Math-Net.Ru

Общероссийский математический портал

В. А. Копытцев, О числе решений систем линейных булевых уравнений в множестве векторов, обладающих заданным числом единиц, *Дискрет. матем.*, 2002, том 14, выпуск 4, 87–109

DOI: <https://doi.org/10.4213/dm265>

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: 3.85.73.92

26 апреля 2023 г., 11:20:10

О числе решений систем линейных булевых уравнений в множестве векторов, обладающих заданным числом единиц

© 2002 г. В. А. Копытцев

Исследуется распределение числа решений случайных систем булевых уравнений в множестве векторов, обладающих заданным числом единиц (заданным весом). Как для систем уравнений с независимыми левыми и правыми частями, так и для заведомо совместных систем получены достаточные условия сходимости распределений к закону Пуассона и стандартному нормальному закону.

1. Введение и формулировки результатов

Рассмотрим систему уравнений

$$\begin{aligned} \varepsilon_{t,1}x_1 \oplus \dots \oplus \varepsilon_{t,n}x_n &= a_t, \quad t = 1, \dots, T, \\ \|x\| = \sum_{i=1}^n x_i &= r, \end{aligned} \quad (1)$$

относительно переменных $x_1, \dots, x_n \in GF(2)$. Здесь r — заданное натуральное число, $1 \leq r \leq n-1$, знак $\oplus$ означает сложение в поле $GF(2)$, а знак $\sum$ — сложение в поле действительных чисел. Предполагается, что коэффициенты $\varepsilon_{t,i}$, $i = 1, \dots, n$, $t = 1, \dots, T$ случайны и независимы,

$$\mathbf{P}\{\varepsilon_{t,i} = \varepsilon\} = \frac{1}{2}(1 + (-1)^\varepsilon \Delta_{t,i}), \quad \varepsilon \in \{0, 1\}, \quad 0 \leq |\Delta_{t,i}| < 1.$$

Назовем систему уравнений (1) случайной системой с независимыми частями, если вектор правых частей $a = (a_1, \dots, a_T)$ не зависит от коэффициентов $\varepsilon_{t,i}$, $i = 1, \dots, n$, $t = 1, \dots, T$. Распределение

$$P_T(\alpha) = \mathbf{P}_T(a = \alpha), \quad \alpha \in V_2^T,$$

вектора a может быть произвольным, в том числе сосредоточенным в некотором одном значении $\alpha' \in V_2^T$.

Систему уравнений (1) назовем случайной заведомо совместной системой, если

$$a_t = \varepsilon_{t,1}x_1^0 \oplus \dots \oplus \varepsilon_{t,n}x_n^0, \quad t = 1, \dots, T,$$

при некотором заданном векторе

$$x^0 = (x_1^0, \dots, x_n^0), \quad \sum_{i=1}^n x_i^0 = r.$$

Вектор x^0 назовем истинным решением. Отметим, что данное определение отличается от обычного определения заведомо совместных систем случайных уравнений, которое не содержит ограничений вида

$$\sum_{i=1}^n x_i^0 = r$$

для истинного решения x^0 (см. [1]).

Число решений системы уравнений (1) с независимыми частями определяется значениями случайной матрицы коэффициентов $E = (\varepsilon_{t,i})_{T \times n}$, случайного вектора правых частей $a = (a_1, \dots, a_T)$ и заданным значением параметра r . Число решений заведомо совместной системы (1) определяется значениями случайной матрицы E , заданными значениями истинного решения $x^0 = (x_1^0, \dots, x_n^0)$ и параметра r .

Обозначим $\xi(E, a \mid r)$ число решений системы (1) с независимыми частями и $\eta(E \mid x^0, r)$ число решений заведомо совместной системы (1). В силу того, что значения r и x^0 заданы, $\xi(E, a \mid r)$ является функцией случайных и независимых E и a , а $\eta(E \mid x^0, r)$ — функцией случайной матрицы E . При любых фиксированных значениях вида $E = E', a = a' = E'x^0$ имеют место равенства

$$\xi(E', E'x^0 \mid r) = \eta(E' \mid x^0, r).$$

Положим

$$\Lambda = \binom{n}{r} 2^{-T}, \quad \Delta = \max_{1 \leq t \leq T, 1 \leq i \leq n} |\Delta_{t,i}|. \quad (2)$$

Для обозначений предельных соотношений вида

$$\mathbf{P}\{\xi = k\} \rightarrow \frac{\lambda^k}{k!} e^{-\lambda}, \quad k = 0, 1, 2, \dots, \quad (3)$$

будем использовать запись

$$\xi \rightarrow \Pi(\lambda)$$

и запись

$$\xi \rightarrow N(0, 1)$$

для обозначения сходимости функции распределения случайной величины ξ к стандартной нормальной функции распределения.

Теорема 1. Пусть $n, T \rightarrow \infty, r/n \rightarrow 0, \Delta \rightarrow 0, T\Delta^r \rightarrow 0$ и

$$\Lambda \rightarrow \lambda < \infty. \quad (4)$$

Тогда

$$\xi(E, a \mid r) \rightarrow \Pi(\lambda) \quad (5)$$

равномерно по распределениям вектора a .

Пусть вектор a распределен равномерно, то есть

$$\mathbf{P}_T\{a = \alpha\} = 2^{-T} \quad \forall \alpha \in V_2^T, \quad (6)$$

$n, T \rightarrow \infty$, $(n - r)/n \rightarrow 0$, $\Delta \rightarrow 0$, $T\Delta^{n-r} \rightarrow 0$ и выполняется условие (4).

Тогда

$$\xi(E, a \mid r) \rightarrow \Pi(\lambda).$$

Теорема 2. Пусть $\Delta_{t,i} = \Delta_t$, $i = 1, \dots, n$, и выполняются условия первой части теоремы 1.

Тогда

$$\eta(E \mid x^0, r) - 1 \rightarrow \Pi(\lambda) \quad (7)$$

независимо от значений истинного решения x^0 , $\|x^0\| = r$.

Пусть $\Delta_{t,i} = \Delta_t$, $i = 1, \dots, n$, $n, T \rightarrow \infty$, $(n - r)/n \rightarrow 0$, $\Delta \rightarrow 0$, $T\Delta^{n-r} \rightarrow 0$ и выполняется условие (4).

Тогда выполняется соотношение (7).

Теорема 3. Пусть $n, T \rightarrow \infty$, $r/n \rightarrow 0$, $\Delta \rightarrow 0$, $T\Delta^r \rightarrow 0$,

$$\Lambda \rightarrow \infty, \quad (8)$$

$$\frac{\ln \Lambda}{r \ln(n/r)} \rightarrow 0 \quad (9)$$

и в случае $\Lambda > 0$

$$\frac{\ln \Lambda}{\ln(T\Delta^r)} \rightarrow 0. \quad (10)$$

Тогда

$$(\xi(E, a \mid r) - \Lambda)\Lambda^{-1/2} \rightarrow N(0, 1) \quad (11)$$

равномерно по распределениям вектора a .

Пусть вектор a распределен равномерно и выполняются условия, полученные из условий первой части теоремы после замены параметра r параметром $n - r$.

Тогда

$$(\xi(E, a \mid r) - \Lambda)\Lambda^{-1/2} \rightarrow N(0, 1). \quad (12)$$

Теорема 4. Пусть $\Delta_{t,i} = \Delta_t$, $i = 1, \dots, n$, и выполняются условия первой части теоремы 3.

Тогда

$$(\eta(E \mid x^0, r) - \Lambda)\Lambda^{-1/2} \rightarrow N(0, 1) \quad (13)$$

независимо от значений истинного решения x^0 , $\|x^0\| = r$.

Пусть $\Delta_{t,i} = \Delta_t$, $i = 1, \dots, n$, и выполняются условия, полученные из условий первой части теоремы 3 после замены параметра r параметром $n - r$.

Тогда выполняется соотношение (13).

