ТЕОРИЯ ВЕРОЯТНОСТЕЙ
Том 45 И ЕЕ ПРИМЕНЕНИЯ Выпуск 1
2000

© 2000 г.

*КОПЫТЦЕВ В. А.**

ПРЕДЕЛЬНЫЕ ТЕОРЕМЫ ДЛЯ ЧИСЛА РЕШЕНИЙ СИСТЕМЫ СЛУЧАЙНЫХ УРАВНЕНИЙ

В статье исследуются число и структура множества решений заведомо совместной системы случайных уравнений вида

$$\varphi_t(x_{s_1(t)},\dots,x_{s_{d(t)}(t)}) = a_t, \quad t = 1,\dots,T,$$

относительно переменных $x_1,\dots,x_n \in \{0,\dots,q-1\}$, $q \geqslant 2$, где индексы $s_1(t),\dots,s_{d(t)}(t)$ выбираются случайно и независимо при разных t посредством процедуры равновероятного выбора без возвращения. Найдены условия, при которых распределение числа решений этой системы уравнений сходится к распределению случайной величины вида $A \cdot 2^{\eta_1}\cdots q^{\eta_q-1}$, где A — порядок группы подстановок g: $\{0,\dots,q-1\} \longleftrightarrow \{0,\dots,q-1\}$, удовлетворяющих условиям $\varphi_t(y_1,\dots,y_{d(t)}) \equiv \varphi_t(g(y_1),\dots,g(y_{d(t)}))$, $t = 1,\dots,T$, а $\eta_1,\dots,\eta_{q-1}$ — независимые случайные величины, распределенные по закону Пуассона с параметрами $\lambda_1,\dots,\lambda_{q-1}$ соответственно. Приведены выражения для параметров $\lambda_1,\dots,\lambda_{q-1}$. Эти результаты существенно обобщают аналогичные теоремы для случая $q = 2$, доказанные в работах [2] и [3].

Ключевые слова и фразы: системы случайных уравнений, истинное решение, окрестность истинного решения, общее число решений, группы подстановок, распределение Пуассона.

1. Введение и формулировка основных результатов

Пусть $\varphi(y) = \varphi(y_1,\dots,y_d)$ — некоторая функция, заданная на множестве d-мерных векторов с координатами $y_1,\dots,y_d \in \{0,\dots,q-1\}$, $q \geqslant 2$. Выбор области значений функции не будет играть никакой роли и не скажется на результатах.

Условимся обозначать через Σ_φ группу инерции функции φ в симметрической группе S_d, определяемую условием

$$\sigma \in \Sigma_\varphi \Longleftrightarrow \varphi(y_{\sigma(1)},\dots,y_{\sigma(d)}) \equiv \varphi(y_1,\dots,y_d).$$

Рассмотрим случайное уравнение

$$\varphi(x_{s_1},\dots,x_{s_d}) = a \tag{1}$$

*ФАПСИ, Б. Кисельный пер., 4, 103031 Москва, Россия.

относительно переменных $x_1, \ldots, x_n \in \{0, \ldots, q-1\}$, где индексы $s_1, \ldots, s_d$ образуют случайную выборку без возвращения из множества $\{1, \ldots, n\}$. Предполагается, что упорядоченные выборки $(s_{\sigma(1)}, \ldots, s_{\sigma(d)})$, $\sigma \in \Sigma_\varphi$, не различаются и объединяются в один исход. На множестве $\Omega = \{\omega\}$ возможных исходов (классов эквивалентных левых частей уравнения) задано равномерное распределение вероятностей

$$P_\varphi(\omega) = \left[\binom{n}{d} \frac{d!}{|\Sigma_\varphi|}\right]^{-1}, \quad \forall \omega \in \Omega. \tag{2}$$

Пусть система уравнений

$$\varphi(x_{s_1(t)}, \ldots, x_{s_d(t)}) = a_t, \quad t = 1, \ldots, T, \tag{3}$$

составлена из независимо выбранных уравнений вида (1). Правая часть системы определяется равенствами

$$a_t = \varphi(x^\circ_{s_1(t)}, \ldots, x^\circ_{s_d(t)}), \quad t = 1, \ldots, T,$$

при некотором заданном векторе $x^\circ = (x^\circ_1, \ldots, x^\circ_n)$. Вектор x° назовем истинным решением.

Предположим теперь, что имеется конечный набор функций

$$\Phi = \{\varphi_1, \varphi_2, \ldots, \varphi_R\},$$

где $\varphi_r = \varphi_r(y_1, \ldots, y_{d(r)})$, $y_1, \ldots, y_{d(r)} \in \{0, \ldots, q-1\}$, $r = 1, \ldots, R$. Рассмотрим систему уравнений

$$\begin{gathered} \varphi_r(x_{s_1(t)}, \ldots, x_{s_{d(r)}(t)}) = \varphi_r(x^\circ_{s_1(t)}, \ldots, x^\circ_{s_{d(r)}(t)}), \\ t = 1, \ldots, T(r), \ r = 1, \ldots, R, \end{gathered} \tag{4}$$

составленную из независимо выбранных подсистем вида (3), соответствующих функциям $\varphi_1, \ldots, \varphi_R$.

Система уравнений (4) является заведомо совместной системой случайных уравнений, имеющей, по крайней мере, решение x°. Общее число решений ξ является случайной величиной.

Общее число решений ξ для различных классов систем уравнений вида (3) и (4) с функциями φ, заданными на двоичных векторах, исследовалось в работах [1]–[3]. Новизна данной работы состоит в том, что функции φ определены на векторах с координатами из произвольного конечного множества. Отметим, что заведомо совместные системы уравнений исследовались также в [4] и некоторых других работах, но там использована другая схема формирования левых частей.

Приведем формулировки основных результатов.

Пусть $i, j \in \{0, \ldots, q-1\}$, $i \neq j$, и пусть $d_0, \ldots, d_{q-1}$ — набор целых неотрицательных чисел таких, что $d_0 + \cdots + d_{q-1} = d(r) - 1$. Для каждой функции $\varphi_r = \varphi_r(y_1, \ldots, y_{d(r)}) \in \Phi$ положим

$$\pi_r(i, j;\ d_0, \ldots, d_{q-1}) = \sum_{k=1}^{d(r)} \pi_r^{(k)}(i, j;\ d_0, \ldots, d_{q-1}), \tag{5}$$

где величина $\pi_r^{(k)}(i, j;\ d_0, \ldots, d_{q-1})$ равна числу пар (y', y'') векторов вида

$$\begin{aligned} y' &= (y_1, \ldots, y_{k-1}, y'_k, y_{k+1}, \ldots, y_{d(r)}), \\ y'' &= (y_1, \ldots, y_{k-1}, y''_k, y_{k+1}, \ldots, y_{d(r)}), \end{aligned} \tag{6}$$

удовлетворяющих условиям: 1) $y'_k = i$, $y''_k = j$; 2) среди координат y_ν, $\nu \neq k$, содержится d_w координат, равных $w = 0, \ldots, q-1$; 3) $\varphi_r(y') = \varphi_r(y'')$.

Будем различать два случая:

(А) Для некоторой функции $\varphi_r \in \Phi$ найдутся значения i, j, $i \neq j$, и значения $d_0, \ldots, d_{q-1}$ такие, что $\pi_r(i, j;\ d_0, \ldots, d_{q-1}) > 0$.

(Б) Для любых $\varphi_r \in \Phi$, i, j $(i \neq j)$, $d_0, \ldots, d_{q-1}$ выполняется равенство $\pi_r(i, j;\ d_0, \ldots, d_{q-1}) = 0$.

Зафиксируем набор чисел

$$0 < \theta_i < 1, \quad \sum_{i=0}^{q-1} \theta_i = 1, \tag{7}$$

и введем величины

$$\begin{gathered} \lambda_r(i, j) = \sum_{\substack{d_0, \ldots, d_{q-1} \\ d_0 + \cdots + d_{q-1} = d(r)-1}} \theta_0^{d_0} \cdots \theta_{q-1}^{d_{q-1}} \pi_r(i, j;\ d_0, \ldots, d_{q-1}), \\ \lambda_r^* = \max_{i,j} \lambda_r(i, j). \end{gathered} \tag{8}$$

Пусть выполняется случай (А). Сопоставим функциям φ_r: $\lambda_r^* > 0$ некоторые фиксированные числа $t(r) > 0$. Немного ниже мы определим связь этих чисел с параметрами $T(r)$ и n. Положим

$$\begin{gathered} \lambda(i, j) = \sum_{r:\, \lambda_r^* > 0} t(r)\, \lambda_r(i, j), \qquad \lambda^* = \max_{i,j} \lambda(i, j), \\ M = \bigl\{(i, j)\colon \lambda(i, j) = \lambda^*\bigr\}. \end{gathered} \tag{9}$$

Отметим, что, согласно определению, $\lambda^* > 0$.

