$

где случайные величины η_k принимают лишь значения 0, 1 и, вообще говоря, зависимы между собой. Положим

$$J_r = J_r(n) = \{(i_1, \dots, i_r) \in \{1, \dots, n\}^r : i_\alpha \neq i_\beta \ (\alpha \neq \beta)\},$$

$$b_{i_1 \dots i_r} = \mathbf{P}\{\eta_{i_1} = \dots = \eta_{i_r} = 1\},$$

$$\lambda(n) = \sum_{i=1}^n b_i, \quad \lambda^*(n) = \sum_{i=1}^n b_i(1 - b_i).$$

Отметим, что величина $\lambda^*(n)$ равна дисперсии величины $\xi = \eta_1 + \eta_2 + \dots + \eta_n$ в случае, когда слагаемые $\eta_1, \eta_2, \dots, \eta_n$ попарно независимы.

Лемма 2. Пусть при $n \rightarrow \infty$ выполняются условия

$$\lambda^*(n) \rightarrow \infty, \quad \frac{\lambda(n)}{(\lambda^*(n))^{3/2}} \rightarrow 0, \quad (31)$$

и при всех $r = 2, 3, \dots$

$$\Delta_r(n) = \sum_{(i_1, \dots, i_r) \in J_r} (b_{i_1 \dots i_r} - b_{i_1} \dots b_{i_r}) = o(\lambda^{-t}(n)), \quad (32)$$

где t – любое натуральное число. Тогда

$$\lim_{n \rightarrow \infty} \mathbf{P} \left\{ \frac{\xi - \lambda(n)}{\sqrt{\lambda^*(n)}} < x \right\} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-t^2/2} dt. \quad (33)$$

Замечание 2. Заменяем условие (31) более узким условием

$$\lambda(n) \rightarrow \infty, \quad \frac{1}{\lambda(n)} \sum_{j=1}^n b_j^2 = o(1).$$

Тогда $\lambda^*(n) = \lambda(n)(1 + o(1))$, выполняется (31) и в левой части соотношения (33) величину $\lambda^*(n)$ можно заменить величиной $\lambda(n)$.

Доказательство леммы 2. Рассмотрим аппроксимацию распределения величины ξ распределением суммы независимых индикаторов.

Пусть η'_i , $i = 1, \dots, n$, — независимые величины, распределенные так же, как и величины η_i , т. е.

$$\mathbf{P}\{\eta'_i = s\} = \mathbf{P}\{\eta_i = s\}, \quad s = 0, 1,$$

при всех $i = 1, \dots, n$. Положим

$$\xi' = \eta'_1 + \dots + \eta'_n.$$

Используя формулу для бинома степени r , получаем

$$\mathbf{E} \left(\frac{\xi - \lambda(n)}{\sqrt{\lambda^*(n)}} \right)^r - \mathbf{E} \left(\frac{\xi' - \lambda(n)}{\sqrt{\lambda^*(n)}} \right)^r = (\lambda^*(n))^{-r/2} \sum_{u=1}^r \bar{\Delta}_u \cdot C_r^u (-1)^{r-u} (\lambda(n))^{r-u}, \quad (34)$$

где $\bar{\Delta}_u = \mathbf{E}\xi^u - \mathbf{E}(\xi')^u$. При этом (здесь пользуемся известными формулами, см. [5], стр. 19)

$$\mathbf{E}\xi^u = \sum_{j=0}^u \sigma(u, j) \mathbf{E}\xi^{[j]}, \quad \mathbf{E}(\xi')^u = \sum_{j=0}^u \sigma(u, j) \mathbf{E}(\xi')^{[j]},$$

где

$$\mathbf{E}\xi^{[j]} = \mathbf{E}\xi(\xi - 1) \dots (\xi - j + 1) = \sum_{(i_1, \dots, i_j) \in J_j} b_{i_1 \dots i_j},$$

$$\mathbf{E}(\xi')^{[j]} = \mathbf{E}\xi'(\xi' - 1) \dots (\xi' - j + 1) = \sum_{(i_1, \dots, i_j) \in J_j} b_{i_1} \dots b_{i_j},$$

а $\sigma(u, j)$ — числа Стирлинга второго рода:

$$\sigma(u, j) = \frac{1}{j!} \sum_{i=0}^j (-1)^{i+j} C_j^i i^u.$$

Значит,

$$\bar{\Delta}_u = \mathbf{E}\xi^u - \mathbf{E}(\xi')^u = \sum_{j=0}^u \sigma(u, j) \Delta_j(n). \quad (35)$$

Используя (34), (35) и условие (32), получаем, что

$$\mathbf{E} \left(\frac{\xi - \lambda(n)}{\sqrt{\lambda^*(n)}} \right)^r - \mathbf{E} \left(\frac{\xi' - \lambda(n)}{\sqrt{\lambda^*(n)}} \right)^r \rightarrow 0, \quad r = 1, 2, \dots \quad (36)$$

В силу (36) для завершения доказательства леммы 2 достаточно показать, что моменты величины

$$W = \frac{\xi' - \lambda(n)}{\sqrt{\lambda^*(n)}}$$

сходятся к моментам нормального распределения с параметрами $(0, 1)$.