Замечание 1. Наряду с системой (1) можно рассмотреть системы уравнений

$$\begin{aligned} \varepsilon_{t,1}x_1 \oplus \dots \oplus \varepsilon_{t,n}x_n &= a_t, \quad t = 1, \dots, T, \\ 1 \leq \|x\| \leq r \leq n-1, \end{aligned} \quad (14)$$

и

$$\begin{aligned} \varepsilon_{t,1}x_1 \oplus \dots \oplus \varepsilon_{t,n}x_n &= a_t, \quad t = 1, \dots, T, \\ 1 \leq r \leq \|x\| \leq n-1, \end{aligned} \quad (15)$$

и точно так же, как и для системы (1), определить случайную систему (14) (систему (15)) с независимыми частями и случайную заведомо совместную систему (14) (систему (15)), полагая в последнем случае, что истинное решение $x^0 = (x_1^0, \dots, x_n^0)$ удовлетворяет ограничению $\sum_{i=1}^n x_i^0 = r$. Обозначим $\xi_1(E, a | r)$ и $\xi_2(E, a | r)$, соответственно, числа решений систем с независимыми частями (14) и (15); обозначим $\eta_1(E | x^0, r)$ и $\eta_2(E | x^0, r)$, соответственно, числа решений заведомо совместных систем (14) и (15).

Для введенных величин справедливы утверждения, аналогичные теоремам 1–4 и отличающиеся некоторыми дополнительными условиями. Действительно, пусть выполняются условия первой части теоремы 1. Случай $r = 1$ тривиален, так как влечет равенство

$$\xi_1(E, a | r) = \xi(E, a | r).$$

При $r \geq 2$ и при условии, что $T\Delta = O(1)$, математическое ожидание

$$\begin{aligned} \mathbf{M}(\xi_1(E, a | r) - \xi(E, a | r)) &\leq \left(\frac{1+\Delta}{2}\right)^T \sum_{v=1}^{r-1} \binom{n}{v} \\ &\leq (1+\Delta)^T \Delta \sum_{k \geq 1} \left(\frac{r}{n-r}\right)^k \rightarrow 0. \end{aligned} \quad (16)$$

Поэтому согласно (5) выполняется соотношение

$$\xi_1(E, a | r) \rightarrow \Pi(\lambda)$$

равномерно относительно распределений вектора a .

Аналогично показывается, что в условиях первой части теоремы 2 при $r \geq 2$ и $T\Delta = O(1)$ выполняется соотношение

$$\eta_1(E | x^0, r) \rightarrow \Pi(\lambda)$$

равномерно по значениям истинного решения x^0 . Действительно, пусть $\|x^0\| = r \geq 2$, и пусть x' — произвольный вектор с весом $1 \leq \|x'\| \leq r-1$. Вектор x' удовлетворяет заведомо совместной системе (14), если и только если скалярное произведение

$$\langle \varepsilon_t, x^0 \oplus x' \rangle = 0, \quad t = 1, \dots, T,$$

где

$$\varepsilon = (\varepsilon_{t,1}, \dots, \varepsilon_{t,n}), \quad x^0 \oplus x' = (x_1^0 \oplus x'_1, \dots, x_n^0 \oplus x'_n).$$

При любом значении x^0 , $\|x^0\| = r$,

$$\mathbf{P}\{\langle \varepsilon_t, x^0 \oplus x' \rangle = 0, t = 1, \dots, T\} \leq 2^{-T} (1+\Delta)^T.$$

Отсюда получаем соотношения, аналогичные соотношениям (16),

$$\mathbf{M}(\eta_1(E | x^0, r) - \eta(E | x^0, r)) \leq (1 + \Delta)^t \Delta \sum_{k \geq 1} \left(\frac{r}{n-r} \right)^k \rightarrow 0. \quad (17)$$

Утверждения для величин $\xi_1(E, a | r)$ и $\eta_1(E | x^0, r)$, соответствующие первой части теоремы 3 и первой части теоремы 4, вытекают из оценок (16), (17) при $r \geq 2$ и соотношений

$$T\Delta = O(1), \quad \Delta r/n \rightarrow 0, \quad \Delta \rightarrow \infty.$$

Утверждения для $\xi_2(E, a | r)$, соответствующие вторым частям теорем 1, 3, получаются с помощью следующего утверждения: пусть вектор a распределен равномерно, тогда

$$\mathbf{P}\{\xi(E, a | r) = k\} = \mathbf{P}\{\xi_1(E, a | n-r) = k\}, \quad k = 0, 1, \dots$$

Это утверждение доказывается точно так же, как используемая ниже при доказательстве теорем 1, 3 лемма 9.

Утверждения для $\eta_2(E | x^0, r)$, соответствующие вторым частям теорем 2, 4, получаются с помощью очевидного равенства

$$\eta_2(E | x^0, r) = \eta_1(E | x^1, n-r),$$

где $x^1 = (x_1^0 \oplus 1, \dots, x_n^0 \oplus 1)$.

Замечание 2. Рассмотрим систему уравнений

$$\begin{aligned} \varepsilon_{t,1}x_1 \oplus \dots \oplus \varepsilon_{t,n}x_n &= a_t, & t = 1, \dots, T, \\ \|Lx\| &= r, \end{aligned} \quad (18)$$

где L — невырожденное линейное преобразование пространства V_2^n . Пусть

$$\mathbf{P}\{\varepsilon_{t,i} = 1\} = \mathbf{P}\{\varepsilon_{t,i} = 0\} = 1/2.$$

Тогда посредством замены переменных $y = Lx$ система (18) сводится к системе уравнений вида (1) с независимыми и равномерно распределенными коэффициентами. Поэтому для системы (18) справедливы теоремы 1–4 при $\Delta = 0$.

Рассмотрим теперь случай, когда имеется бесконечная последовательность независимых уравнений

$$\varepsilon_{t,1}x_1 \oplus \dots \oplus \varepsilon_{t,n}x_n = a_t, \quad t = 1, 2, \dots, \quad (19)$$

где при каждом $t = 1, 2, \dots$ правая часть a_t не зависит от независимых между собой коэффициентов $\varepsilon_{t,1}, \dots, \varepsilon_{t,n}$, причем

$$\mathbf{P}\{\varepsilon_{t,i} = 1\} = \mathbf{P}\{\varepsilon_{t,i} = 0\} = \frac{1}{2}.$$

Определим случайную величину $\tau(r)$, положив ее равной максимальному T , при котором система, образованная первыми T уравнениями из последовательности (19), имеет решение x , $\|x\| = r$, где $1 \leq r \leq n-1$.

Пусть теперь в уравнениях (19)

$$a_t = \varepsilon_{t,1}x_1^0 \oplus \dots \oplus \varepsilon_{t,n}x_n^0$$

при некотором векторе

$$x^0 = (x_1^0, \dots, x_n^0), \quad \|x^0\| = r, \quad 1 \leq r \leq n-1.$$

Пусть $\tau^*(r)$ есть максимальное T , при котором система, образованная первыми T уравнениями из последовательности (14), имеет более одного решения x , $\|x\| = r$.

Теорема 5. Пусть $\hat{\tau} = \tau(r)$ или $\hat{\tau} = \tau^*(r)$, $n \rightarrow \infty$, $\min(r, n-r) = o(n)$.

Тогда

$$\limsup_{n \rightarrow \infty} \mathbf{P} \left\{ \hat{\tau} < \frac{1}{\ln 2} \left(\ln \binom{n}{r} + z \right) \right\} \leq \exp(-e^{-z-\ln 2}), \quad (20)$$

$$\liminf_{n \rightarrow \infty} \mathbf{P} \left\{ \hat{\tau} < \frac{1}{\ln 2} \left(\ln \binom{n}{r} + z \right) \right\} \geq \exp(-e^{-z}). \quad (21)$$

Замечание 3. Можно ввести аналогичные величины $\tau_1(r)$, $\tau_2(r)$, соответствующие последовательности уравнений (14) с независимыми частями и ограничениями

$$1 \leq r \leq \|x\| \leq n-1, \quad 1 \leq r \leq \|x\| \leq n-1,$$

а также величины $\tau_1^*(r)$, $\tau_2^*(r)$, соответствующие последовательности заведомо совместных уравнений (14) и вышеуказанным ограничениям. Для каждой величины

$$\hat{\tau} \in \{\tau_1(r), \tau_2(r), \tau_1^*(r), \tau_2^*(r)\}$$

справедливо утверждение, аналогичное теореме 5, которое доказывается точно так же, как теорема 5.