Каждому элементу $i \in \{0, \ldots, q-1\}$ поставим в соответствие множество

$$J_i = \{j\colon (i, j) \in M\}. \tag{10}$$

Всякое непустое множество (10) разобьем на классы эквивалентных элементов

$$J_i = J_1^{(1)} + \cdots + J_i^{(N_i)}, \quad N_i \geqslant 1, \tag{11}$$

с учетом отношения эквивалентности: $j_1 \sim j_2$, если для любой функции φ_r: $\lambda_r^* > 0$ каждое равенство $\varphi_r(y') = \varphi_r(y'')$, которое выполняется при некоторых векторах y', y'' вида (6), где $y'_k = i$, $y''_k = j_1$, $k \in \{1, \ldots, d(r)\}$, влечет равенство $\varphi_r(y') = \varphi_r(y''')$, где $y''' = (y_1, \ldots, y_{k-1}, y'''_k, y_{k+1}, \ldots, y_{d(r)})$, $y'''_k = j_2$.

Для описания свойств числа ξ и множества Ξ решений системы уравнений (4) нам понадобятся также следующие определения.

Пусть g': $\{0, \ldots, q-1\} \longrightarrow \{0, \ldots, q-1\}$ — некоторое отображение множества $\{0, \ldots, q-1\}$ в себя, и пусть $y = (y_1, \ldots, y_{d(r)})$ — вектор с координатами из этого множества. С целью упрощения обозначений будем полагать $g'(y) = (g'(y_1), \ldots, g'(y_{d(r)}))$.

Обозначим G_r группу подстановок g: $\{0, \ldots, q-1\} \longleftrightarrow \{0, \ldots, q-1\}$, удовлетворяющих условию $\varphi_r(y) \equiv \varphi_r(g(y))$, и положим

$$G = \bigcap_{r=1}^{R} G_r. \tag{12}$$

Ясно, что если некоторый вектор $x = (x_1, \ldots, x_n)$ является решением системы (4), то ее решением является любой вектор $g(x) = (g(x_1), \ldots, g(x_n))$, $g \in G$. Следовательно, любой вектор $g(x^0)$, $g \in G$, является решением этой системы.

Зафиксируем некоторую подстановку $g \in G$ и сопоставим множествам

$$gJ_i^{(l)} = \{g(j)\colon j \in J_i^{(l)}\}, \quad i\colon J_i \neq \varnothing,\ l = 1, \ldots, N_i,$$

множества индексов

$$S_{t,r}(gJ_i^{(l)}) \subseteq \{s\colon g(x_s^0) = g(i)\} = \{s\colon x_s^0 = i\} = \{s(i)\},$$

которые определим условием: $s(i) \in S_{t,r}(gJ_i^{(l)}) \Longleftrightarrow$ любой вектор $(x_1, \ldots, x_n) \in X_{t,r}$, где

$$x_s = g(x_s^0), \quad s \neq s(i),$$
$$x_{s(i)} \in g(i) \cup gJ_i^{(l)} \qquad (g(i) = g(x_{s(i)}^0));$$

$X_{t,r}$ — множество решений уравнения с номером $t \in \{1, \ldots, T(r)\}$ в подсистеме уравнений с функцией φ_r.

Отметим, что, согласно этому определению,

$$S_{t,r}(gJ_i^{(l)}) = S_{t,r}(J_i^{(l)}), \quad \forall g \in G.$$

Положим

$$S_i^{(l)} = \bigcap_{r=1}^{R} \bigcap_{t=1}^{T(r)} S_{t,r}(gJ_i^{(l)}).$$

Каждое переменное $x_{s(i)}$ с индексом $s(i) \in S_i^{(l)}$ можно называть несущественным относительно решения $g(x^\circ) = (g(x_1^\circ), \ldots, g(x_n^\circ))$ по множеству значений $g(i) \cup gJ_i^{(l)}$. Это название мотивируется тем, что, по определению множеств $S_i^{(l)}$, решениями системы (4), кроме решения $g(x^\circ)$ (где $x_{s(i)} = g(x_{s(i)}^\circ) = g(i)$), являются все векторы, отличные от вектора $g(x^\circ)$ только по значениям переменной $x_{s(i)}$ и в которых переменная $x_{s(i)}$ может принимать любое значение из множества $gJ_i^{(l)}$.

Относительно системы $\{S_i^{(l)}\}$ подмножеств $S_i^{(l)}$, где i: $J_i \neq \varnothing$, $l = 1, \ldots, N_i$, определим множество векторов вида

$$X_{g(x^\circ)}(\{S_i^{(l)}\}) = \Big\{(x_1, \ldots, x_n)\colon x_s = g(x_s^\circ),\ \forall s \notin S_i^{(l)};\\ x_s \in g(i) \cup gJ_i^{(l)}\ \ (g(i) = g(x_s^\circ))\ \forall s \in S_i^{(l)}\Big\}.$$

Это множество содержит вектор $g(x^\circ)$ и все векторы, отличные от $g(x^\circ)$ по значениям переменных с индексами из множеств $S_i^{(l)}$: для этих переменных допускаются все значения из множеств $g(i) \cup gJ_i^{(l)}$. Таким образом,

$$\left|X_{g(x^\circ)}(\{S_i^{(l)}\})\right| = \prod_{i:\, J_i \neq \varnothing} \prod_{l=1}^{N_i} \left|g(i) \cup gJ_i^{(l)}\right|^{m_i^{(l)}} = \prod_{i:\, J_i \neq \varnothing} \prod_{l=1}^{N_i} (1 + h_i^{(l)})^{m_i^{(l)}},$$

где $m_i^{(l)} = |S_i^{(l)}|$, $h_i^{(l)} = |gJ_i^{(l)}| = |J_i^{(l)}|$, $\forall g \in G$.

Теорема 1. *Пусть выполняется случай* (A) *и, кроме того,*

1) *все функции* $\varphi_r \in \Phi = \{\varphi_1, \ldots, \varphi_R\}$ *обладают свойством: для любых элементов* $i, j \in \{0, \ldots, q-1\}$, $i \neq j$, *найдется пара векторов* y', y'' *вида* (6), *где* $y'_k = i$, $y''_k = j$, $k \in \{1, \ldots, d(r)\}$, *и таких, что* $\varphi_r(y') \neq \varphi_r(y'')$;

при $n \to \infty$

2) *истинное решение содержит* n_i *координат, принимающих значение* i, *причем* $n_i = \theta_i(n) \cdot n$, $\theta_i(n) = \theta_i + o(\ln^{-1} n)$, $0 < \theta_i < 1$;

3) *величины* $T(r)$ *связаны с числом неизвестных* n *соотношениями*

3.1) $T(r)/n \to \infty$, $r = 1, \ldots, R$,

3.2) $T(r) = T \cdot t(r) + o(n)\ \ \forall r\colon \lambda_r^* > 0$,

3.3) $\sum_{r=1}^{R} T(r)\, d(r) - T\lambda^* = n(\ln n + z)$, $z = O(1)$.

Тогда при $n \to \infty$

1) *предельное распределение числа решений* ξ *имеет вид*

$$\mathbf{P}\{\xi = w\} = \sum \prod_{i:\, J_i \neq \varnothing} \prod_{l=1}^{N_i} \frac{(\theta_i e^{-z})^{m_i^{(l)}}}{m_i^{(l)}!} \exp\{-\theta_i e^{-z} + o(1)\}, \qquad (13)$$

сумма $\sum$ *берется по значениям величин* $m_i^{(l)}$, i: $J_i \neq \varnothing$, $l = \overline{1, N_i}$, *таким, что*

$$w = |G| \prod_{i:\, J_i \neq \varnothing} \prod_{l=1}^{N_i} (1 + h_i^{(l)})^{m_i^{(l)}},$$

где $|G|$ — *порядок группы подстановок* (12);

2) *структура множества* Ξ *решений описывается предельным соотношением*

$$\mathbf{P}\Big\{\Xi = \bigcup_{g \in G} X_{g(x^\circ)}(\{S_i^{(l)}\})\Big\} \longrightarrow 1. \tag{14}$$

Следствие. *В условиях теоремы* 1 *распределение числа решений слабо сходится к распределению случайной величины* $|G| \cdot 2^{\eta_1} \cdots q^{\eta_{q-1}}$, *где* $\eta_1, \ldots, \eta_{q-1}$ — *независимые случайные величины, распределенные по закону Пуассона с параметрами* $\lambda_1, \ldots, \lambda_{q-1}$ *соответственно,*

$$\lambda_h = e^{-z} \sum_{i:\, J_i \neq \varnothing} \theta_i \Big| \{l \in (1, \ldots, N_i) \colon h_i^{(l)} = h\} \Big|, \quad h = 1, \ldots, q-1.$$

Это утверждение вытекает из соотношения (13).