Обозначим $\Psi(t)$ характеристическую функцию распределения случайной величины W . Исследуем асимптотическое поведение семиинвариантов $\chi_k(W)$, $k = 1, 2, \dots$. Эти величины являются коэффициентами в разложениях

$$\ln \Psi(t) = \ln \mathbf{E} \exp \{itW\} = \sum_{k=1}^r \frac{\chi_k(W)}{k!} (it)^k + o(t^r), \quad r = 1, 2, \dots \quad (37)$$

Используя выражение для W , получаем

$$\begin{aligned} \ln \Psi(t) &= \ln \mathbf{E} \exp \left\{ it(\xi' - \lambda(n)) / \sqrt{\lambda^*(n)} \right\} \\ &= -it \frac{\lambda(n)}{\sqrt{\lambda^*(n)}} + \ln \mathbf{E} \exp \left\{ it(\eta'_1 + \eta'_2 + \dots + \eta'_n) / \sqrt{\lambda^*(n)} \right\} \\ &= -it \frac{\lambda(n)}{\sqrt{\lambda^*(n)}} + \sum_{j=1}^n \ln(1 + z_j(n)), \end{aligned} \quad (38)$$

где

$$\begin{aligned} z_j(n) &= b_j \left(\exp \left\{ it / \sqrt{\lambda^*(n)} \right\} - 1 \right) \\ &= b_j \left(\sum_{\nu=1}^r \frac{1}{\nu!} \left\{ it / \sqrt{\lambda^*(n)} \right\}^\nu \right) + o(t^r), \quad r = 1, 2, \dots \end{aligned} \quad (39)$$

Теперь используя в (38) разложения

$$\ln(1 + z) = \sum_{s=1}^r \frac{(-1)^{s-1}}{s} z^s + o(z^r), \quad r = 1, 2, \dots,$$

а также разложения (39), находим (здесь применяем методику, аналогичную использованной в [7] для вывода формул связи моментов и семиинвариантов; см. стр. 399 в [7])

$$\sum_{j=1}^n \ln(1 + z_j(n)) = \sum_{s=1}^r \frac{(-1)^{s-1}}{s} \sum_{j=1}^n b_j^s \left(\sum_{\nu=1}^r \frac{1}{\nu!} \left\{ it / \sqrt{\lambda^*(n)} \right\}^\nu \right)^s + o(t^r). \quad (40)$$

Поэтому, согласно (38), (40), при любом $r \geq 3$ имеем

$$\begin{aligned} \ln \Psi(t) = & -it \frac{\lambda(n)}{\sqrt{\lambda^*(n)}} + \sum_{j=1}^n b_j \cdot \left\{ it / \sqrt{\lambda^*(n)} \right\} \\ & + \sum_{j=1}^n b_j \cdot \left\{ it / \sqrt{\lambda^*(n)} \right\}^2 / 2 - \sum_{j=1}^n b_j^2 \cdot \left\{ it / \sqrt{\lambda^*(n)} \right\}^2 / 2 \\ & + \sum_{k=3}^r \frac{\chi_k(W)}{k!} (it)^k + o(t^r) = -\frac{t^2}{2} + \sum_{k=3}^r \frac{\chi_k(W)}{k!} (it)^k + o(t^r). \end{aligned} \quad (41)$$

Общий вид величин $\chi_k(W)$, $k \geq 3$, следующий:

$$\chi_k(W) = \sum_{s=1}^k a_s^{(k)} (-1)^{s-1} \sum_{j=1}^n b_j^s \cdot (\lambda^*(n))^{-k/2} = O\left(\frac{\lambda(n)}{(\lambda^*(n))^{3/2}}\right), \quad (42)$$

