УДК 519.21

**А.А. ЛЕВИТСКАЯ**

# РЕШЕНИЕ ПРОБЛЕМЫ ИНВАРИАНТНОСТИ ВЕРОЯТНОСТНЫХ ХАРАКТЕРИСТИК ЗАВЕДОМО СОВМЕСТНЫХ СИСТЕМ СЛУЧАЙНЫХ НЕЛИНЕЙНЫХ УРАВНЕНИЙ НАД КОНЕЧНЫМ КОММУТАТИВНЫМ КОЛЬЦОМ С ЕДИНИЦЕЙ

**Ключевые слова:** *система случайных нелинейных уравнений над конечным коммутативным кольцом с единицей (над конечным полем), факториальный момент числа решений системы, распределение числа решений системы.*

Проблема инвариантности является одной из ключевых проблем в современной теории систем случайных уравнений над конечными алгебраическими структурами. Суть ее состоит в установлении ограничений на распределение коэффициентов системы, когда число неизвестных в последней стремится к бесконечности, при которых вероятностные характеристики системы (моменты, распределение числа решений) остаются неизменными, например, как в случае равномерного распределения коэффициентов. Первые фундаментальные результаты, связанные с инвариантностью предельного поведения характеристик случайных линейных однородных систем над полем $\mathbf{GF}(2)$, получены И.Н. Коваленко в работе [1]. Их можно считать основополагающими для развития нового направления в исследовании систем случайных уравнений, которое привело к созданию теории инвариантности для систем случайных уравнений над конечными алгебраическими структурами. Более подробный материал о теоретических выводах этой теории содержится в обзоре [2].

Настоящая работа посвящена решению вопросов инвариантности для вероятностных характеристик одного класса нелинейных случайных систем. Предметом изучения являются так называемые заведомо совместные системы случайных нелинейных уравнений над произвольным коммутативным кольцом $\mathbf{R}$ с единицей мощности $|\mathbf{R}|=m$ следующего вида:

$$\sum_{k=1}^{d_i} \sum_{1\le j_1<j_2<\ldots<j_k\le n} a_{i,j_1\ldots j_k} x_{j_1}\cdot\ldots\cdot x_{j_k}=b_i\,,\quad i=\overline{1,n-s}\,, \tag{1}$$

$$\sum_{k=1}^{d_i} \sum_{1\le j_1\le j_2\le\ldots\le j_k\le n} a_{i,j_1\ldots j_k} x_{j_1}\cdot\ldots\cdot x_{j_k}=b_i\,,\quad i=\overline{1,n-s}\,. \tag{2}$$

Здесь в каждой из систем $a_{i,j_1\ldots j_k}$ — независимые в совокупности случайные величины, вектор-солбец $\mathbf{b}{\downarrow}$ правых частей, т.е. $\mathbf{b}{\downarrow}=(b_1,\ldots,b_{n-s}){\downarrow}$, — результат подстановки в правую часть некоторого фиксированного вектора $\mathbf{x}^0=(x_1^0,\ldots,x_n^0)$, $d_i$, $2\le d_i\le n$, $i=\overline{1,n-s}$, — натуральные числа, $s$ — целочисленная константа произвольного знака.

В дальнейшем в целях сокращения записи будем придерживаться одинаковых обозначений для аналогичных понятий в случае каждой из двух приведенных выше систем.

Пусть $\nu_n$ — число решений (1) ((2)), отличных от вектора $\mathbf{x}^0=(x_1^0,\ldots,x_n^0)$. Для каждой из указанных систем нужно установить границу области (инвариантности) изменения распределений коэффициентов, в которой соответственно факториальные моменты и распределение случайной величины $\nu_n$ при $n\to\infty$ будут такими же, как и в случае равномерного распределения коэффициентов.

В работах А.М. Зубкова (результаты не опубликованы), И.Н. Коваленко [1, 3–5], В.И. Масола [6, 7] для случая системы (1) над полем $\mathbf{GF}(2)$ при определенных ограничениях на распределения коэффициентов (1), число единиц в векторе $\mathbf{x}^0=(x_1^0,\ldots,x_n^0)$ и величины $d_i$, $i=\overline{1,n-s}$, на основании анализа факториальных моментов $\nu_n$ установлено, что в пределе при $n\to\infty$ для распределения $\nu_n$ имеет место закон Пуассона с параметром $2^s$.