Пусть выполняется случай (Б). Относительно подмножества $S \subseteq \{1, \ldots, n\}$ индексов переменных, не вошедших ни в одно уравнение системы (4), определим множество векторов

$$X_{g(x^\circ)}(S) = \Big\{(x_1, \ldots, x_n) \colon x_s = g(x_s^\circ)\ \forall\, s \notin S;\ x_s \in \{0, \ldots, q-1\}\ \forall\, s \in S\Big\}.$$

Теорема 2. *Пусть имеет место случай* (Б) *и выполняется условие* 1 *теоремы* 1. *Пусть, кроме того, при* $n \to \infty$

2) *доля* $\theta_i(n) = n_i/n$ *координат в истинном решении* x°, *принимающих значение* i, *заключена в границах* $0 < \delta \leqslant \theta_i(n) \leqslant 1 - \delta < 1$, $i = 0, \ldots, q-1$;

3) *величины* $T(r)$ *связаны с числом неизвестных* n *соотношениями*

3.1) $T(r)/n \to \infty$, $r = 1, \ldots, R$,

3.2) $\sum_{r=1}^{R} T(r)\, d(r) = n(\ln n + z)$, $z = O(1)$.

Тогда

1) *при* $n \to \infty$

$$\mathbf{P}\{\xi = |G|\, q^m\} = \frac{e^{-zm}}{m!} \exp\{-e^{-z} + o(1)\}, \quad m = 0, 1, 2, \ldots; \tag{15}$$

2) *при* $n \to \infty$

$$\mathbf{P}\Big\{\Xi = \bigcup_{g \in G} X_{g(x^\circ)}(S)\Big\} \longrightarrow 1; \tag{16}$$

3) *если* $|G_r| = 1$, $r = 1, \ldots, R$, *то утверждения* 1, 2 *выполняются независимо от условия* 3.1.

Обозначим $\widetilde{\lambda}_r(i,j)$ величину, полученную по формуле (8) после замены в ней постоянных параметров θ_i, $i=0,\ldots,q-1$, на переменные $\theta_i(n)$.

Пусть $q=2$. Относительно произвольного подмножества $S\subseteq\{1,\ldots,n\}$ определим множество векторов

$$X_{g(x^\circ)}(S)=\{\boldsymbol{x}=(x_1,\ldots,x_n)\colon x_s=g(x_s^\circ)\ \forall s\notin S;\ x_s\in\{0,1\}\ \forall s\in S\}.$$

Теорема 3. *Пусть $q=2$, выполняется условие 1 теоремы 1 (это условие принимает вид: $\varphi_r\not\equiv\mathrm{const}$, $\forall\varphi_r\in\Phi$) и при $n\to\infty$*

2) *выполняется условие 2 теоремы 2;*

3) *величины $T(r)$ связаны с величиной n соотношениями*

3.1) $T(r)/n\to\infty$, $r=1,\ldots,R$,

3.2) $\sum_{r=1}^{R}T(r)\,(d(r)-\widetilde{\lambda}_r(0,1))=n(\ln n+z)$, $z=O(1)$.

Тогда

1) *при $n\to\infty$*

$$\mathbf{P}\{\xi=|G|\,2^m\}=\frac{e^{-mz}}{m!}\exp\{-e^{-z}+o(1)\},\quad m=0,1,2,\ldots; \tag{17}$$

2) *при $n\to\infty$*

$$\mathbf{P}\Big\{\exists S\colon \Xi=\bigcup_{g\in G}X_{g(x^\circ)}(S)\Big\}\longrightarrow 1, \tag{18}$$

если выполняется случай (Б) *и, следовательно,* $\widetilde{\lambda}_r(0,1)=0$, $r=1,\ldots,R$, *то множество S состоит из индексов переменных, не вошедших ни в одно уравнение системы;*

3) *если $|G_r|=1$, $r=1,\ldots,R$, то утверждения 1, 2 выполняются независимо от условия* 3.1.

Замечание 1. Вариант теоремы 3 для случая $|G_r|=1$, $r=1,\ldots,R$, доказан в работе [3].

Замечание 2. Условие 3.3 теоремы 1 с учетом условия 3.2 эквивалентно соотношению

$$\sum_{r\colon\lambda_r^*=0}T(r)\,d(r)+T\Big[\sum_{r\colon\lambda_r^*>0}t(r)\,d(r)-\lambda^*\Big]=n\Big(\ln n+z+o(1)\Big).$$

Это соотношение является корректным (выполнимо, в частности, в случае $\{r\colon\lambda_r^*=0\}=\varnothing$), если

$$\lambda^*<\sum_{r\colon\lambda_r^*>0}t(r)\,d(r). \tag{19}$$

Покажем, что строгое неравенство (19) обеспечивается условиями 1, 2 теоремы 1. Действительно, из формул (9) вытекает:

$$\lambda^*\leqslant\sum_{r\colon\lambda_r^*>0}t(r)\max_{i,j}\lambda_r(i,j). \tag{20}$$

Для величины $\pi_r^{(k)}(i,j;\ d_0,\dots,d_{q-1})$, согласно ее определению (см. (5) и ниже), выполняется неравенство

$$\pi_r^{(k)}(i,j;\ d_0,\dots,d_{q-1}) \leqslant \frac{(d(r)-1)!}{d_0!\cdots d_{q-1}!}. \tag{21}$$

Поэтому с учетом (7), (8) имеем

$$\max_{i,j} \lambda_r(i,j) \leqslant d(r). \tag{22}$$

Если для функции φ_r и любых элементов i,j, $i \neq j$, найдутся указанные в условии 1 теоремы 1 векторы y', y'', то при некотором наборе значений $d_0,\dots,d_{q-1}$, $d_0+\cdots+d_{q-1} = d(r)-1$, в (21) будет выполняться строгое неравенство. Из этого неравенства и (7), (8) следует строгое неравенство в (22), из которого с учетом (20) следует (19).

2. Вспомогательные утверждения

Утверждение 1. *Пусть функция $\varphi_r \in \Phi$ обладает свойством из условия* 1 *теоремы* 1, *тогда для любого вырожденного (не взаимно однозначного) отображения g': $\{0,\dots,q-1\} \longrightarrow \{0,\dots,q-1\}$ найдется вектор y такой, что $\varphi_r(y) \neq \varphi_r(g'(y))$, $g'(y) = (g'(y_1),\dots,g'(y_{d(r)}))$.*

Доказательство. Предположим противное, а именно: существует вырожденное отображение g' такое, что $\varphi_r(y) \equiv \varphi_r(g'(y))$. В силу вырожденности g' для некоторых элементов $i,j \in \{0,\dots,q-1\}$, $i \neq j$, выполняется равенство $g'(i) = g'(j)$. Тогда для каждой пары векторов y', y'', вида (6), где $y'_k = i$, $y''_k = j$, $k = 1,\dots,d(r)$, должно выполняться равенство $\varphi_r(y') = \varphi_r(y'')$, так как $\varphi_r(y') = \varphi_r(g'(y'))$, $\varphi_r(y'') = \varphi_r(g'(y''))$, и $g'(y') = g'(y'')$, согласно равенству $g'(i) = g'(j)$. Утверждение 1 доказано.

Пусть $\mathbf{E}\xi$ — математическое ожидание числа ξ.

Лемма 1. *Пусть выполняются условия теоремы* 1. *Тогда при $n \to \infty$*

$$\mathbf{E}\xi = |G| \exp\left\{\sum_{i=0}^{q-1} \theta_i h_i e^{-z} + o(1)\right\}, \tag{23}$$

где h_i — число элементов в множестве J_i.