где $a_s^{(k)}$ – положительные числа. При выводе оценки в правой части (42) мы учли, что при всех $s = 1, \dots, k$

$$\sum_{j=1}^n b_j^s \leq \sum_{j=1}^n b_j = \lambda(n).$$

Соотношения (37), (41), (42) означают, что $\chi_1(W) = \mathbf{E}W = 0$, $\chi_2(W) = \mathbf{D}W = 1$ и при $k \geq 3$ семиинварианты $\chi_k(W)$ по условию (31) сходятся к нулю. Поэтому, согласно теореме 1 из [6], моменты величины W сходятся к моментам нормального распределения с параметрами $(0, 1)$. В силу (36) к моментам этого распределения сходятся и моменты величины $(\xi - \lambda(n)) / \sqrt{\lambda^*(n)}$. Лемма 2 доказана. $\square$

Возвращаясь к обозначениям, использованным до леммы 2, положим

$$\dot{J} = \dot{D} \times B$$

и

$$\dot{J}_k = \{(v^1, \dots, v^k) \in \dot{J}^k : v^\alpha \neq v^\beta (\alpha \neq \beta)\}, \quad (43)$$

где $v^i = (x^i, b^i)$, $i = 1, \dots, k$.

Как было отмечено (см. (30) и далее), для доказательства теоремы 1 достаточно доказать асимптотическую нормальность величины $(\dot{\xi} - \hat{\Lambda}_{n,T}) / \hat{\Lambda}_{n,T}^{1/2}$, где $\hat{\Lambda}_{n,T} = \mathbf{E}\dot{\xi}$. Из общей леммы 2 с учетом замечания 2 получаем для этой величины следующее утверждение.

Следствие 2. Пусть при $n, T \rightarrow \infty$ выполняются условия

$$\hat{\Lambda}_{n,T} = \sum_{(x,b) \in \dot{J} = \dot{D} \times B} \mathbf{P} \{F(x) = b\} \rightarrow \infty, \quad (44)$$

$$\frac{1}{\hat{\Lambda}_{n,T}} \sum_{(x,b) \in \dot{J} = \dot{D} \times B} \mathbf{P}^2 \{F(x) = b\} = o(1) \quad (45)$$

и при всех $k = 2, 3, \dots$

$$\Delta_k = \sum_{(v^1, \dots, v^k) \in \dot{J}_k} \left[\mathbf{P} \{F(x^1) = b^1, \dots, F(x^k) = b^k\} - \prod_{i=1}^k \mathbf{P} \{F(x^i) = b^i\} \right] = o(\hat{\Lambda}_{n,T}^{-t}), \quad (46)$$

где t – любое натуральное число. Тогда

$$\lim_{n, T \rightarrow \infty} \mathbf{P} \left\{ \frac{\xi - \hat{\Lambda}_{n,T}}{\sqrt{\hat{\Lambda}_{n,T}}} < x \right\} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-t^2/2} dt.$$

Для завершения доказательства теоремы 1 проверим выполнение условий (44), (45), (46). Условие (44) следует из условия (6) теоремы 1 и соотношения (29). Условие (45) выполняется, так как согласно верхнему неравенству (20)

$$\frac{1}{\hat{\Lambda}_{n,T}} \sum_{(x,b) \in \dot{J} = \dot{D} \times B} \mathbf{P}^2 \{F(x) = b\} \leq \left(\frac{1 + \Delta^{n-1}}{2} \right)^T = O(2^{-T}).$$

Осталось проверить условие (46). Определим (исключительные) множества $\dot{I}_k \subset \dot{J}_k$ равенством

$$\dot{I}_k = \left\{ (v^1, \dots, v^k) \in \dot{J}_k : (x^1, \dots, x^k) \in \dot{D}_k \right\} \quad (47)$$

(см. (14)) и разобьем величину Δ_k (см. (46)) на два слагаемых

$$\Delta_k = \Delta_k^{(1)} + \Delta_k^{(2)}, \quad (48)$$

где в сокращенной записи

$$\Delta_k^{(1)} = \sum_{(v^1, \dots, v^k) \in \dot{J}_k \setminus \dot{I}_k}, \quad \Delta_k^{(2)} = \sum_{(v^1, \dots, v^k) \in \dot{I}_k}.$$

Для величин $\Delta_k^{(1)}$ получаем

$$\Delta_k^{(1)} = \sum_{(v^1, \dots, v^k) \in \dot{J}_k \setminus \dot{I}_k} \prod_{i=1}^k \mathbf{P}\{F(x^i) = b^i\} \times R(v_1, \dots, v_k), \quad (49)$$

где

$$R(v_1, \dots, v_k) = \left(\frac{\mathbf{P}\{F(x^1) = b^1, \dots, F(x^k) = b^k\}}{\mathbf{P}\{F(x^1) = b^1\} \dots \mathbf{P}\{F(x^k) = b^k\}} - 1 \right).$$