В статьях [8, 9] исследуются однородные нелинейные системы случайных уравнений, т.е. заведомо совместные системы, в которых правые части $b_i=0$, $i=\overline{1,n-s}$, а $\mathbf{x}^0=(0,\ldots,0)$. Так, в [8] установлено, что для системы (1), где $2\le d_i\le n$, $b_i=0$, $i=\overline{1,n-s}$, рассматриваемой над конечным полем $\mathbf{GF}(q)$, условия

$$\frac{\ln c_n n}{(q-1)n}=\delta_n\le \mathbf{P}\,(a_{i,j_1\ldots j_k}=z),\quad z\in\mathbf{GF}(q), \tag{3}$$

$$1\le j_1<\ldots<j_k\le n,\quad k=\overline{1,d_i},\quad i=\overline{1,n-s},$$

где $c_n$ — произвольная последовательность, стремящаяся к $\infty$, когда $n\to\infty$, определяют (в данной терминологии) границу области инвариантности, в которой при $n\to\infty$ случайная величина $\nu_n$ распределена по закону Пуассона с параметром $q^s$; кроме того, в указанной области инвариантности определены предельные факториальные моменты $\lim\limits_{n\to\infty}\mathbf{M}(\nu_n)_r$, $r$ — натуральное число, и описана геометрическая структура множества решений системы (1). В [9] доказано, что для систем (1), (2) над произвольным конечным кольцом с левой единицей, где $b_i=0$, $i=\overline{1,n-s}$, и при этом в (2) отсутствуют слагаемые вида $ax^k$, $k=\overline{2,d_i}$, $i=\overline{1,n-s}$, условия

$$\frac{l_0}{m(l_0-1)}\,\frac{\ln c_n n}{n}=\delta_n\le \mathbf{P}\,(a_{i,j_1\ldots j_k}=z),\quad z\in\mathbf{R}, \tag{4}$$

где $l_0$ — число, равное наименьшей из мощностей ненулевых левых идеалов $\mathbf{R}$, $m$ — мощность кольца $\mathbf{R}$, $c_n$ то же, что и в (3), определяют (в данной терминологии) границу области инвариантности любого факториального момента $\mathbf{M}(\nu_n)_r$ порядка $r$ ($r$ — некоторое натуральное число) и распределения случайной величины $\nu_n$, когда $n\to\infty$. Установлено также, что в случае отсутствия в $\mathbf{R}$ ненулевого идеала $\mathbf{I}$, для которого $\mathbf{I}\cdot\mathbf{I}=\{0\}$, для системы (2), где $d_i=d$, $i=\overline{1,n-s}$, условия

$$\frac{l_0}{m\,(l_0-1)}\,\frac{\ln c_n n}{dn}=\delta_n\le \mathbf{P}\,(a_{i,j_1,\ldots,j_k}=z),\quad z\in\mathbf{R}, \tag{5}$$

$$1\le j_1\le\ldots\le j_k\le n,\quad k=\overline{1,d},$$

определяют (в данной терминологии) границу области инвариантности $\lim\limits_{n\to\infty}\mathbf{M}(\nu_n)$ и предельного распределения числа решений $\nu_n$. Кроме того, в каждой из областей инвариантности (4), (5) описана геометрическая структура множества решений систем (1), (2) и указаны типы колец (простейший из которых $\mathbf{R}=\mathbf{GF}(q)$), когда при $n\to\infty$ распределение числа решений $\nu_n$ или числа решений специального вида, составляющего часть от общего числа $\nu_n$, распределено по закону Пуассона.

Данная статья является естественным продолжением исследований, представленных в [8, 9]. Ее результаты обобщают соответствующие результаты этих работ.

Приступим к изложению теоретических выводов настоящей работы.

Введем следующие обозначения:

$\mathbf{R}^r=\underbrace{\mathbf{R}\times\ldots\times\mathbf{R}}_{r}$ — векторное пространство над $\mathbf{R}$, элементами которого являются $r$-мерные векторы-столбцы;

$\mathbf{u}=\begin{pmatrix} u_1 \\ \vdots \\ u_r \end{pmatrix}$ (возможны индексы вверху) — элемент $\mathbf{R}^r$;

$\mathbf{0}$ — единица аддитивной группы $\mathbf{R}^r$;

$\mathbf{I}$ (возможны индексы внизу) — некоторый идеал $\mathbf{R}$;

$\mathbf{I}_0$ — минимальный по мощности ненулевой идеал $\mathbf{R}$;