2. Доказательства теорем

Доказательство первой части теоремы 1. Положим

$$\xi = \xi(E, a \mid r), \quad N = \binom{n}{r}, \quad X(r) = \{x: \|x\| = r\}.$$

Занумеруем некоторым образом элементы множества $X(r)$. Пусть

$$X(r) = \{x^s\}_{s=1}^N, \quad x^s = (x_1^s, \dots, x_n^s).$$

Представим ξ в виде суммы индикаторов

$$\xi = \xi_1 + \dots + \xi_N,$$

где

$$\xi_s = I\{x^s \text{ является решением системы}\}, \quad s = 1, \dots, N.$$

Для факториальных моментов $\mathbf{E}(\xi)_l$ величины ξ справедливы равенства

$$\mathbf{E}(\xi)_l = \mathbf{E}\xi(\xi-1)\dots(\xi-l+1) = \sum_{(s(1), \dots, s(l))} b_{s(1)\dots s(l)},$$

где

$$b_{s(1)\dots s(l)} = \mathbf{P}\{\xi_{s(1)} = \xi_{s(2)} = \dots = \xi_{s(l)} = 1\}$$

и суммирование проводится по всем упорядоченным наборам $(s(1), \dots, s(l))$ попарно различных индексов, принадлежащих множеству $\{1, \dots, N\}$. Положим

$$\begin{aligned} M(x^s) &= \{i : x_i^s = 1\} \subseteq \{1, \dots, n\}, \\ M(x^{s(1)}, \dots, x^{s(l)}) &= \bigcup_{j=1}^l M(x^{s(j)}), \\ \mu(x^{s(1)}, \dots, x^{s(l)}) &= |M(x^{s(1)}, \dots, x^{s(l)})|. \end{aligned}$$

Следуя работе [2] (см. также [3, 4]), введем исключительные множества S_l , $l = 2, 3, \dots$. Пусть

$$S_l = \{(s(1), \dots, s(l)) : \mu(x^{s(1)}, \dots, x^{s(l)}) \leqslant rl - r/2\}. \quad (22)$$

Покажем, что при любом фиксированном $l = 2, 3, \dots$

$$\sum_{(s(1), \dots, s(l)) \in S_l} b_{s(1) \dots s(l)} \rightarrow 0, \quad (23)$$

$$\sum_{(s(1), \dots, s(l)) \in S_l} b_{s(1)} b_{s(2)} \dots b_{s(l)} \rightarrow 0 \quad (24)$$

и

$$\max_{(s(1), \dots, s(l)) \notin S_l} \left| \frac{b_{s(1) \dots s(l)}}{b_{s(1)} \dots b_{s(l)}} - 1 \right| \rightarrow 0. \quad (25)$$

Тогда, принимая во внимание соотношения

$$b_s \leqslant 2^{-T} (1 + \Delta^r)^T \rightarrow 0, \quad (26)$$

$$\Lambda(1 - \Delta^r)^T \leqslant \sum_{s=1}^N b_s \leqslant \Lambda(1 + \Delta^r)^T, \quad \sum_{s=1}^N b_s \rightarrow \lambda, \quad (27)$$

воспользуемся теоремой 1 работы [2] и получим (5).

В случае $r = 1$

$$\mu(x^{s(1)}, \dots, x^{s(l)}) = l$$

и, согласно определению (22), $S_l = \emptyset$. При этом в силу независимости величин $\xi_1, \dots, \xi_N$ ($N = n$) выполняется соотношение (25), и с учетом (26), (27) имеет место (5). Поэтому везде ниже будем полагать, что

$$r \geqslant 2. \quad (28)$$

Нам понадобятся некоторые вспомогательные утверждения.

Лемма 1. Пусть $1 \leqslant l \leqslant n$, $\text{rank}(x^{s(1)}, \dots, x^{s(l)}) = m \leqslant l$.

Тогда при любом фиксированном $a = (a_1, \dots, a_T)$

$$b_{s(1) \dots s(l)} \leqslant ((1/2)(1 + \Delta))^T m,$$

при этом в случае $m = l$

$$((1/2)(1 - \Delta))^{Tl} \leqslant b_{s(1) \dots s(l)} \leqslant ((1/2)(1 + \Delta))^{Tl}.$$

Доказательство. Пусть

$$\xi_s^{(t)} = I\{x^s \text{ является решением уравнения с номером } t\},$$

$$b_{s(1)\dots s(l)}^{(t)} = \mathbf{P}\{\xi_{s(1)}^{(t)} = \xi_{s(2)}^{(t)} = \dots = \xi_{s(l)}^{(t)} = 1\}.$$

В силу независимости векторов

$$\varepsilon_t = (\varepsilon_{t,1}, \dots, \varepsilon_{t,n}), \quad t = 1, \dots, T,$$

справедливо равенство

$$b_{s(1)\dots s(l)}^{(t)} = \prod_{i=1}^T b_{s(1)\dots s(l)}^{(i)}.$$

Положим

$$x^{s(j)} = (x_1^{s(j)}, \dots, x_n^{s(j)})$$

и рассмотрим систему уравнений

$$x_1^{s(j)} \varepsilon_{t,1} \oplus \dots \oplus x_n^{s(j)} \varepsilon_{t,n} = a_t, \quad j = 1, \dots, l, \quad (29)$$

относительно переменных $\varepsilon_{t,1}, \dots, \varepsilon_{t,n}$.

Пусть

$$\text{rank}(x^{s(1)}, \dots, x^{s(l)}) = m \leq l < n.$$

При этом без ограничения общности условимся, что первые m векторов столбцов

$$(x_1^{s(1)}, \dots, x_1^{s(l)}), \dots, (x_m^{s(1)}, \dots, x_m^{s(l)})$$

матрицы коэффициентов системы (29) линейно независимы. Введем индикатор

$$I_t(\varepsilon'_{m+1}, \dots, \varepsilon'_n) = I\{\text{система (24) имеет решение, где } \varepsilon_{t,m+1} = \varepsilon'_{m+1}, \dots, \varepsilon_{t,n} = \varepsilon'_n\}.$$

Теперь, учитывая, что

$$b_{s(1)\dots s(l)}^{(t)} = \sum_{\varepsilon'_{m+1}, \dots, \varepsilon'_n \in \{0,1\}} \mathbf{P}\{I_t(\varepsilon'_{m+1}, \dots, \varepsilon'_n) = 1\},$$

$$\mathbf{P}\{I_t(\varepsilon'_{m+1}, \dots, \varepsilon'_n) = 1\} \leq ((1/2)(1 + \Delta))^m \prod_{i=m+1}^n ((1/2)(1 + (-1)^{\varepsilon'_i} \Delta_{t,i}),$$

и в случае $m = l$

$$((1/2)(1 - \Delta))^l \prod_{i=l+1}^n ((1/2)(1 + (-1)^{\varepsilon'_i} \Delta_{t,i}) \leq \mathbf{P}\{I_t(\varepsilon'_{l+1}, \dots, \varepsilon'_n) = 1\}$$

$$\leq ((1/2)(1 + \Delta))^l \prod_{i=l+1}^n ((1/2)(1 + (-1)^{\varepsilon'_i} \Delta_{t,i}),$$

получаем утверждение леммы. Лемма доказана.

Положим

$$\rho(x^{s(1)}, \dots, x^{s(l)}) = rl - \mu(x^{s(1)}, \dots, x^{s(l)}). \quad (30)$$

Обозначим через $A(x^{s(1)}, \dots, x^{s(l)})$ матрицу размера $l \times n$, составленную из строк

$$x^{s(1)}, \dots, x^{s(l)} \in X(r) = \{x^s\}_{s=1}^N.$$

Лемма 2. Пусть

$$x^{s(j_1)} + \dots + x^{s(j_k)} = 0. \quad (31)$$

Тогда

$$\rho(x^{s(j_1)}, \dots, x^{s(j_k)}) \geq \frac{1}{2}rk. \quad (32)$$

Доказательство. Отметим, что матрица $A(x^{s(j_1)}, \dots, x^{s(j_k)})$ содержит rk ненулевых (единичных) элементов, а число ненулевых столбцов в ней равно

$$\mu(x^{s(j_1)}, \dots, x^{s(j_k)}).$$

В силу (31) каждый ненулевой столбец содержит не менее двух единиц. Поэтому

$$2\mu(x^{s(j_1)}, \dots, x^{s(j_k)}) \leq rk.$$

Отсюда, а также из (30) следует (32).