Лемма 2. *Пусть выполняются условия теоремы* 2. *Тогда*

1) *при $n \to \infty$* $\mathbf{E}\xi = |G| \exp\{(q-1)\,e^{-z} + o(1)\}$; (24)

2) *если $|G_r| = 1$, $r = 1,\dots,R$, то утверждение* 1 *выполняется независимо от условия* 3.1 *теоремы.*

Лемма 3. *Пусть* $q = 2$ *и выполняются условия теоремы* 3. *Тогда*
1) *при* $n \to \infty$ $\mathbf{E}\xi = |G| \exp\{e^{-z} + o(1)\}$;
2) *если* $|G_r| = 1$, $r = 1, \ldots, R$, *то утверждение* 1 *выполняется независимо от условия* 3.1 *теоремы.*

2.1. Доказательство леммы 1. Обозначим $\rho(x', x'')$ расстояние Хемминга между векторами $x' = (x'_1, \ldots, x'_n)$ и $x'' = (x''_1, \ldots, x''_n)$:

$$\rho(x', x'') = \sum_{k=1}^{n} I(x'_k \neq x''_k), \quad I(x'_k \neq x''_k) = \begin{cases} 1, & \text{если } x'_k \neq x''_k; \\ 0, & \text{если } x'_k = x''_k. \end{cases}$$

Определим ε-окрестность вектора x' как множество векторов

$$M_\varepsilon(x') = \{x\colon \rho(x', x'') \leqslant \varepsilon n\}.$$

Без ограничения общности мы можем положить в условии 2 теоремы 1, что $0 < \delta \leqslant \theta_i(n) \leqslant 1 - \delta < 1$. Тогда при любых подстановках $g_1, g_2 \in G$, $g_1 \neq g_2$,

$$\rho(g_1(x^\circ), g_2(x^\circ)) = \rho(x^\circ, g_1^{-1} g_2(x^\circ)) \geqslant n \min_{i \in \{0,\ldots,q-1\}} \theta_i \geqslant n\delta.$$

Выберем $\varepsilon < \delta/2$. При этом условии $M_\varepsilon(g_1(x^\circ)) \cap M_\varepsilon(g_2(x^\circ)) = \varnothing$, $\forall\, g_1, g_2 \in G$, $g_1 \neq g_2$, и математическое ожидание $\mathbf{E}\xi$ можно представить в следующем виде:

$$\begin{aligned} \mathbf{E}\xi &= \Sigma_1 + \Sigma_2, \\ \Sigma_1 &= \sum_{g \in G} \sum_{x \in M_\varepsilon(g(x^\circ))} \prod_{r=1}^{R} [P_r(x)]^{T(r)}, \\ \Sigma_2 &= \sum_{x \notin \cup_{g \in G} M_\varepsilon(g(x^\circ))} \prod_{r=1}^{R} [P_r(x)]^{T(r)}, \end{aligned} \tag{25}$$

где $P_r(x)$ — вероятность того, что вектор x удовлетворяет одному уравнению системы (4), связанному с функцией φ_r.

Оценим суммы Σ_1, Σ_2 из разложения (25). Согласно равенству $\rho(x^\circ, x) = \rho(g(x^\circ), g(x))$, имеем $M_\varepsilon(g(x^\circ)) = \{g(x)\colon x \in M_\varepsilon(x^\circ)\}$. Кроме того, $P_r(g(x)) = P_r(x)$ $\forall\, g \in G$, так как по определению группы G векторы x и $g(x)$ одновременно удовлетворяют или не удовлетворяют одному уравнению системы с функцией φ_r. Поэтому для внутренней суммы в слагаемом Σ_1 из разложения (25) получаем

$$\begin{aligned} \sum_{x \in M_\varepsilon(g(x^\circ))} \prod_{r=1}^{R} [P_r(x)]^{T(r)} &= \sum_{x \in M_\varepsilon(x^\circ)} \prod_{r=1}^{R} [P_r(g(x))]^{T(r)} \\ &= \sum_{x \in M_\varepsilon(x^\circ)} \prod_{r=1}^{R} [P_r(x)]^{T(r)}. \end{aligned}$$

Следовательно,

$$\Sigma_1 = |G|\,\Sigma_1^*, \quad \Sigma_1^* = \sum_{x \in M_\varepsilon(x^\circ)} \prod_{r=1}^{R} [P_r(x)]^{T(r)}. \tag{26}$$

Положим

$$n_{ij}(x^\circ, x) = \Big|\{s\colon x_s^\circ = i,\ x_s = j\}\Big|.$$

По определению расстояния Хемминга имеем

$$\rho(x^\circ, x) = \sum_{i,j\colon i \neq j} n_{ij}(x^\circ, x).$$

Ясно, что все векторы x, имеющие одинаковый набор чисел

$$n_{ij}(x^\circ, x) = n_{ij}, \quad i, j = \overline{0, q-1}, \tag{27}$$

имеют одинаковую вероятность

$$P_r(x) = P_r[n_{ij};\ i, j = \overline{0, q-1}]. \tag{28}$$

Количество векторов x, которым соответствует фиксированный набор чисел (27), равно $\prod_{i=0}^{q-1} n_i!\,[n_{i,0}! \cdots n_{i,q-1}!]^{-1}$. Следовательно, сумму (26) можно переписать в следующем виде

$$\Sigma_1^* = \sum_{n_{ij}\colon \sum_{i \neq j} n_{ij} \leqslant \varepsilon n} D\,[n_{ij};\ i, j = \overline{0, q-1}], \tag{29}$$

где

$$D\,[n_{ij};\ i, j = \overline{0, q-1}] = \prod_{i=0}^{q-1} \frac{n_i!}{n_{i,0}! \cdots n_{i,q-1}!} \prod_{r=1}^{R} \Big(P_r[n_{ij};\ i, j = \overline{0, q-1}]\Big)^{T(r)}$$

и суммирование проводится по всем значениям величин n_{ij}, удовлетворяющим условию $\sum_{i \neq j} n_{ij} = \sum_{i,j\colon i \neq j} n_{ij} \leqslant \varepsilon n$.

Обозначим $v = v(x)$ число координат вектора x из множества $\{x_s \in (x_1, \ldots, x_n)\colon x_s \neq x_s^\circ\}$, входящих в уравнение

$$\varphi_r(x_{s_1(t)}, \ldots, x_{s_{d(r)}(t)}) = \varphi_r(x^\circ_{s_1(t)}, \ldots, x^\circ_{s_{d(r)}(t)}). \tag{30}$$

Для вероятности (28), согласно формуле полной вероятности, получим

$$P_r(x) = \mathbf{P}\{v = 0\}\,P_r(x \mid v = 0) + \mathbf{P}\{v = 1\}\,P_r(x \mid v = 1) + \sum_{v' \geqslant 2} \mathbf{P}\{v = v'\}\,P_r(x \mid v = v'), \tag{31}$$

где через $P_r(x \mid v = v')$ обозначена вероятность того, что при условии $v(x) = v'$ вектор x удовлетворяет уравнению (30).

Пусть $\sum_{i \neq j} n_{ij} = o(n)$. Последовательно раскрывая слагаемые в правой части равенства (31), найдем

$$P_r(x) = P_r[n_{ij};\ i, j = \overline{0, q-1}] = \left[\binom{n}{d(r)} \frac{d(r)!}{|\Sigma_{\varphi_r}|}\right]^{-1} \times \left[\binom{\sum_{i=0}^{q-1} n_{ii}}{d(r)} \frac{d(r)!}{|\Sigma_{\varphi_r}|} + \sum_{i \neq j} n_{ij} \sum_{\substack{d_0, \ldots, d_{q-1} \\ d_0 + \cdots + d_{q-1} = d(r)-1}} \prod_{i=0}^{q-1} \binom{n_{ii}}{d_i} \pi_r(i, j; d_0, \ldots, d_{q-1}) \frac{\prod_{i=0}^{q-1} d_i!}{|\Sigma_{\varphi_r}|} + O\left(n^{d-2}\left(\sum_{i \neq j} n_{ij}\right)^2\right)\right], \tag{32}$$

где величина $\pi_r(i, j; d_0, \ldots, d_{q-1})$ определяется формулой (5). Выражение (32) перепишем в следующем виде:

$$P_r[n_{ij};\ i, j = \overline{0, q-1}] = 1 - \frac{1}{n} \sum_{i \neq j} n_{ij}(d(r) - \widetilde{\lambda}_r(i, j)) + O\left(\left(\sum_{i \neq j} \frac{n_{ij}}{n}\right)^2\right), \tag{33}$$

где величина $\widetilde{\lambda}_r(i, j)$ получена по формуле (8) после замены в ней фиксированных параметров θ_i, $i = 0, \ldots, q-1$, на переменные $\theta_i(n)$.

Разобьем сумму (29) на две части

$$\Sigma_1^* = \Sigma_{1,1}^* + \Sigma_{1,2}^*, \tag{34}$$

полагая

$$\Sigma_{1,1}^* = \sum_{n_{ij}:\, 0 \leqslant \sum_{i \neq j} n_{ij} \leqslant n^{1/3}} D[n_{ij};\ i, j = \overline{0, q-1}],$$

$$\Sigma_{1,2}^* = \sum_{n_{ij}:\, n^{1/3} < \sum_{i \neq j} n_{ij} \leqslant \varepsilon n} D[n_{ij};\ i, j = \overline{0, q-1}],$$

и оценим каждую часть по отдельности.