$\mathbf{I}^r=\left\{\begin{pmatrix} z_1 \\ \vdots \\ z_r \end{pmatrix},\ z_i \in \mathbf{I},\ i=\overline{1,r}\right\}$ — $r$-мерное векторное пространство над $\mathbf{I}$;

$$\mathbf{I}_1 \times \mathbf{I}_2 \times \cdots \times \mathbf{I}_t=\left\{\begin{pmatrix} z_1 \\ \vdots \\ z_t \end{pmatrix},\ z_i \in \mathbf{I}_i,\ i=\overline{1,t}\right\};$$

$$\mathbf{I} \cdot \mathbf{I}=\{z_1 \cdot z_2 : z_1, z_2 \in \mathbf{I}\};$$

$\mathbf{M}_r$ (возможны индексы вверху) — некоторый подмодуль $\mathbf{R}^r$;

$$\mathbf{u}^1 \cdot \mathbf{u}^2=\begin{pmatrix} u_1^1 u_1^2 \\ \vdots \\ u_r^1 u_r^2 \end{pmatrix},\quad \mathbf{u}^1, \mathbf{u}^2 \in \mathbf{R}^r;\ z\mathbf{u}=\begin{pmatrix} z u_1 \\ \vdots \\ z u_r \end{pmatrix},\quad \mathbf{u} \in \mathbf{R}^r;$$

$$(\mathbf{M}_r)^2=\{\mathbf{u} \cdot \mathbf{v} : \mathbf{u}, \mathbf{v} \in \mathbf{M}_r\};$$

$\mathbf{x}=(x_1, \cdots, x_n)$ (возможны индексы вверху) — $n$-мерный вектор, координаты которого являются элементами $\mathbf{R}$;

$$\mathbf{X}_r=\begin{pmatrix} \mathbf{x}^1 \\ \vdots \\ \mathbf{x}^r \end{pmatrix}=\begin{pmatrix} x_1^1 & \cdots & x_n^1 \\ \vdots & \cdots & \vdots \\ x_r^1 & \cdots & x_n^r \end{pmatrix};\ \mathbf{X}_r^0=\begin{pmatrix} \mathbf{x}^0 \\ \vdots \\ \mathbf{x}^0 \end{pmatrix}=\begin{pmatrix} x_1^0 & \cdots & x_n^0 \\ \vdots & \cdots & \vdots \\ x_r^0 & \cdots & x_n^0 \end{pmatrix};$$

$(\mathbf{0})_{r \times n}$ — матрица размера $r \times n$, в которой все элементы равны нулю;

$$\mathbf{a}_i \mathbf{X}_r=\sum_{k=1}^{d_i} \sum_{\mathfrak{J}} a_{i, j_1 \cdots j_k} \begin{pmatrix} x_{j_1}^1 & \cdot & x_{j_2}^1 & \cdot \ldots \cdot & x_{j_k}^1 \\ \vdots & & \vdots & \cdot \ldots \cdot & \vdots \\ x_{j_1}^r & \cdot & x_{j_2}^r & \cdot \ldots \cdot & x_{j_k}^r \end{pmatrix},\quad i=\overline{1, n-s},$$

где область суммирования $\mathfrak{J}=\{1 \leq j_1<\cdots<j_k \leq n\}$ в случае системы (1) и $\mathfrak{J}=\{1 \leq j_1 \leq \cdots \leq j_k \leq n\}$ для системы (2);

$$\mathbf{N}_{\mathbf{M}_r}=\left\{\mathbf{X}_r : \left\{\sum_{j=1}^n \alpha_j \begin{pmatrix} x_j^1 \\ \vdots \\ x_j^r \end{pmatrix}+\sum_{j=1}^n n_j \begin{pmatrix} x_j^1 \\ \vdots \\ x_j^r \end{pmatrix},\ \alpha_j \in \mathbf{R},\ n_j \in \mathbf{Z}^+,\ j=\overline{1,n}\right\}=\mathbf{M}_r\right\},$$

т.е. $\mathbf{N}_{\mathbf{M}_r}$ — множество матриц $\mathbf{X}_r$, столбцы каждой из которых порождают модуль $\mathbf{M}_r$;

$\xi_i(\mathbf{X}_r)$ — индикатор события $\{\mathbf{a}_i \mathbf{X}_r=\mathbf{b}_i\downarrow\}$, где $\mathbf{b}_i\downarrow=(b_i, \ldots, b_i)\downarrow$ — $r$-мерный вектор-столбец, $i=\overline{1, n-s}$;

$|\mathbf{T}|$ — мощность множества $\mathbf{T}$; $l_0 \overset{\text{def}}{=} |\mathbf{I}_0|$;

$$k_{\mathbf{u}}(\mathbf{X}_r)=\left[\left\{j : \begin{pmatrix} x_j^1 \\ \vdots \\ x_j^r \end{pmatrix}=\mathbf{u},\ j=\overline{1,n}\right\}\right],\quad \mathbf{u} \in \mathbf{R}^r;$$