Лемма 3. Пусть

$$x^{s(j_1)}, \dots, x^{s(j_k)} \in \{x^{s(1)}, \dots, x^{s(l)}\} \subseteq X(r). \quad (33)$$

Тогда

$$\rho(x^{s(1)}, \dots, x^{s(l)}) \geq \rho(x^{s(j_1)}, \dots, x^{s(j_k)}). \quad (34)$$

Доказательство. Положим

$$\rho_i(x^{s(1)}, \dots, x^{s(l)}) = \begin{cases} 0, & \text{если } i\text{-й столбец матрицы } A(x^{s(1)}, \dots, x^{s(l)}) \text{ нулевой} \\ & \text{или содержит одну единицу;} \\ \nu - 1, & \text{если } i\text{-й столбец матрицы } A(x^{s(1)}, \dots, x^{s(l)}) \\ & \text{содержит } \nu \geq 2 \text{ единиц.} \end{cases}$$

Нетрудно установить, что

$$\rho(x^{s(1)}, \dots, x^{s(l)}) = \sum_{i=1}^n \rho_i(x^{s(1)}, \dots, x^{s(l)}) \quad (35)$$

и при условии (33)

$$\rho_i(x^{s(1)}, \dots, x^{s(l)}) \geq \rho_i(x^{s(j_1)}, \dots, x^{s(j_k)}), \quad i = 1, \dots, n.$$

Отсюда и из (35) следует (34).

Лемма 4. Пусть

$$r(l-1) - r/2 < \mu(x^{s(1)}, \dots, x^{s(l)}). \quad (36)$$

Тогда

$$\text{rank}(x^{s(1)}, \dots, x^{s(l)}) = l. \quad (37)$$

Доказательство. При $l = 1$ и при $l = 2$ это утверждение очевидно. Пусть $l \geq 3$, выполняется (36) и

$$\text{rank}(x^{s(1)}, \dots, x^{s(l)}) < l.$$

Тогда найдутся такие векторы $x^{s(j_1)}, \dots, x^{s(j_k)} \in \{x^{s(1)}, \dots, x^{s(l)}\}$, $k \geq 3$, что $x^{s(j_1)}, \dots, x^{s(j_k)} = 0$. Поэтому, согласно леммам 2 и 3,

$$\rho(x^{s(1)}, \dots, x^{s(l)}) \geq \rho(x^{s(j_1)}, \dots, x^{s(j_k)}) \geq \frac{1}{2} rk \geq \frac{3}{2} r.$$

Отсюда получаем, что

$$\begin{aligned} \mu(x^{s(1)}, \dots, x^{s(l)}) &= rl - \rho(x^{s(1)}, \dots, x^{s(l)}) \\ &\leq rl - 3r/2 = r(l-1) - r/2. \end{aligned}$$

Последнее неравенство противоречит неравенству (36). Значит, из (36) следует (37).

Лемма 5. Пусть $l \geq 3$, $\text{rank}(x^{s(1)}, \dots, x^{s(l)}) < l$ и при некоторых

$$\varepsilon_1, \dots, \varepsilon_{l-1} \in \{0, 1\}, \quad \sum_{s=1}^{l-1} \varepsilon_s \geq 2,$$

выполняется равенство

$$x^{s(l)} = \varepsilon_1 x^{s(1)} + \dots + \varepsilon_{l-1} x^{s(l-1)}. \quad (38)$$

Тогда

$$\mu(x^{s(1)}, \dots, x^{s(l-1)}) = \mu(x^{s(1)}, \dots, x^{s(l)}), \quad (39)$$

$$\text{rank}(x^{s(1)}, \dots, x^{s(l-1)}) = \text{rank}(x^{s(1)}, \dots, x^{s(l)}). \quad (40)$$

Доказательство. Из (38) вытекает, что столбцы матрицы $A(x^{s(1)}, \dots, x^{s(l)})$, соответствующие ненулевым элементам вектора $x^{s(l)}$, содержат не менее двух единиц. Поэтому вычеркивание строки $x^{s(l)}$ из матрицы $A(x^{s(1)}, \dots, x^{s(l)})$ не изменяет общего числа ненулевых столбцов. Отсюда следует (39). Равенство (40) очевидно.

Лемма 6. Пусть $l \geq 3$ и выполняются неравенства

$$r(m-1) - r/2 < \mu(x^{s(1)}, \dots, x^{s(l)}) \leq rm - r/2, \quad (41)$$

где m — целое число, $2 \leq m \leq l$.

Тогда

$$\text{rank}(x^{s(1)}, \dots, x^{s(l)}) \geq m. \quad (42)$$

Доказательство. В случае $m = l$ это утверждение вытекает из леммы 4, а в случае $m = 2$ оно тривиально. Пусть

$$2 < m < l, \quad \text{rank}(x^{s(1)}, \dots, x^{s(l)}) < m. \quad (43)$$

Тогда применим последовательно $l - m$ раз лемму 5 и установим, что найдутся векторы $x^{s(1)}, \dots, x^{s(m)}$ (без ограничения общности будем полагать, что эти векторы первые) такие, что

$$\begin{aligned} \mu(x^{s(1)}, \dots, x^{s(m)}) &= \mu(x^{s(1)}, \dots, x^{s(l)}), \\ \text{rank}(x^{s(1)}, \dots, x^{s(m)}) &= \text{rank}(x^{s(1)}, \dots, x^{s(l)}). \end{aligned} \quad (44)$$

Из (41), (44) и леммы 4 следует, что

$$\text{rank}(x^{s(1)}, \dots, x^{s(l)}) = m.$$

Это равенство противоречит предположению (43). Значит, из (41) следует (42). Лемма 6 доказана.

Обозначим $W_l(h)$ число упорядоченных наборов $(s(1), \dots, s(l))$ попарно различных индексов таких, что

$$\mu(x^{s(1)}, \dots, x^{s(l)}) = h.$$

Используя лемму 1 и лемму 6 при $l \geq 2$, получаем оценку

$$\begin{aligned} \sum_{(s(1), \dots, s(l)) \in S_l} b_{s(1), \dots, s(l)} &\leq ((1/2)(1 + \Delta))^{2T} \sum_{r+1 \leq h \leq 2r-r/2} W_l(h) \\ &+ \sum_{m=3}^l ((1/2)(1 + \Delta))^{mT} \sum_{r(m-1)-r/2 < 2 < h \leq rm-r/2} W_l(h), \end{aligned} \quad (45)$$

причем в случае $l = 2$ правая часть неравенства (45) содержит только первое слагаемое. Нетрудно установить, что

$$W_l(h) \leq \binom{n}{h} \binom{h}{r}^l. \quad (46)$$

Пусть $\omega = [r/2]$ — целая часть числа $r/2$. Из (45), (46) вытекает, что

$$\sum_{(s(1), \dots, s(l)) \in S_l} b_{s(1), \dots, s(l)} \leq Q_l = (1 + \Delta)^{lT} \sum_{m=2}^l Q_l^{(m)}(\omega), \quad (47)$$

где

$$\begin{aligned} Q_l^{(m)}(\omega) &= r(1/2)^{mT} \binom{n}{rm - \omega} \binom{rm - \omega}{r}^l \\ &= r \Delta^m \binom{n}{r}^{-m} \binom{n}{rm - \omega} \binom{rm - \omega}{r}^l. \end{aligned} \quad (48)$$

Докажем теперь утверждение, которое будет использовано как для доказательства теоремы 1, так и для доказательства теоремы 3.

Лемма 7. Найдется постоянная $C < \infty$ такая, что

$$Q_l^{(m)}(\omega) \leq \Lambda^m \exp\{-\omega \ln(n/r) + rl(\ln l + C)\} \quad (49)$$

при всех n, r, l , $rl/n \leq 1/2$, $2 \leq m \leq l$.

Доказательство. Воспользуемся формулой (см. [5], гл., 5, §2, теорема 4)

$$\binom{s}{k} = \frac{1}{2\pi s p^*(1-p^*)} \exp\{-s(p^* \ln p^* + (1-p^*) \ln(1-p^*)) + \theta(k, s)\}, \quad (50)$$

где

$$p^* = k/s, \quad |\theta(k, s)| < \frac{1}{12k} + \frac{1}{12(s-k)} = \frac{1}{12sp^*(1-p^*)}.$$

Применяя формулу (50) к отдельным множителям из выражения (48), с учетом неравенств

$$2 \leq m \leq l \quad (51)$$

получаем, что

$$\begin{aligned} \binom{rm - \omega}{r}^l &\leq (2\pi r(1 - 1/(2 - \omega/r))) \exp\left\{rl(\ln l + m^*) + \frac{1}{12r(1 - 1/(2 - \omega/r))}\right\} \\ &\leq \exp\{rl(\ln l + m^*) + l\}, \end{aligned}$$

где

$$m^* = \sup_{r, m \geq 2} (-(m - \omega/r) \ln(1 - 1/(m - \omega/r))).$$

Следовательно,

$$\binom{rm - \omega}{r}^l \leq \exp\{rl(\ln l + C_1)\}, \quad (52)$$

где C_1 — положительная постоянная.