Согласно определениям множество $\dot{J}_k \setminus \dot{I}_k$ (см. (43), (47)) образуют наборы $((x^1, b^1), \dots, (x^k, b^k))$, в которых $(x^1, \dots, x^k) \in \dot{D}_{k,k}$ (см. (13)). Из неравенств (18) вытекает, что для них

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

Значит, согласно (23)

$$R(v_1, \dots, v_k) = O(n \exp\{n \ln \Delta\}). \quad (50)$$

При этом

$$\begin{aligned} \sum_{(v^1, \dots, v^k) \in \dot{J}_k \setminus \dot{I}_k} \prod_{i=1}^k \mathbf{P}\{F(x^i) = b^i\} &\leq \left(\sum_{v \in \dot{J}} \mathbf{P}\{F(x) = b\} \right)^k \\ &\leq \Lambda_{n,T}^k (1 + \Delta_{L_1(n)})^{kT} = O(\Lambda_{n,T}^k). \end{aligned} \quad (51)$$

Из (49)–(51) получаем (с учетом равенств $T = n(1 + o(1))$, $\Lambda_{n,T} = \hat{\Lambda}_{n,T}(1 + o(1))$ и условия $\ln \Lambda_{n,T} = o(n)$), что при всех $k = 2, 3, \dots$

$$\Delta_k^{(1)} = O(n \exp\{n \ln \Delta\} \Lambda_{n,T}^k) = o(\hat{\Lambda}^{-t}), \quad (52)$$

где t – любое натуральное число.

Покажем, что аналогичные соотношения выполняются для величин $\Delta_k^{(2)}$ и, следовательно, выполняется условие (46). Имеем

$$|\Delta_k^{(2)}| \leq S_{1,k} + S_{2,k}, \quad (53)$$

где

$$S_{1,k} = \sum_{(v^1, \dots, v^k) \in \dot{I}_k} \prod_{i=1}^k \mathbf{P}\{F(x^i) = b^i\}, \quad (54)$$

$$S_{2,k} = \sum_{(v^1, \dots, v^k) \in \dot{I}_k} \mathbf{P}\{F(x^1) = b^1, \dots, F(x^k) = b^k\}. \quad (55)$$

Для суммы (54) получаем (используя оценку (20))

$$\begin{aligned} S_{1,k} &\leq |B|^k \sum_{j=1}^{k-1} \sum_{(x^1, \dots, x^k) \in \dot{D}_{k,j}} \left(\frac{1 + \Delta^{n-1}}{2} \right)^{kT} \leq |B|^k \sum_{j=1}^{k-1} |\dot{D}_{k,j}| \left(\frac{1 + \Delta^{n-1}}{2} \right)^{kT} \\ &\leq \left(\frac{|D||B|}{2^T} \right)^k (1 + \Delta^{n-1})^{kT} \frac{1}{|D|^k} \sum_{j=1}^{k-1} |\dot{D}_{k,j}|, \end{aligned} \quad (56)$$

где $D = K^n \setminus \{0^n\}$. Отсюда с учетом оценок (15) и соотношений $\Lambda_{n,T}^t = o(2^n)$, при любом $t \geq 0$, которые следуют из условия (7), находим, что при всех $k = 2, 3, \dots$

$$S_{1,k} = O\left(\hat{\Lambda}^k \cdot |D|^{-1}\right) = o(\hat{\Lambda}^{-t}), \quad (57)$$

где t – любое натуральное число.

Осталось оценить сумму (55). Отметим, что согласно определению множеств $\dot{J}_k, \dot{I}_k$ (см. (43), (47)) суммирование в (55) проводится по всем цепочкам $(v^1, \dots, v^k) \in \dot{I}_k$, где $v^\alpha \neq v^\beta$ ($\alpha \neq \beta$) и, следовательно, $x^\alpha \neq x^\beta$ ($\alpha \neq \beta$). Введем множество

$$\dot{D}'_{k,j} = \left\{ (x^1, \dots, x^k) \in \dot{D}_{k,j} : x^\alpha \neq x^\beta \ (\alpha \neq \beta) \right\}. \quad (58)$$

Заметим, что $\dot{D}'_{k,1} = \emptyset$, $k = 2, 3, \dots$. Положим

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

Далее полагаем $k \geq 3$. Имеем

$$S_{2,k} = \sum_{\substack{(v^1, \dots, v^k) \in \dot{J}_k \\ (x^1, \dots, x^k) \in \dot{D}'_k}} \mathbf{P}\{F(x^1) = b^1, \dots, F(x^k) = b^k\}. \quad (59)$$

Рассмотрим произвольный набор $(x^1, \dots, x^k) \in \dot{D}'_k$. Ему соответствует система $L_G(x^1, \dots, x^k)$ уравнений вида

$$\alpha_1 G(x^1) + \dots + \alpha_k G(x^k) = 0^{n+m},$$

состоящая из всех линейных соотношений, которым удовлетворяет набор $G(x^1), \dots, G(x^k)$, где $G(x) = (x, f(x))$. 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 $L_b(x^1, \dots, x^k)$.