т.е. $k_{\mathbf{u}}(\mathbf{X}_r)$ — число столбцов в матрице $\mathbf{X}_r$, равных $\mathbf{u}$;

$$\nu_{n\mathbf{M}_r} = \left|\left\{ \mathbf{X}_r : \mathbf{X}_r \in \mathbf{N}_{\mathbf{M}_r},\ \prod_{i=1}^{n-s} \xi_i(\mathbf{X}_r) = 1 \right\}\right|.$$

Отметим, что все арифметические операции над элементами $\mathbf{R}^r$ выполняются по модулю $m$, те же операции над величинами, не являющимися элементами $\mathbf{R}^r$, — обычные операции в поле действительных чисел.

Не ограничивая общности, условимся считать, что в векторе $\mathbf{x}^0 = (x_1^0, \ldots, x_n^0)$ последние $k_0$ координат равны 0, т.е. $\mathbf{x}^0 = (z_1, \ldots, z_{n-k_0}, 0, \ldots, 0)$, $z_i \in \mathbf{R} \setminus 0$, $i = \overline{1, n-k_0}$, и $k_0(\mathbf{x}^0) = k_0$.

Как и в работах [8, 9], вероятностный анализ систем (1), (2) начнем с вычисления факториальных моментов $\mathbf{M}(\nu_n)_r \overset{\text{def}}{=} \mathbf{M}\nu_n(\nu_n - 1)\ldots(\nu_n - r + 1)$, $r$ — некоторое натуральное число.

Можно записать

$$\mathbf{M}(\nu_n)_r = \sum_{\mathbf{X}_r} \mathbf{M} \prod_{i=1}^{n-s} \xi_i(\mathbf{X}_r), \tag{6}$$

где суммирование ведется по различным матрицам $\mathbf{X}_r$, все строки которых отличны от вектора $\mathbf{x}^0$ и одна от другой.

Преобразуем правую часть (6) таким образом, чтобы в ней были представлены заданные в условии рассматриваемой задачи параметры систем (1), (2). Это позволит в дальнейшем дать естественную интерпретацию теоретических выводов, полученных в результате анализа $\mathbf{M}(\nu_n)_r$ при $n \to \infty$.

Поскольку $\{\mathbf{x}^0 + \mathbf{x}, \mathbf{x} \in \mathbf{R}^n\} = \mathbf{R}^n$, перепишем (6) в виде

$$\mathbf{M}(\nu_n)_r = \sum_{\mathbf{X}_r} \mathbf{M} \prod_{i=1}^{n-s} \xi_i(\mathbf{X}_r^0 + \mathbf{X}_r) = \sum_{\mathbf{X}_r} \prod_{i=1}^{n-s} \mathbf{P}(\mathbf{a}_i(\mathbf{X}_r^0 + \mathbf{X}_r) = \mathbf{a}_i(\mathbf{X}_r^0)) =$$

$$= \sum_{\mathbf{X}_r} \prod_{i=1}^{n-s} \mathbf{P}(\mathbf{a}_i(\mathbf{X}_r^0 + \mathbf{X}_r) - \mathbf{a}_i(\mathbf{X}_r^0) = \mathbf{0}), \tag{7}$$

где суммирование ведется по всем матрицам $\mathbf{X}_r$, все строки которых отличны между собой и от нулевого вектора.

Для вычисления $\mathbf{M}(\nu_n)_r$ используем подход, предложенный в [9] для вычисления моментов числа решений однородных систем случайных нелинейных уравнений.

Выделим из всего множества подмодулей модуля $\mathbf{R}^r$ класс $\mathbf{K}_r$ таких модулей $\mathbf{M}_r = \{\mathbf{u}^1, \ldots, \mathbf{u}^{|\mathbf{M}_r|}\}$, у соответствующих матриц $\hat{\mathbf{M}}_r \overset{\text{def}}{=} \left(\mathbf{u}^1, \ldots, \mathbf{u}^{|\mathbf{M}_r|}\right) \overset{\text{def}}{=}$

$\overset{\text{def}}{=} \begin{pmatrix} u_1^1 & \ldots & u_1^{|\mathbf{M}_r|} \\ \vdots & \ldots & \vdots \\ u_r^1 & \ldots & u_r^{|\mathbf{M}_r|} \end{pmatrix}$ которых все строки различны и отличны от нулевого вектора.