Аналогично, пользуясь тем, что при $0 \leq x \leq 1/2$ имеют место неравенства

$$\begin{aligned} -3x/2 &\leq \ln(1-x) \leq -x, \\ \frac{1}{1-x} &\leq 1+2x, \end{aligned}$$

учитывая (46) и полагая, что $rl/n \leq 1/2$, получаем, что

$$\binom{n}{rm - \omega} \leq \exp\{(rm - \omega) \ln(n/r) + rlC_2\}, \quad (53)$$

$$\binom{n}{r}^{-m} \leq \exp\{-rm \ln(n/r) + rlC_3\}, \quad (54)$$

где C_2 и C_3 — положительные постоянные.

Используя теперь равенство (48) и оценки (52), (53), (54), получаем оценку (49).

Лемма 7 доказана.

С учетом (49) получаем, что

$$\begin{aligned} Q_l &= (1 + \Delta)^{lT} \sum_{m=2}^l Q_l^{(m)}([r/2]) \\ &\leq (1 + \Delta)^{lT} \frac{\Delta^l - 1}{\Delta - 1} \exp\{-[r/2]\} \ln(n/r) + rl(\ln l + C), \end{aligned}$$

где правая часть в условиях первой части теоремы 1 стремится к нулю, так как

$$(1 + \Delta)^{lT} \leq \exp\{lT\Delta\}$$

и в силу неравенства

$$\Lambda = \binom{n}{r} 2^{-T} \geq C',$$

где C' — положительная постоянная, имеют место оценки

$$T = O(r \ln(n/r)), \quad T\Delta = o(r \ln(n/r)). \quad (55)$$

Таким образом, принимая во внимание (47), получаем (23). Используя неравенство

$$\sum_{(s(1), \dots, s(l)) \in S_l} b_{s(1)} b_{s(2)} \dots b_{s(l)} \leq Q_l$$

получаем также (24).

Осталось показать, что

$$|b_{s(1) \dots s(l)} / (b_{s(1)} \dots b_{s(l)} - 1)| \rightarrow 0 \quad (56)$$

при условии, что

$$rl - r/2 < \mu(s(1), \dots, s(l)), \quad l \geq 2. \quad (57)$$

Положим

$$\begin{aligned} x^{s(j)} &= (x^{s(j)}_1, \dots, x^{s(j)}_n), \quad \varepsilon = (\varepsilon_1, \dots, \varepsilon_n), \\ \langle x^{s(j)}, \varepsilon \rangle &= \varepsilon_1 x^{s(j)}_1 \oplus \dots \oplus \varepsilon_n x^{s(j)}_n \end{aligned}$$

и обозначим

$$P(x^{s(1)}, \dots, x^{s(l)}; \gamma_1, \dots, \gamma_l)$$

вероятность события

$$\langle x^{s(j)}, \varepsilon \rangle = \gamma_j, \quad j = 1, \dots, l, \quad (58)$$

при случайных и независимых $\varepsilon_1, \dots, \varepsilon_n$ таких, что

$$\mathbf{P}\{\varepsilon_i = \alpha\} = (1 + (-1)^\alpha \Delta_i)/2, \quad |\Delta_i| \leq \Delta < 1, \quad i = 1, \dots, n.$$

Здесь $\gamma_1, \dots, \gamma_l$ — произвольные фиксированные двоичные величины.

Лемма 8. Пусть выполняется условие (57). Тогда при $\Delta \rightarrow 0$

$$P(x^{s(1)}, \dots, x^{s(l)}; \gamma_1, \dots, \gamma_l) = 2^{-l}(1 + O(\Delta^r)) \quad (59)$$

равномерно относительно $\gamma_1, \dots, \gamma_l \in \{0, 1\}$.

Доказательство. Введем в рассмотрение множества

$$\begin{aligned} A_j &= \{i: x_i^{s(j)} = 1\}, & j &\in \{1, \dots, l\}; \\ A_{j_1, \dots, j_k} &= \bigcap_{v=1}^k A_{j_v}, & j_1, \dots, j_k &\in \{1, \dots, l\}; \\ B_{j_1, \dots, j_k} &= \bigcup_{j \in \{1, \dots, l\} \setminus \{j_1, \dots, j_k\}} A_j, & B_{1, \dots, l} &= \emptyset; \\ C_{j_1, \dots, j_k} &= A_{j_1, \dots, j_k} \setminus (A_{j_1, \dots, j_k} \cap B_{j_1, \dots, j_k}). \end{aligned}$$

Нетрудно заметить, что каждое множество A_j , $j \in \{1, \dots, l\}$, представляется суммой попарно не пересекающихся подмножеств:

$$A_j = C_j + \sum_{k=2}^l \sum_{(j_1, \dots, j_k) \in M_j^k} C_{j_1, \dots, j_k}, \quad (60)$$

где M_j^k — множество наборов попарно различных индексов из $\{1, \dots, l\}$ объема $k \leq l$, содержащих фиксированный индекс $j = \{1, \dots, l\}$. Пусть

$$\sigma(j) = \sum_{k=2}^l \sum_{(j_1, \dots, j_k) \in M_j^k} C_{j_1, \dots, j_k}. \quad (61)$$

Учитывая (60) и (61), находим, что

$$A_j = C_j + \sigma(j). \quad (62)$$

Сопоставим множествам $C_{j_1, \dots, j_k}$ двоичные переменные $\alpha_{j_1, \dots, j_k}$ и положим

$$\sigma^*(j) = \sum_{k=2}^l \sum_{(j_1, \dots, j_k) \in M_j^k} \alpha_{j_1, \dots, j_k}, \quad (63)$$

где суммирование проводится в $GF(2)$. Пусть

$$\begin{aligned} x^j &= (x_1^j, \dots, x_n^j), & x_i^j &= \begin{cases} 1, & i \in C_j, \\ 0, & i \notin C_j, \end{cases} \\ x^{j_1, \dots, j_k} &= (x_1^{j_1, \dots, j_k}, \dots, x_n^{j_1, \dots, j_k}), & x_i^{j_1, \dots, j_k} &= \begin{cases} 1, & i \in C_{j_1, \dots, j_k}, \\ 0, & i \notin C_{j_1, \dots, j_k}, \end{cases} \end{aligned}$$

и для любых подмножеств $D, D_1, \dots, D_v \subseteq \{1, \dots, n\}$

$$\Delta(D) = \begin{cases} \prod_{i \in D} \Delta_i, & D \neq \emptyset, \\ 1, & D = \emptyset, \end{cases}$$

$$\Delta(D_1, \dots, D_v) = \Delta(D_1) \dots \Delta(D_v).$$

Представим событие (58) суммой попарно несовместных событий

$$\prod_{k=2}^l \prod_{1 \leq j_1 < \dots < j_k \leq l} \{\langle x^{j_1, \dots, j_k}, \varepsilon \rangle = \alpha_{j_1, \dots, j_k}\} \prod_{j=1}^l \{\langle x^j, \varepsilon \rangle = \gamma_j \oplus \sigma^*(j)\},$$

взятых для всех значений наборов переменных

$$\alpha_{j_1, \dots, j_k}, \quad 1 \leq j_1 < \dots < j_k \leq l, \quad k = 2, \dots, l.$$

Используя вышеуказанное представление, с учетом равенств

$$\begin{aligned} \mathbf{P}\{\langle x^{j_1, \dots, j_k}, \varepsilon \rangle = \alpha_{j_1, \dots, j_k}\} &= \frac{1}{2} (1 + (-1)^{\alpha_{j_1, \dots, j_k}} \Delta(C_{j_1, \dots, j_k})), \\ \mathbf{P}\{\langle x^j, \varepsilon \rangle = \gamma_j \oplus \sigma^*(j)\} &= \frac{1}{2} (1 + (-1)^{\gamma_j \oplus \sigma^*(j)} \Delta(C_j)) \end{aligned}$$