Из определений следует: если $(x^1, \dots, x^k) \in \dot{D}'_{k,j}$, $2 \leq j \leq k-1$, то

$$|B(x^1, \dots, x^k)| \leq |B|^j. \quad (60)$$

Используя соотношения (17), (60) получаем

$$\begin{aligned} S_{2,k} &\leq \sum_{j=2}^{k-1} \sum_{(x^1, \dots, x^k) \in \dot{D}'_{k,j}} \sum_{(b^1, \dots, b^k) \in B(x^1, \dots, x^k)} \left(\frac{1 + \Delta^{L_j(n)}}{2} \right)^{jT} \\ &\leq \sum_{j=2}^{k-1} \sum_{(x^1, \dots, x^k) \in \dot{D}'_{k,j}} \left(\frac{1 + \Delta^{L_j(n)}}{2} \right)^{jT} |B(x^1, \dots, x^k)| \\ &= O \left(\sum_{j=2}^{k-1} \frac{|\dot{D}'_{k,j}|}{|D|^j} \left(\frac{|D| |B|}{2^T} \right)^j \right), \end{aligned} \quad (61)$$

где $D = K^n \setminus \{0^n\}$. Оценим величину $|\dot{D}'_{k,j}|$ в (61). Пусть

$$(D)_f = \{(x, f(x)) : x \in D\}.$$

Обозначим через $N(k_1, k_2, k_3, c, (D)_f)$ число решений уравнения $k_1 y^1 + k_2 y^2 + k_3 y^3 = c$ относительно тройки векторов $y^1, y^2, y^3 \in (D)_f$, где $k_1, k_2, k_3 \in K \setminus \{0\}$, $c \in K^{n+m}$ (напомним, что m — размерность вектора $f(x)$). Пусть

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

Лемма 3. Пусть $K = GF(q)$, тогда при $k \geq 3$, $2 \leq j \leq k-1$

$$|\dot{D}'_{k,j}| \leq \rho((D)_f) |D|^j Q_{k,j}(q), \quad (62)$$

где

$$Q_{k,j}(q) = C_k^j \cdot [q^j - j(q-1) - 1]_{k-j}$$

$$u[h]_t = h(h-1) \cdot \dots \cdot h-t+1, [h]_0 = 1.$$

Доказательство. Введем множество

$$H_{k,j} = \{(x^1, \dots, x^k) \in D'_{k,j} : \text{rank}((G(x^1), \dots, G(x^j)) = j\}, \quad (63)$$

где $G(x) = (x, f(x))$. Ясно, что

$$|\{(x^1, \dots, x^k) \in D'_{k,j}\}| \leq C_k^j |H_{k,j}|. \quad (64)$$

Положим $y^i = G(x^i) = (x^i, f(x^i))$, где $x^i \in K^n$, и обозначим через $l_j = l_j(y^1, \dots, y^j)$ произвольную линейную форму своих аргументов $y^1, \dots, y^j$, а через L_j — множество всех форм $a_1 y^1 + \dots + a_j y^j$, имеющих не менее двух ненулевых коэффициентов. Имеем

$$|L_j| = q^j - j(q-1) - 1. \quad (65)$$

Тогда

$$H_{k,j} = \{(x^1, \dots, x^k) \in D'_{k,j} : \exists \text{ попарно разные } l_j^{(j+1)}, \dots, l_j^{(k)} \in L_j : \\ y^s = l_j^{(s)}(y^1, \dots, y^j), s = j+1, \dots, k\}. \quad (66)$$

Пусть

$$(L_j)_{k-j} = \{(l_j^{(j+1)}, \dots, l_j^{(k)}) \in L_j^{k-j} : l_j^{(s)} \not\equiv l_j^{(t)}, \text{ если } s \neq t\}.$$

Для $(l_j^{(j+1)}, \dots, l_j^{(k)}) \in (L_j)_{k-j}$ определим множество

$$H_{k,j}(l_j^{(j+1)}, \dots, l_j^{(k)}) = \{(x^1, \dots, x^k) \in D'_{k,j} : \\ y^s = l_j^{(s)}(y^1, \dots, y^j), s = j+1, \dots, k\}. \quad (67)$$