В области $0 \leqslant \sum_{i \neq j} n_{ij} \leqslant n^{1/3}$ имеем оценки

$$\prod_{i=0}^{q-1} \frac{n_i!}{n_{i,0}! \cdots n_{i,q-1}!} = \exp\left\{\sum_{i \neq j} n_{ij} \ln n + o(1)\right\} \prod_{i=0}^{q-1} \prod_{j:\, j \neq i} \frac{(\theta_i(n))^{n_{ij}}}{n_{ij}!},$$

$$\prod_{r=1}^{R}\Big(P_r[n_{ij};\ i,j=\overline{0,\,q-1}]\Big)^{T(r)}$$
$$=\exp\Big\{-\sum_{i\neq j}n_{ij}\,\frac{1}{n}\sum_{r=1}^{R}T(r)\Big(d(r)-\widetilde{\lambda}_r(i,\,j)\Big)+o(1)\Big\}.$$

Положим

$$\sigma(i,\,j)=\frac{1}{n}\sum_{r=1}^{R}T(r)\Big(d(r)-\widetilde{\lambda}_r(i,\,j)\Big)-\ln n. \tag{35}$$

Согласно условиям 2, 3.2, 3.3 теоремы 1,

$$\sigma(i,\,j)=\frac{1}{n}\Big(\sum_{r=1}^{R}T(r)\,d(r)-T(\lambda^*-\Delta(i,\,j))+o(n)\Big)-\ln n$$
$$=\frac{T}{n}\,\Delta(i,\,j)+z+o(1), \tag{36}$$

где $\Delta(i,j)=0$, $(i,j)\in M$ и $\Delta(i,j)>0$, $(i,j)\notin M$, множество M определено формулами (9). Следовательно, при условии 3.1 теоремы 1

$$\sigma(i,j)\to\infty,\quad (i,j)\notin M. \tag{37}$$

Поэтому с учетом неравенств $\Psi(n^{1/3}/q^2)\leqslant\Sigma_{1,1}^{*}\leqslant\Psi(n^{1/3})$, где

$$\Psi(z)=\prod_{i=0}^{q-1}\prod_{j:\,j\neq i}\sum_{n_{ij}=0}^{z}\exp\Big\{-n_{ij}\sigma(i,j)+o(1)\Big\}\,\frac{(\theta_i(n))^{n_{ij}}}{n_{ij}!},$$

а также с учетом соотношений (36), (37) и условия 2 теоремы 1 найдем

$$\Sigma_{1,1}^{*}\approx\prod_{i:\,J_i\neq\varnothing}\prod_{j:\,j\in J_i}\sum_{n_{ij}=0}^{\infty}\exp\{-n_{ij}z\}\,\frac{\theta_i^{n_{ij}}}{n_{ij}!}$$
$$=\prod_{i:\,J_i\neq\varnothing}\exp\{\theta_i h_i e^{-z}\}=\prod_{i=0}^{q-1}\exp\{\theta_i h_i e^{-z}\}, \tag{38}$$

где h_i — число элементов в множестве J_i.

Оценим теперь сумму $\Sigma_{1,2}^{*}$ из разложения (34). Из представления (33) вытекает

$$\prod_{r=1}^{R}\Big(P_r[n_{ij};\ i,\,j=\overline{0,\,q-1}]\Big)^{T(r)}\leqslant\exp\Big\{-\frac{\sigma}{n}\,\delta(\varepsilon)\sum_{i\neq j}n_{ij}\Big\},$$

где $\sigma = \sum_{r=1}^{R} T(r)\, d(r) - T\lambda^*$, $\lim_{\varepsilon\to 0}\delta(\varepsilon) = 1$. Пользуясь этой оценкой и неравенствами

$$\prod_{i=0}^{q-1} \frac{n_i!}{n_{i,0}!\cdots n_{i,q-1}!} \leqslant \prod_{i=0}^{q-1} \frac{n_i!}{n_{ii}!(n_i - n_{ii})\,!}\,(q-1)^{n_i - n_{ii}}$$
$$\leqslant (q-1)^{\sum_{i\neq j} n_{ij}} \binom{n}{\sum\limits_{i\neq j} n_{ij}},$$

а также полагая $H(u) = -u\ln u - (1-u)\,\ln(1-u)$, получаем

$$\Sigma_{1,2}^* \leqslant \sum_{n_{ij}:\, n^{1/3} < \sum_{i\neq j} n_{ij} \leqslant \varepsilon n} \exp\Big\{ -[\sigma\delta(\varepsilon) - n\ln(q-1)]\,u + nH(u) + O(\ln n)\Big\}\Big|_{u=\sum_{i\neq j} n_{ij}/n}.$$

Функция $H(u)$ в области $0 < u < \varepsilon$ выпукла вверх, поэтому с учетом условия 3.3 теоремы 1 имеем

$$\Sigma_{1,2}^* \leqslant n^{q(q-1)} \exp\Big\{ -\sigma(\delta(\varepsilon) + o(1))\,u + n\,H(u) + O(\ln n)\Big\}\Big|_{u=n^{1/3}/n}$$
$$\leqslant n^{q(q-1)} \exp\Big\{ -\Big(\delta(\varepsilon) - \tfrac{2}{3} + o(1)\Big)\, n^{1/3}\ln n + O(n^{1/3})\Big\} = o(1), \quad (39)$$

если значение ε достаточно мало.

Нам осталось оценить сумму Σ_2 из разложения (25). Покажем, что для любого вектора $x \notin \cup_{g\in G} M_\varepsilon(g(x^0))$ найдется функция $\varphi_r \in \Phi$ такая, что

$$P_r(x) = P_r[n_{ij};\ i,j = \overline{0,\, q-1}] \leqslant 1 - \alpha(\varepsilon), \quad (40)$$

где $0 < \alpha(\varepsilon) = \text{const}$. Из неравенства (40) будет следовать оценка

$$\Sigma_2 \leqslant q^n (1 - \alpha(\varepsilon))^{T'} = o(1), \quad (41)$$

где $T' = \min_r T(r)$, и $T'/n \to \infty$, согласно условию 3.1 теоремы 1.

Собирая вместе (25), (26), (34) и оценки (38), (39), (41), получим (23).

Пусть набор чисел $n_{ij}(x^0, x) = n_{ij}$, $i,j = 0,\ldots,q-1$, удовлетворяет условию

$$\sum_{i\neq j} n_{ij} = \sum_{i=0}^{q-1} \sum_{j:\, j\neq i} n_{ij} \geqslant \varepsilon n.$$

Из этого условия следует, что существует (единственный) набор индексов $i_1,\ldots,i_k$, $1 \leqslant k \leqslant q$, которому соответствуют неравенства

$$\sum_{j:\, j\neq i_1} n_{i_1,j} > \frac{\varepsilon n}{q},\ \ldots,\ \sum_{j:\, j\neq i_k} n_{i_k,j} > \frac{\varepsilon n}{q}; \quad (42)$$

$$\sum_{j:\, j\neq i} n_{ij} \leqslant \frac{\varepsilon n}{q}, \quad i \notin \{i_1,\ldots,i_k\}. \quad (43)$$

В свою очередь, из неравенств (42) вытекает, что найдется набор индексов $j_1, \dots, j_k$, $j_1 \neq i_1, \dots, j_k \neq i_k$, для которого

$$n_{i_1,j_1} > \frac{\varepsilon n}{q(q-1)}, \ \dots, \ n_{i_k,j_k} > \frac{\varepsilon n}{q(q-1)}, \tag{44}$$

а из неравенств (43) с учетом соотношений $\sum_{j=0}^{q-1} n_{ij} = n_i = \theta_i(n)\, n$ следует:

$$n_{ii} = n_i - \sum_{j:\, j\neq i} n_{ij} \geqslant \left(\theta_i(n) - \frac{\varepsilon}{q}\right) n, \quad i \notin \{i_1, \dots, i_k\}. \tag{45}$$

Сопоставим системе неравенств (44), (45) отображение g': $\{0, \dots, q-1\} \longrightarrow \{0, \dots, q-1\}$, определяемое условиями

$$g'(i_1) = j_1, \dots, g'(i_k) = j_k; \qquad g'(i) = i, \quad i \notin \{i_1, \dots, i_k\}, \tag{46}$$

и рассмотрим два возможных случая: (В) $g' \notin G$, (Г) $g' \in G$.

(В) Пусть $g' \notin G$. Тогда для некоторой функции $\varphi_r \in \Phi$ найдется вектор y такой, что $\varphi_r(y) \neq \varphi_r(g'(y))$. Действительно, если отображение g' является вырожденным, то указанный вектор y найдется согласно утверждению 1, в противном случае он найдется согласно определению группы G.