Теперь перепишем правую часть (7) в виде

$$\mathbf{M}(\nu_n)_r = \sum_{\mathbf{M}_r \in \mathbf{K}_r} \mathbf{M}\nu_{n\mathbf{M}_r} = \sum_{\mathbf{M}_r \in \mathbf{K}_r} \sum_{\mathbf{X}_r \in \mathbf{N}_{\mathbf{M}_r}} \mathbf{M} \prod_{i=1}^{n-s} \xi(\mathbf{X}_r^0 + \mathbf{X}_r) =$$

$$= \sum_{\mathbf{M}_r \in \mathbf{K}_r} \sum_{\mathbf{X}_r \in \mathbf{N}_{\mathbf{M}_r}} \prod_{i=1}^{n-s} \mathbf{P}(\mathbf{a}_i(\mathbf{X}_r^0 + \mathbf{X}_r) - \mathbf{a}_i(\mathbf{X}_r^0) = \mathbf{0}). \tag{8}$$

В [9] для модулей из $\mathbf{K}_r$ введены понятия расширяемости и нерасширяемости и доказано одно утверждение, связанное с ними. Поскольку они важны и в данной работе, целесообразно их напомнить.

**Определение 1.** Модуль $\mathbf{M}_r \in \mathbf{K}_r$ называется расширяемым, если существуют элементы $\mathbf{u}, \mathbf{v} \in \mathbf{M}_r$ (не обязательно $\mathbf{u} \neq \mathbf{v}$) такие, что $\mathbf{u} \cdot \mathbf{v} \notin \mathbf{M}_r$.

**Определение 2.** Если $\mathbf{u} \cdot \mathbf{v} \in \mathbf{M}_r$ для всех $\mathbf{u}, \mathbf{v} \in \mathbf{M}_r$, то модуль $\mathbf{M}_r$ называется нерасширяемым.

Множество нерасширяемых модулей в $\mathbf{K}_r$ обозначим $\mathbf{K}_r^0$.

**Утверждение 1.** Если $\mathbf{R} = \mathbf{GF}(q)$, то любой собственный подмодуль $\mathbf{M}_r \in \mathbf{K}_r$ модуля $\mathbf{R}^r = (\mathbf{GF}(q))^r$ может быть расширен до $\mathbf{R}^r$ для любого натурального $r$.

В [8, 9] последнее утверждение играет ключевую роль при обосновании в случае выполнения ограничений (4) сходимости распределения числа ненулевых решений соответствующей (1) однородной системы над $\mathbf{R} = \mathbf{GF}(q)$ к закону Пуассона, когда $n \to \infty$. В [9] также приведен пример, демонстрирующий, что для $\mathbf{R} \neq \mathbf{GF}(q)$ утверждение 1 не имеет места.

Следующие две леммы являются аналогами лемм 1, 2 из работы [9].

**Лемма 1.** Если $\mathbf{M}_r \in \mathbf{K}_r^0$ и для коэффициентов систем (1), (2) выполняются условия (4), то $\lim\limits_{n \to \infty} \mathbf{M}\nu_{n\mathbf{M}_r} = |\mathbf{M}_r|^s$.

**Лемма 2.** Для любого расширяемого модуля $\mathbf{M}_r \in \mathbf{K}_r \setminus \mathbf{K}_r^0$ при выполнении условий (4) имеет место соотношение $\lim\limits_{n \to \infty} \mathbf{M}\nu_{n\,\mathbf{M}_r} = 0$.

Доказательство лемм 1 и 2 опускаем, поскольку они полностью повторяют доказательства аналогичных лемм в [9] при условии, что в рассматриваемом случае в соответствующих неравенствах вместо однородных линейных систем будут фигурировать соответствующие (1), (2) однородные нелинейные системы.

На основании лемм 1, 2 справедливы следующие теоремы, доказательство которых аналогичны доказательству соответствующих теорем в работе [9].

**Теорема 1.** При выполнении условий (4) для любого натурального $r$

$$\lim_{n \to \infty} \mathbf{M}(\nu_n)_r = \sum_{\mathbf{M}_r \in \mathbf{K}_r^0} |\mathbf{M}_r|^s. \tag{9}$$

**Следствие 1.** При выполнении условий (4) для любого набора $\mathbf{x}^0 + \mathbf{x}^1, \ldots$ $\ldots, \mathbf{x}^0 + \mathbf{x}^r$, отличных от $\mathbf{x}^0$ и один от другого векторов-решений системы (1) ((2)), с вероятностью, стремящейся к 1 при $n \to \infty$, существует модуль $\mathbf{M}_r \in \mathbf{K}_r^0$ такой, что соответствующая матрица $\mathbf{X}_r = \begin{pmatrix} \mathbf{x}^1 \\ \vdots \\ \mathbf{x}^r \end{pmatrix} \in \mathbf{N}_{\mathbf{M}_r}$ и при этом $k_{\mathbf{u}}(\mathbf{X}_r) \underset{n \to \infty}{\sim} \dfrac{n}{|\mathbf{M}_r|}$, $\mathbf{u} \in \mathbf{M}_r$.