Тогда

$$|H_{k,j}| \leq \sum_{(l_j^{(j+1)}, \dots, l_j^{(k)}) \in (L_j)_{k-j}} |H_{k,j}(l_j^{(j+1)}, \dots, l_j^{(k)})|. \quad (68)$$

Возьмем произвольный набор $(l_j^{(j+1)}, \dots, l_j^{(k)}) \in (L_j)_{k-j}$ и рассмотрим равенство $y^{j+1} = l_j^{(j+1)}(y^1, \dots, y^j)$ в (67). Линейная форма в правой части этого равенства имеет по крайней мере два ненулевых слагаемых (скажем, содержащие переменные y^{u_1}, y^{u_2}), и представляется как $a_{u_1} y^{u_1} + a_{u_2} y^{u_2} + g^{(j+1)}$, где $a_{u_1}, a_{u_2} \in K \setminus \{0\}$ и остаточный член $g^{(j+1)}$ от переменных y^{u_1}, y^{u_2} не зависит. Поэтому наше равенство принимает вид

$$a_{u_1} y^{u_1} + a_{u_2} y^{u_2} - y^{j+1} = -g^{(j+1)}. \quad (69)$$

Зафиксируем некоторым образом все переменные $y^t, t \in \{1, \dots, j\} \setminus \{u_1, u_2\}$. Имеется не более чем $|D|^{j-2}$ вариантов фиксации этих переменных. Для каждого варианта уравнение (69) имеет не более $\rho(D)|D|^2$ решений (троек $(y^{u_1}, y^{u_2}, y^{j+1})$). Значит, всего имеется не более $\rho(D)|D|^j$ допустимых вариантов наборов $(y^1, \dots, y^{j+1})$. Осталось заметить, что переменные $(y^{j+2}, \dots, y^k)$ определяются переменными $(y^1, \dots, y^j)$ однозначно (при заданном наборе $(l_j^{(j+1)}, \dots, l_j^{(k)}) \in (L_j)_{k-j}$). Следовательно,

$$|H_{k,j}(l_j^{(j+1)}, \dots, l_j^{(k)})| \leq \rho((D)_f)|D|^j. \quad (70)$$

Из этого неравенства, а также неравенства (68), равенств $|(L_j)_{k-j}| = |L_j|_{k-j}$ и (65) получаем

$$|H_{k,j}| \leq |(L_j)_{k-j}| \cdot \rho((D)_f)|D|^j = [q^j - j(q-1) - 1]_{k-j} \cdot \rho((D)_f)|D|^j.$$

Отсюда и из (64) следует (62). Лемма 3 доказана. $\square$

Используя формулы (61), (62), получаем

$$S_{2,k} = O(\rho((D)_f)\Lambda_{n,T}^k). \quad (71)$$

Лемма 4. Пусть $K = GF(2)$, выполнено условие (1), где $g \geq 2, n \geq 2$. Тогда

$$\rho((D)_f) \leq (3 \cdot 2^{-n} - 2^{1-2n}) \left(\frac{2^n}{2^n - 1} \right)^2. \quad (72)$$

Лемма 4 следует из соотношений

$$\rho((D)_f) \leq \rho(\{(x, f(x)) : x \in K^n\}) \left(\frac{2^n}{2^n - 1} \right)^2 = \rho((K^n)_f) \left(\frac{2^n}{2^n - 1} \right)^2$$

и теоремы 6 работы [3], где приведена оценка для величины $\rho((K^n)_f)$.

Используя соотношение (71) и лемму 4, находим, что при всех $k = 2, 3, \dots$

$$S_{2,k} = o\left(\hat{\Lambda}_{n,T}^{-t}\right), \quad (73)$$

где t – любое натуральное число. Из (48), (52), (53), (57), (73) следует (46). Теорема 1 доказана. $\square$

Доказательство теоремы 2. Как и прежде, будем полагать, что $D = K^n \setminus \{0^n\}$ и $G(x) = (x, f(x))$. Пусть

$$D_{k,j} = \{(x^1, \dots, x^k) \in D^k : \text{rank}\langle G(x^1), \dots, G(x^k) \rangle = j\}, \quad (74)$$

$$D_k = \bigcup_{j=1}^{k-1} D_{k,j}. \quad (75)$$

Отметим, что

$$|D_{k,j}| \leq \sum_{s=1}^j \left| \{(x^1, \dots, x^k) \in D^k : \text{rank}\langle x^1, \dots, x^k \rangle = s\} \right|.$$