Пусть вектор y содержит d_w координат, принимающих значение $w = 0, \dots, q-1$. Тогда вероятность того, что упорядоченная выборка координат $(x_{s_1(t)}, \dots, x_{s_{d(r)}(t)})$ из вектора $x = (x_1, \dots, x_n)$, соответствующая уравнению

$$\varphi_r\big(x_{s_1(t)}, \dots, x_{s_{d(r)}(t)}\big) = \varphi_r\big(x^{\circ}_{s_1(t)}, \dots, x^{\circ}_{s_{d(r)}(t)}\big),$$

образует вектор y, равна

$$P = \prod_{\nu=1}^{k} \binom{n_{i_\nu,j_\nu}}{d_{i_\nu}}\, d_{i_\nu}! \prod_{i\notin\{i_1,\dots,i_k\}} \binom{n_{ii}}{d_i} \frac{d_i!}{|\Sigma_{\varphi_r}|} \left[\binom{n}{d(r)} \frac{d(r)!}{|\Sigma_{\varphi_r}|}\right]^{-1}$$

Отсюда с учетом (44), (45) вытекает

$$\begin{aligned} &1 - P_r[n_{ij};\ i, j = \overline{0, q-1}] \\ &\quad \geqslant P = (1 + o(1)) \left(\frac{\varepsilon}{q(q-1)}\right)^k \prod_{i\notin\{i_1,\dots,i_k\}} \left(\theta_i - \frac{\varepsilon}{q}\right). \end{aligned} \tag{47}$$

Следовательно, существует функция $\varphi_r \in \Phi$, для которой выполняется оценка (40) (при достаточно больших значениях n).

(Г) Рассмотрим теперь второй случай:

$$g' = g \in G. \tag{48}$$

Выберем ε такое, что

$$\theta_{i_\nu}(n) - \frac{\varepsilon}{q(q-1)} > \frac{\varepsilon}{q(q-1)}, \quad \nu = \overline{1,k},$$

и предположим, что выполняются более жесткие по сравнению с неравенствами (44) ограничения

$$n_{i_1,j_1} \geqslant \left(\theta_{i_1}(n) - \frac{\varepsilon}{q(q-1)}\right) n, \ldots, n_{i_k,j_k} \geqslant \left(\theta_{i_k}(n) - \frac{\varepsilon}{q(q-1)}\right) n. \quad (49)$$

Положим $n_{ij}^{(g)} = n_{ij}^{(g)}(x^\circ, x) = |\{s\colon g(x_s^\circ) = i,\ x_s = j\}|$ и с учетом (49) и (45) получим, что

$$n_{i_\nu,j_\nu} = n_{e(i_\nu),j_\nu}^{(e)} = n_{g(i_\nu),j_\nu}^{(g)} = n_{j_\nu,j_\nu}^{(g)} \geqslant \left(\theta_{i_\nu}(n) - \frac{\varepsilon}{q(q-1)}\right) n, \quad \nu = \overline{1,k};$$

$$n_{ii} = n_{e(i),i}^{(e)} = n_{g(i),i}^{(g)} = n_{ii}^{(g)} \geqslant \left(\theta_i(n) - \frac{\varepsilon}{q}\right) n, \quad i \notin \{i_1, \ldots, i_k\},$$

где e — единичный элемент группы G. Следовательно,

$$\rho(g(x^\circ), x) = n - \sum_{j_\nu \in \{i_1,\ldots,i_k\}} n_{j_\nu,j_\nu}^{(g)} - \sum_{i \notin \{i_1,\ldots,i_k\}} n_{ii}^{(g)}$$

$$\leqslant \varepsilon n \left(1 - \frac{k}{q} + \frac{k}{q(q-1)}\right) \leqslant \varepsilon n, \quad \forall\, q \geqslant 2.$$

Значит, при условии (49) вектор x принадлежит ε-окрестности решения $g(x^\circ)$ и не должен учитываться в сумме Σ_2 из разложения (25). Поэтому, по крайней мере, одно из неравенств (49) должно нарушаться.

Пусть

$$n_{i_\nu,j_\nu} < \left(\theta_{i_\nu}(n) - \frac{\varepsilon}{q(q-1)}\right) n, \quad \nu \in \{1, \ldots, k\}. \quad (50)$$

С учетом (50) и равенств $\sum_{j=0}^{q-1} n_{i_\nu,j} = \sum_{j\colon j \neq j_\nu} n_{i_\nu,j} + n_{i_\nu,j_\nu} = \theta_{i_\nu}(n)\, n$ получим, что найдется элемент $j \in \{0, \ldots, q-1\} \backslash j_\nu$, для которого

$$n_{i_\nu,j} > \left[\theta_{i_\nu}(n)\, n - \left(\theta_{i_\nu}(n) - \frac{\varepsilon}{q(q-1)}\right) n\right] \frac{1}{q-1} = \frac{\varepsilon}{q(q-1)^2}\, n. \quad (51)$$

Согласно (44) и (51), имеем

$$\begin{aligned} n_{i_1,j_1}, \ \ldots, \ n_{i_{\nu-1},j_{\nu-1}} &\geqslant \frac{\varepsilon}{q(q-1)}\, n; \\ n_{i_\nu,j} &\geqslant \frac{\varepsilon}{q(q-1)^2}\, n; \\ n_{i_{\nu+1},j_{\nu+1}}, \ \ldots, \ n_{i_k,j_k} &\geqslant \frac{\varepsilon}{q(q-1)}\, n, \end{aligned} \quad (52)$$

где $\nu \in \{1, \ldots, k\}$, $j \in \{0, \ldots, q-1\} \backslash j_\nu$. При этом остаются в силе ограничения (45).

Сопоставим ограничениям (52) и (45) отображение g'': $\{0, \ldots, q-1\} \longrightarrow \{0, \ldots, q-1\}$, определяемое равенствами

$$\begin{aligned} g''(i_1) &= j_1, \ldots, g''(i_{\nu-1}) = j_{\nu-1}; \\ g''(i_\nu) &= j \in \{0, \ldots, q-1\} \backslash j_\nu; \\ g''(i_{\nu+1}) &= j_{\nu+1}, \ldots, g''(i_k) = j_k; \\ g''(i) &= i, \quad i \notin \{i_1, \ldots, i_k\}. \end{aligned} \tag{53}$$

Отображение g'' отличается от заданного равенствами (46) взаимно однозначного по условию (48) отображения g' только одним переходом: $g''(i_\nu) = j \in \{0, \ldots, q-1\} \backslash j_\nu$. Следовательно, отображение g'' является вырожденным. Поэтому по условию 1 теоремы 1 и согласно утверждению 1, для любой функции $\varphi_r \in \Phi$ найдется вектор y такой, что $\varphi_r(y) \neq \varphi_r(g''(y))$.

Теперь мы можем повторить рассуждения, использованные для вывода оценки (47) в случае (В) (см. (46) и ниже), и с учетом (45), (52) заменить в (47) один множитель, равный $\varepsilon/q(q-1)$, на величину $\varepsilon/q(q-1)^2$. Таким образом получим оценку (40) в случае (Г). Лемма 1 доказана.

2.2. Доказательство леммы 2. Доказательство леммы 2 до формулы (35) повторяет доказательство леммы 1. Для величины (35) согласно условию 3.2 теоремы 2 имеем $\sigma(i,j) = z$. Используя это равенство, аналогично выводу оценки (38) получим

$$\begin{aligned} \Sigma^*_{1,1} &\approx \prod_{i=0}^{q-1} \prod_{j:\, j \neq i} \sum_{n_{ij}=0}^{\infty} \exp\{-n_{ij} z\} \frac{\theta_i^{n_{ij}}}{n_{ij}!} \\ &= \prod_{i=0}^{q-1} \exp\{(q-1)\,\theta_i e^{-z}\} = \exp\{(q-1)\,e^{-z}\}, \end{aligned} \tag{54}$$

и эта оценка не зависит от условия 3.1 теоремы 2 (условие 3.1 использовалось в доказательстве леммы 1 при обосновании оценки (38) и при обосновании оценки (41)).

Совершенно аналогично показывается (с учетом условия 3.2 теоремы 2 вместо условия 3.3 теоремы 1), что выполняется оценка (39) и эта оценка не зависит от условия 3.1.

Без каких-либо изменений (с учетом условия 3.1) доказывается оценка (41) и, таким образом, завершается доказательство утверждения 1 леммы 2.