**Следствие 2.** При выполнении условий (4)

$$\lim_{n \to \infty} \mathbf{M}(\nu_n)_1 = \lim_{n \to \infty} \mathbf{M}\nu_n = \sum_{\mathbf{I} \subseteq \mathbf{R}} |\mathbf{I}|^s,$$

где суммирование ведется по всем идеалам кольца $\mathbf{R}$, отличным от нулевого.

**Замечание**. Поскольку для случая $\mathbf{R} \neq \mathbf{GF}(q)$

$$\lim_{n \to \infty} \mathbf{M}(\nu_n)_2 = \sum_{\mathbf{M}_2 \in \mathbf{K}_2^0} |\mathbf{M}_2|^s \neq \left( \sum_{\mathbf{I} \subseteq \mathbf{R}} |\mathbf{I}|^s \right)^2,$$

следовательно, для $\mathbf{R} \neq \mathbf{GF}(q)$ распределение случайной величины $\nu_n$ при $n \to \infty$ не может стремиться к закону Пуассона. Однако для решений определенного вида закон Пуассона имеет место и в случае $\mathbf{R} \neq \mathbf{GF}(q)$.

Предположим, что в $\mathbf{R}$ существуют идеалы, изоморфные полям. Выделим их: $\{\mathbf{I}_{01}, \ldots, \mathbf{I}_{0t}\} = \mathbf{D}_0$. Относительно таких идеалов справедливы следующие теоремы, аналогом которых являются соответственно теоремы 2–4 в [9].

**Теорема 2.** Если выполнены условия (4), то для любого натурального $r$

$$\lim_{n\to\infty} \mathbf{M}(\nu_{n\mathbf{I}_{0i}})_r = |\mathbf{I}_{0i}|^{rs}, \ i=\overline{1,t}. \tag{10}$$

**Теорема 3.** Пусть выполнены условия (4). Тогда для каждого фиксированного $i, i=\overline{1,t}$, случайная величина $\nu_{n\,\mathbf{I}_{0i}}$ при $n\to\infty$ распределена по закону Пуассона с параметром $|\mathbf{I}_{0i}|^s$.

**Теорема 4.** Пусть выполнены условия (4) и пусть для кольца $\mathbf{R}$ множество $\mathbf{D}_0 \neq \varnothing$. Тогда случайная величина $\nu_{n\mathbf{D}_0} \overset{\text{def}}{=} \left|\left\{\mathbf{x}^0+\mathbf{x} : \mathbf{x}\in \bigcup\limits_{\mathbf{I}\in\mathbf{D}_0}\mathbf{N}_\mathbf{I} \wedge \prod\limits_{i=1}^{n-s}\xi_i(\mathbf{x}^0+\mathbf{x})=1\right\}\right|$ распределена по закону Пуассона с параметром $\sum\limits_{i=1}^{t}|\mathbf{I}_{0i}|^s$. При этом для любого набора $\mathbf{x}^0+\mathbf{x}^1,\ldots,\mathbf{x}^0+\mathbf{x}^r$, отличных одно от другого и от $\mathbf{x}^0$ решений системы (1) ((2)), для которого матрица $\mathbf{X}_r = \begin{pmatrix}\mathbf{x}^1\\ \vdots \\ \mathbf{x}^r\end{pmatrix} \in \mathbf{N}_{\mathbf{I}_{0i_1}\times\ldots\times\mathbf{I}_{0i_r}}$, где $\mathbf{I}_{0i_j}\in\mathbf{D}_0$, $j=\overline{1,r}$, $r$ — некоторое натуральное число, с вероятностью, стремящейся к 1, когда $n\to\infty$, имеют место соотношения

$$k_\mathbf{u}(\mathbf{X}_r) \ \underset{n\to\infty}{\sim} \ \frac{n}{\prod\limits_{j=1}^{r}|\mathbf{I}_{0i_j}|}, \quad \mathbf{u}\in\mathbf{I}_{0i_1}\times\ldots\times\mathbf{I}_{0i_r}.$$

Вообще говоря, ограничения (4) в условиях теорем 1–4 выступают в роли достаточных. Теперь нужно для каждой из систем (1), (2) установить такие ограничения на распределение коэффициентов, чтобы они были не только достаточными, но и необходимыми для справедливости утверждений теорем 1–4.