Следовательно,

$$|D_{k,j}| \leq \sum_{s=1}^j C_k^s 2^{s(k-s)} |D|^s. \quad (76)$$

Лемма 5. Пусть $K = GF(2)$, выполнены условие (1), где $g \geq 2$, условия (2), (3), где $\Delta = 0$, и включения $(x^1, \dots, x^k) \in D_{k,j}$, $b^1, \dots, b^k \in K^T$. Тогда при всех $k = 1, 2, \dots$

$$\mathbf{P}\{F(x^1) = b^1, \dots, F(x^k = b^k)\} \leq \left(\frac{1}{2}\right)^{jT}, \quad (77)$$

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

$$\mathbf{P}\{F(x^1) = b^1, \dots, F(x^k) = b^k\} = \left(\frac{1}{2}\right)^{kT}. \quad (78)$$

Лемма 5 является следствием леммы 1а работы [4] (где для множества (74) использовано обозначение $D_{k,j}^f$).

Введем обозначение

$$J = D \times B$$

и положим

$$J_k = \{(v^1, \dots, v^k) \in J^k : v^\alpha \neq v^\beta (\alpha \neq \beta)\}, \quad (79)$$

где $v^i = (x^i, b^i)$, $i = 1, \dots, k$.

Воспользуемся утверждением, аналогичным следствию 2, также вытекающему из леммы 2 и замечания 2.

Следствие 3. Пусть при $n, T \rightarrow \infty$ выполняются условия

$$\Lambda_{n,T} = \sum_{(x,b) \in J=D \times B} \mathbf{P}\{F(x) = b\} \rightarrow \infty, \quad (80)$$

$$\frac{1}{\Lambda_{n,T}} \sum_{(x,b) \in J=D \times B} \mathbf{P}^2\{F(x) = b\} = o(1), \quad (81)$$

и при всех $k = 2, 3, \dots$

$$\Delta_k = \sum_{(v^1, \dots, v^k) \in J_k} \left[\mathbf{P}\{F(x^1) = b^1, \dots, F(x^k) = b^k\} - \prod_{i=1}^k \mathbf{P}\{F(x^i) = b^i\} \right] = o(\Lambda_{n,T}^{-t}), \quad (82)$$

где t – любое натуральное число. Тогда

$$\lim_{n,T \rightarrow \infty} \mathbf{P} \left\{ \frac{\xi(D, F, B) - \Lambda_{n,T}}{\sqrt{\Lambda_{n,T}}} < x \right\} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-t^2/2} dt.$$

Для завершения доказательства теоремы 2 проверим выполнение условий (80), (81), (82). Условие (80) повторяет условие (6) теорем 1 и 2. Условие (81), очевидно, выполняется, так как

$$\frac{1}{\Lambda_{n,T}} \sum_{(x,b) \in J = D \times B} \mathbf{P}^2 \{F(x) = b\} = 2^{-T}.$$

Осталось проверить условие (82). Определим (исключительные) множества $I_k \subset J_k$ равенством

$$I_k = \{(v^1, \dots, v^k) \in J_k : (x^1, \dots, x^k) \in D_k\}, \quad (83)$$

где множество D_k определяется равенством (75). Разобьем величину Δ_k на два слагаемых

$$\Delta_k = \Delta_k^{(1)} + \Delta_k^{(2)}, \quad (84)$$

где в сокращенной записи

$$\Delta_k^{(1)} = \sum_{(v^1, \dots, v^k) \in J_k \setminus I_k}, \quad \Delta_k^{(2)} = \sum_{(v^1, \dots, v^k) \in I_k}.$$

Для величин $\Delta_k^{(1)}$ получаем

$$\Delta_k^{(1)} = \sum_{\substack{(v^1, \dots, v^k) \\ \in J_k \setminus I_k}} \left[\mathbf{P}\{F(x^1) = b^1, \dots, F(x^k) = b^k\} - \prod_{i=1}^k \mathbf{P}\{F(x^i) = b^i\} \right] = 0, \quad (85)$$

так как $J_k \setminus I_k = \{(v_1, \dots, v_k) \in J_k : (x_1, \dots, x_k) \in D_{k,k}\}$ и согласно лемме 5 (см. (78))

$$\mathbf{P}\{F(x^1) = b^1, \dots, F(x^k) = b^k\} = \prod_{i=1}^k \mathbf{P}\{F(x^i) = b^i\} = 2^{-kT},$$

если $(x_1, \dots, x_k) \in D_{k,k}$.