Для доказательства утверждения 2 леммы 2 осталось показать, что в случае $|G_\varphi| = 1$, $r = 1, \ldots, R$, независимо от условия 3.1 выполняется оценка вида (41). Пусть $|G_\varphi| = 1$, $r = 1, \ldots, R$, тогда неравенство (40)

выполняется для любого вектора $x \notin \cup_{g\in G} M_\varepsilon(g(x^0))$ и для любой функции $\varphi_r \in \Phi$, так как для любой функции $\varphi_r \in \Phi$ найдется вектор y такой, что $\varphi_r(y) \neq \varphi_r(g'(y))$, где отображение $g' \notin G$ определено равенствами (46). Поэтому

$$\Sigma_2 \leqslant q^n(1-\alpha(\varepsilon))^{T''} = o(1),$$

где $T'' = \max_r T(r)$ и $T''/n \to \infty$, согласно условию 3.2 теоремы 2. Лемма 2 доказана.

2.3. Доказательство леммы 3. Доказательство леммы 3 фактически вытекает из доказательств лемм 1, 2. Следует только учесть, что при $q = 2$ как в случае (А), так и в случае (Б) для величины (35) имеем $\sigma(0,1) = z$. Поэтому независимо от условия 3.1 теоремы 3 выполняется оценка (54), где $q = 2$.

3. Доказательства теорем

3.1. Доказательство теоремы 1. Обозначим η число пар переменных $x_{s_1(i_1)}, x_{s_2(i_2)}$, где

$$i_1 \leqslant i_2,\ s_1(i) < s_2(i), \quad s_1(i_1), s_2(i_2) \in \bigcup_{i:\, J_i \neq \varnothing} \bigcup_{l=1}^{N_i} S_i^{(l)},$$

содержащихся одновременно, по крайней мере, в одном уравнении системы. Пусть событие B_0 состоит в том, что $\eta = 0$.

Для набора фиксированных неотрицательных целых чисел $m_i^{(l)}$, где i, l пробегают значения $i\colon J_i \neq \varnothing$, $l = 1, \ldots, N_i$, определим событие $B_0(\{m_i^{(l)}\})$, состоящее в том, что $\eta = 0$ и, кроме того, выполняется система равенств $|S_i^{(l)}| = m_i^{(l)}$. Согласно определениям, имеем

$$\begin{aligned} \mathbf{P}\Big\{\Xi \supseteq \bigcup_{g\in G} X_{g(x^0)}(\{S_i^{(l)}\}) \mid B_0\Big\} &= 1, \\ \mathbf{P}\Big\{\xi \geqslant |G| \prod_{i:\, J_i\neq\varnothing} \prod_{l=1}^{N_i} (1+h_i^{(l)})^{m_i^{(l)}} \mid B_0(\{m_i^{(l)}\})\Big\} &= 1, \end{aligned} \tag{55}$$

где $h_i^{(l)} = |J_i^{(l)}|$. Покажем теперь, что

$$\mathbf{P}\Big(B_0(\{m_i^{(l)}\})\Big) = \prod_{i:\, J_i\neq\varnothing} \prod_{l=1}^{N_i} \frac{(\theta_i e^{-z})^{m_i^{(l)}}}{m_i^{(l)}!} \exp\{-\theta_i e^{-z} + o(1)\}. \tag{56}$$

Тогда с учетом (23)

$$|G| \exp\left\{\sum_{i=0}^{q-1} \theta_i h_i e^{-z} + o(1)\right\} = \mathbf{E}\xi \geqslant \sum_{m_i^{(l)}} \mathbf{P}\Big(B_0(\{m_i^{(l)}\})\Big)\, \mathbf{E}\Big(\xi \mid B_0(\{m_i^{(l)}\})\Big),$$

и, согласно (55), (56), правая часть этого неравенства не превосходит величины

$$E' = |G| \exp\left\{\sum_{i=0}^{q-1} \theta_i h_i e^{-z} + o(1)\right\}.$$

Отсюда вытекает, что

$$\mathbf{P}\left\{\xi = |G| \prod_{i:\, J_i \neq \varnothing} \prod_{l=1}^{N_i} (1 + h_i^{(l)})^{m_i^{(l)}} \mid B_0(\{m_i^{(l)}\})\right\} = 1 + o(1). \qquad (57)$$

Из (56), (57) следуют соотношения (13), (14).

Итак, нам осталось доказать соотношение (56). Оценим сначала вероятность $\mathbf{P}\{|S_i^{(l)}| = m_i^{(l)}\}$, $m_i^{(l)} \in \{0, 1, 2, \ldots\}$, выполнения системы равенств $|S_i^{(l)}| = m_i^{(l)}$, где i, l пробегают значения i: $J_i \neq \varnothing$, $l = 1, \ldots, N_i$.

Используя формулу включения и исключения, получим выражение вида

$$\begin{aligned}
&\mathbf{P}\left\{|S_i^{(l)}| = m_i^{(l)}\right\} \\
&\quad = \sum_{\mu_i^{(l)}} \prod_{i:\, J_i \neq \varnothing} \prod_{l=1}^{N_i} (-1)^{\mu_i^{(l)}} \binom{m_i^{(l)} + \mu_i^{(l)}}{\mu_i^{(l)}} \binom{n_i - \sum_{p=1}^{l-1} (m_i^{(p)} + \mu_i^{(p)})}{m_i^{(l)} + \mu_i^{(l)}} \\
&\qquad \times \prod_{r=1}^{R} [P_r^*]^{T(r)}, \qquad (58)
\end{aligned}$$

где сумма $\sum_{\mu_i^{(l)}}$ берется по неотрицательным значениям величин $\mu_i^{(l)}$, i: $J_i \neq \varnothing$, $l = 1, \ldots, N_i$;

$$P_r^* = \mathbf{P}\left\{s_{1,l}(i), \ldots, s_{m_i^{(l)} + \mu_i^{(l)}, l}(i) \in S_{i,r}(J_i^{(l)});\ i\colon J_i \neq \varnothing,\ l = \overline{1, N_i}\right\} \qquad (59)$$

и в правой части (59) указан фиксированный набор индексов.

Обозначим $\widetilde{v} = \widetilde{v}(\boldsymbol{x})$ число координат вектора $\boldsymbol{x}$ с индексами из множества

$$\left\{s_{1,l}(i), \ldots, s_{m_i^{(l)} + \mu_i^{(l)}, l}(i);\ i\colon J_i \neq \varnothing,\ l = \overline{1, N_i}\right\},$$

входящих в уравнение (30). Пусть

$$\sum_{i,l}{}^{*} (m_i^{(l)} + \mu_i^{(l)}) = \sum_{i:\, J_i \neq \varnothing} \sum_{l=1}^{N_i} (m_i^{(l)} + \mu_i^{(l)}) = o(n).$$

Разлагая вероятность (59) по формуле полной вероятности относительно системы событий $\widetilde{v}=0$, $\widetilde{v}=1$, $\widetilde{v}\geqslant 2$, аналогично выкладкам (32) найдем

$$P_r^* = \left[\binom{n}{d(r)}\frac{d(r)!}{|\Sigma_{\varphi_r}|}\right]^{-1} \times\left[\binom{n-\sum\limits_{i,l}{}^{*}(m_i^{(l)}+\mu_i^{(l)})}{d(r)}\frac{d(r)!}{|\Sigma_{\varphi_r}|}\right. + \sum_{i,l}{}^{*}(m_i^{(l)}+\mu_i^{(l)}) \sum_{\substack{d_0,\dots,d_{q-1}\\ d_0+\dots+d_{q-1}=d(r)-1}} \prod_{i:\,J_i\neq\varnothing}\binom{n_i-\sum_l(m_i^{(l)}+\mu_i^{(l)})}{d_i} \times\prod_{i:\,J_i=\varnothing}\binom{n_i}{d_i}\pi_r(J_i^{(l)};\,d_0,\dots,d_{q-1})\frac{\prod_{i=0}^{q-1}d_i!}{|\Sigma_{\varphi_r}|} \left.+\,O\left(n^{d-2}\left(\sum_{i,l}{}^{*}(m_i^{(l)}+\mu_i^{(l)})\right)^2\right)\right], \tag{60}$$

где $\pi_r(J_1^{(l)};\ d_0,\dots,d_{q-1}) = \sum_{k=1}^{d(r)}\pi_r^{(k)}(J_1^{(l)};\ d_0,\dots,d_{q-1})$ и величина $\pi_r^{(k)}(J_1^{(l)};\ d_0,\dots,d_{q-1})$ равна числу множеств вида

$$\left\{(y_1,\dots,y_k,\dots,y_{d(r)})\colon y_k\in i\bigcup J_i^{(l)};\quad y_\nu=C_\nu,\quad \nu\neq k;\right. \left.\varphi_r(y)=C=\mathrm{const}\ \ \forall\, y_k\in i\bigcup J_i^{(l)}\right\},$$

соответствующих различным фиксациям $y_\nu=C_\nu$ переменных y_ν, $\nu\neq k$, таким, что d_w переменных y_ν, $\nu\neq k$, принимают значение $w=0,\dots,q-1$.