получаем, что

$$\begin{aligned} &P(x^{s(1)}, \dots, x^{s(l)}; \gamma_1, \dots, \gamma_l) \\ &= \sum_{\alpha_{j_1 j_2} \in \{0,1\}} \dots \sum_{\alpha_{j_1 \dots j_k} \in \{0,1\}} \dots \sum_{\alpha_{1 \dots l} \in \{0,1\}} \prod_{k=2}^l \prod_{1 \leq j_1 < \dots < j_k \leq l} \frac{1}{2} (1 + (-1)^{\alpha_{j_1 \dots j_k}} \\ &\quad \times \Delta(C_{j_1, \dots, j_k})) \prod_{j=1}^l (1/2) (1 + (-1)^{\gamma_j \oplus \sigma^*(j)} \Delta(C_j)), \quad (64) \end{aligned}$$

где в суммах $\sum_{\alpha_{j_1 \dots j_k} \in \{0,1\}}$, $k = 2, \dots, l$, суммирование проводится по всем значениям наборов переменных $\alpha_{j_1 \dots j_k}$, $1 \leq j_1 < \dots < j_k \leq l$. Раскрывая (64), находим, что

$$\begin{aligned} &2^l P(x^{s(1)}, \dots, x^{s(l)}; \gamma_1, \dots, \gamma_l) \\ &= \sum_{\alpha_{j_1 j_2} \in \{0,1\}} \dots \sum_{\alpha_{j_1 \dots j_k} \in \{0,1\}} \dots \sum_{\alpha_{1 \dots l} \in \{0,1\}} \prod_{k=2}^l \prod_{1 \leq j_1 < \dots < j_k \leq l} \frac{1}{2} (1 + (-1)^{\alpha_{j_1 \dots j_k}} \\ &\quad \times \Delta(C_{j_1, \dots, j_k})) \left(1 + (-1)^{\gamma_j \oplus \sigma^*(j)} \Delta(C_j) \right. \\ &\quad \left. + \sum_{k=2}^l \sum_{1 \leq j_1 < \dots < j_k \leq l} (-1)^{\gamma_{j_1} \oplus \dots \oplus \gamma_{j_k} \oplus \sigma^*(j_1) \oplus \dots \oplus \sigma^*(j_k)} \Delta(C_{j_1}, \dots, C_{j_k}) \right) \\ &= 1 + \sum_{j=1}^l (-1)^{\gamma_j} \Delta(C_j, \sigma(j)) \\ &\quad + \sum_{k=2}^l \sum_{1 \leq j_1 < \dots < j_k \leq l} (-1)^{\gamma_{j_1} \oplus \dots \oplus \gamma_{j_k}} \Delta(C_{j_1}, \dots, C_{j_k}, \sigma(j_1), \dots, \sigma(j_k)) \quad (65) \end{aligned}$$

и множества $\sigma(j_1, \dots, j_k)$, $|\sigma(j_1, \dots, j_k)| \geq 0$, в формуле (65) получаются с помощью следующих действий:

- (1) суммированием в $GF(2)$ выражений (63) для $\sigma^*(j_1), \dots, \sigma^*(j_k)$,
- (2) заменой символа α символом C в обозначениях всех оставшихся после суммирования двоичных переменных,
- (3) заменой операций суммирования в $GF(2)$ операциями суммирования (объединения) множеств.

В случае

$$\sigma^*(j_1) \oplus \dots \oplus \sigma^*(j_k) = 0$$

полагаем

$$\sigma(j_1, \dots, j_k) = \emptyset.$$

Например, пусть $l = 3$, тогда

$$\sigma^*(1) \oplus \sigma^*(2) = \alpha_{1,3} \oplus \alpha_{2,3},$$

так как

$$\sigma^*(1) = \alpha_{1,2} \oplus \alpha_{1,3}, \quad \sigma^*(2) = \alpha_{1,2} \oplus \alpha_{2,3},$$

поэтому $\sigma(1, 2) = C_{1,3} + C_{2,3}$;

пусть $l = 2$, тогда

$$\sigma^*(1) \oplus \sigma^*(2) = 0,$$

так как

$$\sigma^*(1) = \sigma^*(2) = \alpha_{1,2},$$

следовательно, $\sigma(1, 2) = \emptyset$.

Поскольку

$$|\Delta(C_j, \sigma(j))| = |\Delta(A_j)| \leq \Delta^r, \quad j = 1, \dots, l,$$

в силу формулы (65) лемма будет доказана, если мы покажем, что при условии (57) имеют место неравенства

$$|C_j| > r/2, \quad j = 1, \dots, l,$$

из которых следует, что

$$|\Delta(C_{j_1}, \dots, C_{j_k}, \sigma(j_1, \dots, j_k))| \leq |\Delta(C_{j_1}, \dots, C_{j_k})| \leq \Delta^r, \quad k \leq 2.$$

Сначала отметим, что согласно равенствам

$$rl = \sum_{j=1}^l |C_j| + \sum_{k=2}^l k \sum_{1 \leq j_1 < \dots < j_k \leq l} |C_{j_1 \dots j_k}|,$$

$$\mu(s(1), \dots, s(l)) = \sum_{j=1}^l |C_j| + \sum_{k=2}^l \sum_{1 \leq j_1 < \dots < j_k \leq l} |C_{j_1 \dots j_k}|,$$

условие (57) принимает вид

$$rl - \mu(s(1), \dots, s(l)) = \sum_{k=2}^l (k-l) \sum_{1 \leq j_1 < \dots < j_k \leq l} |C_{j_1 \dots j_k}| < r/2. \quad (66)$$

Пусть существует $j \in \{1, \dots, l\}$ такое, что $|C_j| \leq r/2$. Тогда в силу (62)

$$|\sigma(j)| \geq r/2,$$

что противоречит условию (66) ((57)), так как согласно (61)

$$\sum_{k=2}^l (k-1) \sum_{1 \leq j_1 < \dots < j_k \leq l} |C_{j_1, \dots, j_k}| \geq |\sigma(j)|$$

для всех $j \in \{1, \dots, l\}$.

Лемма 8 доказана.

Из леммы 8 следует, что при условии (57) имеет место соотношение

$$b_{s(1) \dots s(l)} = (1/2)^{Tl} (1 + O(\Delta^r))^T \quad (67)$$

равномерно по распределениям вектора правых частей a . Вместе с этим

$$((1/2)(1 - \Delta^r))^{Tl} \leq b_{s(1)} \dots b_{s(l)} \leq ((1/2)(1 + \Delta^r))^{Tl}. \quad (68)$$

Из (67), (68) следует (56). Соотношение (5) доказано.

Доказательство второй части теоремы 1. Вначале докажем следующую лемму.

Лемма 9. Пусть выполняются равенства (6) (вектор a распределен равномерно). Тогда

$$\mathbf{P}\{\xi(E, a \mid r) = k\} = \mathbf{P}\{\xi(E, a \mid n - r) = k\}, \quad k = 0, 1, \dots \quad (69)$$

Доказательство. Пусть некоторая реализация (E', a') системы $Ex = a$ имеет решение

$$x' = (x'_1, \dots, x'_n), \quad \|x'\| = r.$$

Тогда, как нетрудно заметить, реализация $(E', a' \oplus \varepsilon')$, где

$$a' \oplus \varepsilon' = (a'_1 \oplus \varepsilon'_1, \dots, a'_T \oplus \varepsilon'_T), \quad \varepsilon'_i = \varepsilon'_{i,1} \oplus \dots \oplus \varepsilon'_{i,n},$$

имеет решение

$$x'' = (x'_1 \oplus 1, \dots, x'_n \oplus 1), \quad \|x''\| = n - r. \quad (70)$$

Отсюда вытекает, что

$$\xi(E', a' \mid r) = \xi(E', a' \oplus \varepsilon' \mid n - r). \quad (71)$$

Согласно (6) при любой реализации (E', a')

$$\mathbf{P}\{(E, a) = (E', a')\} = \mathbf{P}\{(E, a) = (E', a' \oplus \varepsilon')\}. \quad (72)$$

Используя равенства (71), (72), получаем, что

$$\begin{aligned} \mathbf{P}\{\xi(E, a \mid r) = k\} &= \sum_{E', a': \xi(E', a' \mid r) = k} \mathbf{P}\{(E, a) = (E', a')\} \\ &= \sum_{E', a': \xi(E', a' \oplus \varepsilon' \mid n - r) = k} \mathbf{P}\{(E, a) = (E', a' \oplus \varepsilon')\} \\ &= \sum_{E', a'': \xi(E', a'' \mid n - r) = k} \mathbf{P}\{(E, a) = (E', a'')\} \\ &= \mathbf{P}\{\xi(E, a \mid n - r) = k\}, \quad k = 0, 1, \dots \end{aligned}$$

Лемма доказана.