В целях сокращения записи решать поставленную задачу будем для систем (1) и (2) в предположении, что в этих системах $d_i=d$, $i=\overline{1,n-s}$.

Пусть далее $\nu_{*n}$ — число решений системы (1) ((2)), отличных от $\mathbf{x}^0$, при равномерном распределении ее коэффициентов и пусть

$$0<\delta_n \le \mathbf{P}(a_{i,j_1\ldots j_k}=z), \quad z\in\mathbf{R}. \tag{11}$$

Для каждой из систем (1), (2) необходимо определить минимальное $\delta_n$ в (11), при котором

$$\lim_{n\to\infty}\mathbf{M}(\nu_n)_r = \lim_{n\to\infty}\mathbf{M}(\nu_{*n})_r \tag{12}$$

для любого натурального $r$, или, что то же самое, имело бы место соотношение (9) в теореме 1.

В основе решения этой проблемы лежат утверждения следующих теорем.

**Теорема 5.** Пусть $\mathbf{M}_r\in\mathbf{K}_r^0$. Для выполнения соотношения

$$\lim_{n\to\infty}\mathbf{M}\nu_{n\mathbf{M}_r} = \lim_{n\to\infty}\mathbf{M}\nu_{*n\mathbf{M}_r} \tag{13}$$

необходимо и достаточно, чтобы математическое ожидание числа решений вида $\mathbf{X}_r^0+\mathbf{X}_r$, отличных от $\mathbf{X}_r^0$ на матрицу $\mathbf{X}_r\in\mathbf{N}_{\mathbf{M}_r}$, в которой ненулевые столбцы составляют минимальную систему образующих модуля $\mathbf{M}_r$, стремилось к нулю при $n\to\infty$.

**Доказательство**. Доказательство теоремы основывается на анализе вкладов двух точек максимума $\mathbf{X}_r^0$ и $\mathbf{X}_r^0+\overline{\mathbf{X}}_r$, где в матрице $\overline{\mathbf{X}}_r$ для любого $\mathbf{u}\in\mathbf{M}_r$ величина $k_\mathbf{u}(\overline{\mathbf{X}}_r)=\left[\dfrac{n}{|\mathbf{M}_r|}\right]$, которые определяют значение суммы $F_n =$

$$= \sum_{\mathbf{X} \in \mathbf{N}_{\mathbf{M}_r} \cup (\mathbf{0})_{r \times n}} \prod_{i=1}^{n-s} \mathbf{P}\,(\,\mathbf{a}_i\,(\mathbf{X}^0 + \mathbf{X}) - \mathbf{a}_i\,(\mathbf{X}^0\,) = \mathbf{0})$$ при $n \to \infty$. Такой анализ был проведен для ряда конкретных колец и модулей. На основании полученных результатов, имеющих строгое математическое обоснование, была сформулирована данная теорема.

Поскольку система образующих минимального по мощности ненулевого идеала $\mathbf{I}_0$ кольца $\mathbf{R}$ состоит из одного элемента, на основании теоремы 5 очевидно следующее утверждение.

**Теорема 6.** Для выполнения соотношения

$$\lim_{n \to \infty} \mathbf{M}\,\nu_{n\,\mathbf{I}_0} = \lim_{n \to \infty} \mathbf{M}\,\nu_{*n\,\mathbf{I}_0} \tag{14}$$

необходимо и достаточно, чтобы математическое ожидание числа решений системы, отличных от $\mathbf{x}^0$ только по одной координате $x_i^0 + x_i$ на величину $x_i \in \mathbf{I}_0 \setminus 0$, $i = \overline{1, n}$, стремилось к 0 при $n \to \infty$.

Теперь в силу теорем 5, 6 и поскольку в любом $\mathbf{M}_r \in \mathbf{K}_r^0$, $r \ge 1$, минимальная система образующих не меньше чем в $\mathbf{I}_0$, искомое $\delta_n$ определяется на основании следующей теоремы

**Теорема 7.** Искомое $\delta_n$ в (11) равно минимальному $\delta_n$, при котором имеет место (14) $\forall\,(\mathbf{I}_0\,)$, или, что то же самое, минимальному $\delta_n$, при котором математическое ожидание числа решений системы, отличных от $\mathbf{x}^0$ только по одной координате от $x_i^0 + x_i$ на величину $x_i \in \mathbf{I}_0 \setminus 0$, $i = \overline{1, n}$, стремится к нулю при $n \to \infty$ $\forall\,(\mathbf{I}_0\,)$.