Выражение (60) перепишем в следующем виде:

$$P_r^* = 1-\frac{1}{n}\sum_{i,l}{}^{*}(m_i^{(l)}+\mu_i^{(l)})\left(d(r)-\widetilde{\lambda}_r(J_i^{(l)})\right) +O\left(\left(\frac{1}{n}\sum_{i,l}{}^{*}(m_i^{(l)}+\mu_i^{(l)})\right)^2\right), \tag{61}$$

где

$$\widetilde{\lambda}_r(J_i^{(l)}) = \sum_{\substack{d_0,\dots,d_{q-1}\\ d_0+\dots+d_{q-1}=d(r)-1}} (\theta_0(n))^{d_0}\cdots(\theta_{q-1}(n))^{d_{q-1}}\pi_r(J_1^{(l)};\ d_0,\dots,d_{q-1}).$$

Из определения величины $\pi_r^{(k)}(i,j;\ d_0,\dots,d_{q-1})$ (см. (5) и ниже) вытекает $\pi_r^{(k)}(J_i^{(l)};\ d_0,\dots,d_{q-1}) = \pi_r^{(k)}(i,j;\ d_0,\dots,d_{q-1})$, $\forall\, j\in J_i^{(l)}$. Следовательно,

$$\widetilde{\lambda}_r(J_i^{(l)}) = \lambda_r(i,j)+o(\ln^{-1}n),\quad \forall\, j\in J_i^{(l)},$$

$$\sum_{r=1}^{R} t(r)\,\widetilde{\lambda}_r(J_i^{(l)}) = \lambda^* + o(\ln^{-1} n).$$

Поэтому при условиях 3.2, 3.3 теоремы 1 и при условии $\mu_i^{(l)} \leqslant \ln n$, используя (61), найдем

$$\prod_{r=1}^{R}[P_r^*]^{T(r)} = n^{-\sum_{i,l}{}^*(m_i^{(l)}+\mu_i^{(l)})} \times \exp\left\{-(z+o(1))\sum_{i,l}{}^*(m_i^{(l)}+\mu_i^{(l)}) + O\left(\frac{(\ln n)^3}{n}\right)\right\}. \quad (62)$$

Из (58), (62), с учетом неравенств Бонферрони для формулы включения и исключения [5], получим искомую оценку

$$\mathbf{P}\left\{|S_i^{(l)}| = m_i^{(l)}\right\} = \prod_{i:\,J_i\neq\varnothing}\prod_{l=1}^{N_i}\frac{(\theta_i e^{-z})^{m_i^{(l)}}}{m_i^{(l)}\,!}\exp\{-\theta_i e^{-z}+o(1)\}. \quad (63)$$

Оценим теперь вероятность $\mathbf{P}\{\eta > 0\}$. Зафиксируем некоторую пару переменных

$$x_{s_1(i_1)}, \quad x_{s_2(i_2)}, \quad (64)$$

где $s_1(i_1) \in \{s\colon x_s^\circ = i_1\}$, $s_2(i_2) \in \{s\colon x_s^\circ = i_2\}$, $i_1, i_2\colon J_{i_1}, J_{i_2} \neq \varnothing$, и где мы полагаем $i_1 \leqslant i_2$, $s_1(i) < s_2(i)$ в случае $i_1 = i_2 = i$. Введем индикаторы

$$I_{t,r}^{(k)} = I\left(s_1(i_1) \in S_{t,r}(J_{i_1}^{(l_1)}),\ s_2(i_2) \in S_{t,r}(J_{i_2}^{(l_2)}),\ C_{t,r}^{(k)}\right), \quad k = 1, 2,$$

при некоторых фиксированных l_1, l_2. Каждый из этих индикаторов равняется единице, если выполняются все три события, указанные в скобках, и равняется нулю в остальных случаях. Событие $C_{t,r}^{(1)}$ выполняется, если не более одного переменного из пары (64) содержится в (t,r)-уравнении (в уравнении с номером t из подсистемы уравнений с функцией φ_r). Событие $C_{t,r}^{(2)}$ выполняется, если оба переменных (64) содержатся в (t,r)-уравнении.

Введем также индикатор

$$I = I\left(s(i_1) \in S_{i_1}^{(l_1)},\ s(i_2) \in S_{i_2}^{(l_2)},\ C\right),$$

где, согласно принятым ранее обозначениям, $S_i^{(l)} = \cap_{r=1}^{R}\cap_{t=1}^{T(r)} S_{t,r}(J_i^{(l)})$; событие C выполняется, если оба переменных (64) содержатся, по крайней мере, в одном уравнении системы.

С учетом (59), (61) имеем

$$\sum_{k=1}^{2}\mathbf{P}\{I_{t,r}^{(k)} = 1\} = \mathbf{P}\left\{s_1(i_1) \in S_{t,r}(J_{i_1}^{(l_1)}),\ s_2(i_2) \in S_{t,r}(J_{i_2}^{(l_2)})\right\} = 1 - \frac{1}{n}\left(2d(r) - \widetilde{\lambda}_r(J_{i_1}^{(l_1)}) - \widetilde{\lambda}_r(J_{i_2}^{(l_2)})\right) + O(n^{-2}),$$

причем $\mathbf{P}\{I_{t,r}^{(2)} = 1\} = O(n^{-2})$. Поэтому

$$\mathbf{P}\{I = 1\} = \prod_{r=1}^{R} \left[\sum_{k=1}^{2} \mathbf{P}\{I_{t,r}^{(k)} = 1\} \right]^{T(r)} - \prod_{r=1}^{R} \left[\mathbf{P}\{I_{t,r}^{(1)} = 1\} \right]^{T(r)} = O\left(\frac{\ln n}{n^3} \right).$$

Следовательно, для вероятности $\mathbf{P}\{\eta > 0\}$ с учетом равенства

$$\eta = \sum I = \sum_{i_1, i_2} \sum_{s_1(i_1), s_2(i_2)} \sum_{l_1, l_2} I\left(s_1(i_1) \in S_{i_1}^{(l_1)},\ s_2(i_2) \in S_{i_2}^{(l_2)},\ C \right)$$

и неравенств $i, l \leqslant q$, $s(i) \leqslant n$ выполняется оценка

$$\mathbf{P}\{\eta > 0\} \leqslant \sum \mathbf{P}\{I = 1\} = O(n^{-1} \ln n). \tag{65}$$

В силу (63), (65) выполняется (56). Теорема 1 доказана.

3.2. Доказательство теоремы 2 существенно проще, так как вместо величин $|S_i^{(l)}|$ достаточно исследовать одну величину $|S|$, равную числу переменных вектора x, не вошедших ни в одно уравнение системы (4). В эквивалентной терминологии эта величина равна числу пустых ячеек в схеме размещения частиц комплектами и при условии 3.2 теоремы 2 асимптотически распределена по закону Пуассона с параметром e^{-z} (см. [3]). Ясно, что $\mathbf{P}\{\xi \geqslant q^{|S|}\} = 1$. Из этого соотношения, пуассоновости величины $|S|$ и (24) следует (15) и (16).

Учитывая, что для обоснования пуассоновости величины $|S|$ и оценки (24) условие 3.1 не требуется, получаем последнее утверждение теоремы 2. Теорема 2 доказана.

3.3. Доказательство теоремы 3 покрывается доказательствами теорем 1, 2, если вместо лемм 1, 2 использовать лемму 3.

СПИСОК ЛИТЕРАТУРЫ

1. *Балакин Г. В.* Графы систем двучленных уравнений с булевыми неизвестными. — Теория вероятн. и ее примен., 1995, т. 40, в. 2, с. 241–259.
2. *Копытцев В. А.* О распределении числа решений случайных заведомо совместных систем уравнений. — Теория вероятн. и ее примен., 1995, т. 40, в. 2, с. 430–437.
3. *Михайлов В. Г.* Предельные теоремы для случайного покрытия конечного множества и для числа решений системы случайных уравнений. — Теория вероятн. и ее примен., 1996, т. 41, в. 2, с. 272–283.
4. *Масол В. И.* Теорема о предельном распределении числа ложных решений системы нелинейных случайных булевых уравнений. — Теория вероятн. и ее примен., 1998, т. 43, в. 1, с. 41–56.
5. *Сачков В. Н.* Комбинаторные методы дискретной математики. М.: Наука, 1977.

Поступила в редакцию
30.VI.1998