Используя теперь (69) и (5), получаем вторую часть теоремы 1. Теорема 1 доказана.

Доказательство теоремы 2. Вначале докажем следующую лемму.

Лемма 10. Пусть $\Delta_{t,i} = \Delta_t$, $i = 1, \dots, n$. Тогда распределение величины $\eta(E \mid x^0, r)$ инвариантно относительно значений истинного решения $x^0 \in X(r)$.

Доказательство. Пусть x', x'' — произвольные векторы из множества $X(r)$. Очевидно, что существует такая подстановочная $n \times n$ матрица π , что $x'' = \pi x'$. Легко проверяется равенство

$$\eta(E \mid x', r) = \eta(E\pi^{-1} \mid x'', r). \quad (73)$$

Используя (73) и равенство

$$\mathbf{P}\{E = E'\} = \mathbf{P}\{E = E'\pi^{-1}\},$$

получаем, что

$$\begin{aligned} \mathbf{P}\{\eta(E \mid x', r) = k\} &= \sum_{E': \eta(E' \mid x', r) = k} \mathbf{P}\{E = E'\} \\ &= \sum_{E': \eta(E'\pi^{-1} \mid x'', r) = k} \mathbf{P}\{E = E'\pi^{-1}\} \\ &= \sum_{e'': \eta(E'' \mid x'', r) = k} \mathbf{P}\{E = E''\} = \mathbf{P}\{\eta(E \mid x'', r) = k\}. \end{aligned}$$

Лемма доказана.

Следующее утверждение аналогично теореме 4.1 из [1], которая доказана при отсутствии каких-либо ограничений на вес векторов решений.

Лемма 11. Пусть $\Delta_{t,i} = \Delta_t$, $i = 1, \dots, n$, и для системы с независимыми частями (1) выполняется равенство (6) (вектор a распределен равномерно).

Тогда

$$\mathbf{P}\{\xi(E, a \mid r) = k\} = \frac{1}{k} \mathbf{E}\xi(E, a \mid r) \mathbf{P}\{\eta(E \mid x^0, r) = k\}, \quad k = 1, 2, \dots, \quad (74)$$

при любом значении истинного решения x^0 .

Доказательство. Пусть

$$\xi = \xi(E, a \mid r), \quad \eta = \eta(E \mid x^0, r).$$

Представим ξ суммой индикаторов:

$$\xi = \xi_1 + \dots + \xi_N, \quad N = \binom{n}{r}. \quad (75)$$

Справедливы равенства

$$(\xi)_l = (\xi_1 + \dots + \xi_N)(\xi - 1)_{l-1}, \quad l \leq 1.$$

Отсюда,

$$\mathbf{E}(\xi)_l = \sum_{s=1}^N \mathbf{P}\{\xi_s = 1\} \mathbf{E}((\xi - 1)_{l-1} \mid \xi_s = 1), \quad l \geq 1. \quad (76)$$

Пусть выполняются равенства (6). Тогда

$$\begin{aligned} \mathbf{P}\{\xi = k \mid \xi_s = 1\} &= \mathbf{P}\{\xi = k, \xi_s = 1\} / \mathbf{P}\{\xi_s = 1\} \\ &= \mathbf{P}\{\eta(E \mid x^s, r) = k\} 2^{-T} / \mathbf{P}\{\xi_s = 1\} \\ &= \mathbf{P}\{\eta(E \mid x^s, r) = k\}, \end{aligned}$$

так как

$$\begin{aligned} \mathbf{P}\{\xi = k, \xi_s = 1\} &= \sum_{E', a': \xi(E', a' | r) = k, \xi_s = 1} \mathbf{P}\{E = E'\} \mathbf{P}\{a = a'\} \\ &= 2^{-T} \sum_{E', a': \xi(E', a' | r) = k, \xi_s = 1} \mathbf{P}\{E = E'\} \\ &= 2^{-T} \sum_{E': \xi(E', E' x^s | r) = k} \mathbf{P}\{E = E'\} \\ &= 2^{-T} \sum_{E': \eta(E' | x^s, r) = k} \mathbf{P}\{E = E'\} \\ &= 2^{-T} \mathbf{P}\{\eta(E \mid x^s, r) = k\}. \end{aligned}$$

Поэтому согласно лемме 10

$$\mathbf{P}\{\xi = k \mid \xi_s = 1\} = \mathbf{P}\{\eta = k\}, \quad s = 1, \dots, N,$$

где $\eta = \eta(E \mid x^0, r)$. Следовательно,

$$\mathbf{E}((\xi - 1)_{l-1} \mid \xi_s = 1) = \sum_{k \geq 1} \mathbf{P}\{\xi = k \mid \xi_s = 1\} (k - 1)_{l-1} = \mathbf{E}(\eta - 1)_{l-1}. \quad (77)$$

Из (76), (77) вытекает, что

$$\mathbf{E}(\xi)_l = \mathbf{E}\xi \mathbf{E}(\eta - 1)_{l-1}, \quad l \geq 1. \quad (78)$$

Применяя теперь формулу обращения (см., например, [6], стр. 23), с учетом (78) получаем, что

$$\begin{aligned} \mathbf{P}\{\xi = k\} &= \sum_{l \geq k} (-1)^{l-k} \binom{l}{k} \mathbf{E}(\xi)_l / l! \\ &= \mathbf{E}\xi \sum_{l \geq k} (-1)^{l-k} \binom{l}{k} \mathbf{E}(\eta - 1)_{l-1} / l! \\ &= \frac{1}{k} \mathbf{E}\xi \sum_{l-1 \geq k-1} (-1)^{l-k} \binom{l-1}{k-1} \mathbf{E}(\eta - 1)_{l-1} / (l-1)! \\ &= \frac{1}{k} \mathbf{E}\eta \mathbf{P}\{\eta - 1 = k - 1\}, \quad k \geq 1. \end{aligned}$$

Лемма 11 доказана.

Используя лемму 11 и соотношение (5), которые выполняются равномерно по распределениям вектора a , получаем (7).

Для доказательства второй части теоремы 2 воспользуемся следующей очевидной леммой.

Лемма 12. *Имеет место равенство*

$$\eta(E \mid x^0, r) = \eta(E \mid x^1, n - r), \quad (79)$$

где $x^1 = (x_1^0 \oplus 1, \dots, x_n^0 \oplus 1)$.

Вторая часть теоремы 2 вытекает из леммы 12 и первой части теоремы 2. Теорема 2 доказана.

Доказательство теоремы 3. Пусть некоторая случайная величина ζ представляется суммой индикаторов:

$$\zeta = \zeta_1 + \dots + \zeta_N,$$

где $\zeta_k, k = 1, \dots, N$, принимают лишь значения 1, 0. Положим

$$b_{s(1)\dots s(l)} = \mathbf{P}\{\zeta_{s(1)} = \dots = \zeta_{s(l)} = 1\},$$

где $s(1), \dots, s(l) \in \{1, \dots, N\}$. В [7] получены условия, при которых величина ζ асимптотически нормальна. Эти условия можно ослабить. А. П. Барановым был замечен следующий факт.

Лемма 13. *Пусть при $N \rightarrow \infty$ выполняются условия*

$$(1) \hat{\Lambda} = \sum_{s=1}^N b_s \rightarrow \infty;$$

$$(2) \Delta_l = \sum_{(s(1), \dots, s(l))} (b_{s(1)\dots s(l)} - b_{s(1)} \dots b_{s(l)}) = o(\hat{\Lambda}^{-t}), \quad l = 2, 3, \dots, \quad t = 1, 2, \dots;$$

(3) *существует предел*

$$\frac{1}{\hat{\Lambda}} \lim_{N \rightarrow \infty} \sum_{s=1}^N b_s^2 = \gamma.$$

Тогда распределение величины $(\zeta - \hat{\Lambda}/\sqrt{\hat{\Lambda}})$ слабо сходится к нормальному распределению с нулевым средним и дисперсией $\sigma^2 = 1 - \gamma$.