Оценим величину $\Delta_k^{(2)}$. Имеем

$$|\Delta_k^{(2)}| \leq S_{1,k} + S_{2,k}, \quad (86)$$

где

$$S_{1,k} = \sum_{(v^1, \dots, v^k) \in I_k} \prod_{i=1}^k \mathbf{P}\{F(x^i) = b^i\}, \quad (87)$$

$$S_{2,k} = \sum_{(v^1, \dots, v^k) \in I_k} \mathbf{P}\{F(x^1) = b^1, \dots, F(x^k) = b^k\}. \quad (88)$$

Для величины $S_{1,k}$ справедливы выкладки, аналогичные выкладкам (56):

$$\begin{aligned} S_{1,k} &\leq |B|^k \sum_{j=1}^{k-1} \sum_{(x^1, \dots, x^k) \in D_{k,j}} \left(\frac{1}{2}\right)^{kT} \leq |B|^k \sum_{j=1}^{k-1} |D_{k,j}| \left(\frac{1}{2}\right)^{kT} \\ &\leq \left(\frac{|D||B|}{2^T}\right)^k \frac{1}{|D|^k} \sum_{j=1}^{k-1} |D_{k,j}| = O(\Lambda_{n,T}^k |D|^{-1}). \end{aligned} \quad (89)$$

Отсюда и из условия $\ln \Lambda_{n,T} = o(n)$ (которое эквивалентно условию $\Lambda_{n,T}^t = o(2^n)$ при каждом $t \geq 0$) следует, что при всех $k = 2, 3, \dots$

$$S_{1,k} = o(\Lambda_{n,T}^{-t}), \quad (90)$$

где t – любое натуральное число.

Осталось оценить величину $S_{2,k}$. Для этой величины справедливы выкладки, аналогичные выкладкам (61):

$$\begin{aligned} S_{2,k} &\leq \sum_{j=2}^{k-1} \sum_{(x^1, \dots, x^k) \in D'_{k,j}} \sum_{(b^1, \dots, b^k) \in B(x^1, \dots, x^k)} \left(\frac{1}{2}\right)^{jT} \\ &\leq \sum_{j=2}^{k-1} \sum_{(x^1, \dots, x^k) \in D'_{k,j}} \left(\frac{1}{2}\right)^{jT} |B(x^1, \dots, x^k)| \\ &\leq \sum_{j=2}^{k-1} \frac{|D'_{k,j}|}{|D|^j} \left(\frac{|D||B|}{2^T}\right)^j = \sum_{j=2}^{k-1} \frac{|D'_{k,j}|}{|D|^j} \Lambda_{n,T}^j, \end{aligned} \quad (91)$$

где

$$D'_{k,j} = \{(x^1, \dots, x^k) \in D_{k,j} : x^\alpha \neq x^\beta \ (\alpha \neq \beta)\},$$

и в определении множества $B(x^1, \dots, x^k)$ в отличие от множества $\dot{B}(x^1, \dots, x^k)$ (см. определение $\dot{B}(x^1, \dots, x^k)$ перед формулой (60)) используется множество $D'_k = \bigcup_{j=1}^{k-1} D'_{k,j}$ вместо множества $\dot{D}'_k = \bigcup_{j=1}^{k-1} \dot{D}'_{k,j}$ (см. (58)). Из (62), (91) получаем

$$S_{2,k} = O(\rho((D)_f) \Lambda_{n,T}^k). \quad (92)$$

С учетом (92), (72) и условия $\ln \Lambda_{n,T} = o(n)$ находим, что при всех $k = 2, 3, \dots$

$$S_{2,k} = o(\Lambda_{n,T}^{-t}), \quad (93)$$

где t – любое натуральное число. Теорема 2 доказана. $\square$

Список литературы

- [1] Копытцев В.А., Михайлов В.Г., “О распределении чисел решений случайных включений”, *Математические вопросы криптографии*, **2:2** (2011), 81–107.
- [2] Копытцев В.А., Михайлов В.Г., “Оценки для минимального расстояния случайного линейного кода”, *Дискретная математика*, **27:2** (2015), 45–55.
- [3] Копытцев В.А., Михайлов В.Г., “Явные оценки точности пуассоновской аппроксимации для распределения числа решений случайных включений”, *Математические вопросы криптографии*, **6:1** (2015), 34–57.
- [4] Копытцев В.А., Михайлов В.Г., “Теоремы пуассоновского типа для числа решений случайных включений”, *Математические вопросы криптографии*, **1:4** (2010), 63–84.
- [5] Сачков В.Н., *Вероятностные методы в комбинаторном анализе*, М.: Наука, 1978, 288 с.
- [6] Janson S., “Normal convergence by higher semiinvariants with applications to sums of dependent random variables and random graphs”, *Ann. Probab.*, **16:1** (1988), 305–312.
- [7] Ширяев А.Н., *Вероятность–1*, М.: МЦНМО, 2007.