Доказательство. Пусть $\zeta'_1, \dots, \zeta'_N$ — независимые величины, распределенные так же, как и величины $\zeta_1, \dots, \zeta_N$; положим

$$\zeta' = \zeta'_1 + \dots + \zeta'_N.$$

В силу условий леммы

$$\mathbf{E} \left(\frac{\zeta - \hat{\Lambda}}{\sqrt{\hat{\Lambda}}} \right)^k - \mathbf{E} \left(\frac{\zeta' - \hat{\Lambda}}{\sqrt{\hat{\Lambda}}} \right)^k = \sum_{l=1}^k \frac{\Delta_l}{l!} \sum_{v=l}^k \sum_{j=0}^l (-1)^{v+l-j} \binom{k}{v} \binom{l}{j} \hat{\Lambda}^{k/2-v} j^v \rightarrow 0.$$

При этом моменты величины $(\zeta' - \hat{\Lambda})\hat{\Lambda}^{-1/2}$ сходятся к моментам нормального распределения, так как

$$\begin{aligned}\ln \varphi(z) &= \ln \mathbf{E} \exp\{iz(\zeta' - \hat{\Lambda})/\sqrt{\hat{\Lambda}}\} \\ &= -iz\sqrt{\hat{\Lambda}} + \sum_{j=1}^n \ln(1 + b_j(\exp(iz/\sqrt{\hat{\Lambda}}) - 1)) \\ &= -z^2\sigma^2/2 + O(1/\sqrt{\hat{\Lambda}})\end{aligned}$$

равномерно по z в любом конечном интервале $|z| \leq R$. Лемма 13 доказана.

В нашем случае

$$\begin{aligned}2^{-T}(1 - \Delta^r)^T &\leq b_s \leq 2^{-T}(1 + \Delta^r)^T, \\ \Lambda(1 - \Delta^r)^T &\leq \hat{\Lambda} = \sum_{s=1}^N b_s \leq \Lambda(1 + \Delta^r)^T,\end{aligned}$$

и условия (1), (3) леммы 13, очевидно, выполняются, при этом

$$\frac{1}{\hat{\Lambda}} \sum_{s=1}^N b_s^2 \rightarrow 0.$$

Проверим условие (2). Справедлива оценка

$$\Sigma_l^{(1)} = \sum_{(s(1), \dots, s(l)) \in \mathcal{S}_l} |b_{s(1)} \dots s(l) - b_{s(1)} \dots b_{s(l)}| \leq 2Q_l,$$

где Q_l — величина, заданная формулами (47), (48). Используя лемму 7, получаем, что

$$\Sigma_l^{(1)} \leq 2(1 + \Delta)^{lT} \frac{\Lambda^l - 1}{\Lambda - 1} \exp\{-[r/2] \ln(n/r) + rl(\ln l + C)\}.$$

Поэтому согласно оценкам (55),

$$\Sigma_l^{(1)} = o(\hat{\Lambda}^{-t}), \quad l = 2, 3, \dots, \quad t = 1, 2, \dots,$$

при условии, что

$$\frac{\ln \Lambda}{r \ln(n/r)} \rightarrow 0.$$

Рассмотрим теперь суммы

$$\Sigma_l^{(2)} = \sum_{rl-r/2 < \mu(s(1), \dots, s(l))} |b_{s(1)} \dots s(l) - b_{s(1)} \dots b_{s(l)}|.$$

В силу оценки (67), которая выполняется при условии (57), и согласно неравенствам (68)

$$|b_{s(1)} \dots s(l)/b_{s(1)} \dots b_{s(l)} - 1| = O(T\Delta^r).$$

Отсюда следует, что

$$\Sigma_l^{(2)} = o(\hat{\Lambda}^{-t}), \quad l = 2, 3, \dots, \quad t = 1, 2, \dots,$$

при условии, что

$$\frac{\ln \Lambda}{\ln(T \Delta^r)} \rightarrow 0.$$

Таким образом, все условия леммы 13 выполняются, причем равномерно по распределениям вектора a . Используя лемму 13, оценку

$$\hat{\Lambda} = \Lambda(1 + O(T \Delta^r))$$

и соотношение (80), получаем (11).

Вторая часть теоремы 3 (соответствующая случаю $n - r \rightarrow \infty$) вытекает из первой части теоремы 3 и леммы 9 (так же, как вторая часть теоремы 1 вытекает из первой части теоремы 1 и леммы 9). Теорема 3 доказана.

Доказательство теоремы 4. Положим

$$\eta = \eta(E \mid x^0, r), \quad \xi = \xi(E, a \mid r).$$

Используя лемму 11 и первую часть теоремы 3, получаем, что

$$\begin{aligned} \mathbf{P}\{z_1 < (\eta - \Lambda)/\sqrt{\Lambda}\} &= \Lambda^{-1}(1 + o(1)) \sum_{\Lambda + z_1\sqrt{\Lambda} < k < \Lambda + z_2\sqrt{\Lambda}} k \mathbf{P}\{\xi = k\} \\ &= (1 + o(1)) \sum_{\Lambda + z_1\sqrt{\Lambda} < k < \Lambda + z_2\sqrt{\Lambda}} \mathbf{P}\{\xi = k\} \\ &= (1 + o(1))(\Phi(z_2) - \Phi(z_1)), \end{aligned}$$

где $\Phi(z)$ — стандартная нормальная функция распределения. Отсюда следует (13).

Вторая часть теоремы 4 вытекает из леммы 12 и первой части теоремы 4 (так же, как вторая часть теоремы 2 вытекает из леммы 12 и первой части теоремы 2). Теорема 4 доказана.

Доказательство теоремы 5. Пусть $\hat{\tau} = \tau(r)$. Положим

$$\begin{aligned} T(n, r, z) &= \left\lfloor (1/\ln 2) \left(\ln \binom{n}{r} + z \right) \right\rfloor, \\ \Delta(n, r, z) &= (1/\ln 2) \left(\ln \binom{n}{r} + z \right) - T(n, r, z), \end{aligned}$$

и обозначим $\xi_r(T)$ число решений веса r системы, образованной первыми T уравнениями. Пользуясь тождеством

$$\mathbf{P}\{\hat{\tau} < T\} = \mathbf{P}\{\xi_r(T) = 0\}$$

и теоремой 1, получаем, что

$$\begin{aligned} \mathbf{P}\left\{\hat{\tau} \leq (1/\ln 2) \left(\ln \binom{n}{r} + z \right)\right\} &= \mathbf{P}\{\hat{\tau} \leq T(n, r, z)\} \\ &= \mathbf{P}\{\xi_r(T(n, r, z) + 1) = 0\} \\ &= \exp\left(- (1/2)^{T(n, r, z) + 1} \binom{n}{r}\right) + o(1) \\ &= \exp\left(- \exp\left(- (T(n, r, z) + 1) \ln 2 + \ln \binom{n}{r}\right)\right) + o(1) \\ &= \exp(\exp(-z + (\Delta(n, r, z) - 1 \ln 2))) + o(1). \end{aligned}$$

Отсюда с учетом неравенств $0 \leq \Delta(n, r, z) < 1$, получаем (20) и (21). В случае $\hat{\tau} = \tau^*(r)$ доказательство проводится аналогично. Теорема 5 доказана.

Автор признателен В. Г. Михайлову за ряд полезных замечаний.

Список литературы

1. Балакин Г. В., Введение в теорию случайных систем уравнений. *Труды по дискретной математике* (1997), **1**, 1–18.
2. Севастьянов Б. А., Предельный закон Пуассона в схеме сумм зависимых случайных величин. *Теория вероятностей и ее применения* (1972) **17**, №4, 733–738.
3. Колчин В. Ф., Севастьянов Б. А., Чистяков В. П., *Случайные размещения*. Наука, Москва, 1976.
4. Михайлов В. Г., Явные оценки в предельных теоремах для сумм случайных индикаторов. *Обозрение прикладной и промышленной математики* (1994) **1**, №1, 580–617.
5. Боровков А. А., *Теория вероятностей*. Наука, Москва, 1978.
6. Сачков В. Н., *Вероятностные методы в комбинаторном анализе*. Наука, Москва, 1978.
7. Амбросимов А. С., Нормальный закон в схеме сумм зависимых случайных величин, рассмотренных Б. А. Севастьяновым. *Теория вероятностей и ее применения* (1976) **21**, №1, 184–189.

Статья поступила 30.04.2002.

Переработанный вариант поступил 10.09.2002.