Далее покажем, как происходит нахождение искомого $\delta_n$ для каждой из систем (1) и (2). В целях сокращения записи продемонстрируем этот процесс на случае, когда $\mathbf{R} = \mathbf{GF}(q)$, $d_i = d$, $i = \overline{1, n-s}$.

1. Система (1) над $\mathbf{GF}(q)$, в которой $d_i = d$, $i = \overline{1, n-s}$, имеет вид

$$\sum_{k=1}^{d} \sum_{1 \le j_1 < j_2 < \ldots < j_k \le n} a_{i,\,j_1 \ldots\, j_k} x_{j_1} \cdot \ldots \cdot x_{j_k} =$$

$$= \sum_{k=1}^{d} \sum_{1 \le j_1 < j_2 < \ldots < j_k \le n} a_{i,\,j_1 \ldots\, j_k} x_{j_1}^0 \cdot \ldots \cdot x_{j_k}^0, \quad i = \overline{1, n-s}\,.$$

На основании (7) можно записать:

$$\mathbf{M}\nu_n = \sum_{\mathbf{x} \ne 0} \prod_{i=1}^{n-s} \mathbf{P}(\,\mathbf{a}_i\,(\mathbf{x}^0 + \mathbf{x}) - \mathbf{a}_i\,(\mathbf{x}^0\,) = 0)\,.$$

Здесь $\mathbf{x}^0 = (z_1^0, \ldots, z_{n-k_0}^0, 0, \ldots, 0)$, $z_i \ne 0$, $i = \overline{1, n-k_0}$. По определению выражение $\mathbf{a}_i\,(\mathbf{x}^0 + \mathbf{x}) - \mathbf{a}_i\,(\mathbf{x}^0\,)$ представляет собой сумму произведений вида $y_{j_1} \cdot \ldots \cdot y_{j_k} \ne$ $\ne x_{j_1}^0 \ldots x_{j_k}^0$, $1 \le j_1 < j_2 < \ldots < j_k \le n$, $k = \overline{1, d}$; при этом среди них ненулевыми являются только те, в которые входят либо только ненулевые координаты вектора $\mathbf{x}$ и не входят координаты $\mathbf{x}^0$, либо координаты из множества первых $(n - k_0\,)$ координат вектора $\mathbf{x}^0$ и обязательно хотя бы одна из ненулевых координат $\mathbf{x}$.

В зависимости от величины $k_0$ в выражении для $\mathbf{M}\nu_n$ выделим следующие частичные суммы:

а) если $k_0 \ne 0$, рассмотрим две частичные суммы: сумму $S_n^1$ по множеству векторов $\mathbf{x}$, у которых одна из первых $(n - k_0\,)$ координат отлична от 0, а остальные равны 0 (для каждого такого $\mathbf{x}$ выражение $\mathbf{a}_i\,(\mathbf{x}^0 + \mathbf{x}) - \mathbf{a}_i\,(\mathbf{x}^0\,)$ состоит из

$\sum_{i=0}^{\min(d-1,\, n-k_0-1)} C_{n-k_0-1}^{i}$ ненулевых слагаемых), и сумму $S_n^2$ по множеству векторов $\mathbf{x}$, у которых одна из последних $k_0$ координат отлична от нуля, а остальные равны нулю (для каждого такого $\mathbf{x}$ выражение $\mathbf{a}_i(\mathbf{x}^0+\mathbf{x})-\mathbf{a}_i(\mathbf{x}^0)$ состоит из $\sum_{i=0}^{\min(d-1,\, n-k_0)} C_{n-k_0}^{i}$ ненулевых слагаемых);

б) если $k_0=0$, то в выражении для $\mathbf{M}\nu_n$ выделяем одну частичную сумму $S_n^1$, определенную в п. а).

В силу результатов работы [5, гл. 9] для $S_n^1$ и $S_n^2$ имеют место следующие оценки:

$$\frac{(q-1)(n-k_0)}{q^N}\left[1-(1-q\delta_n)^{\sum_{i=0}^{\min(d-1,n-k_0-1)} C_{n-k_0-1}^{i}}\right]^N \le S_n^1 \le$$

$$\le \frac{(q-1)(n-k_0)}{q^N}\left[1+(q-1)(1-q\delta_n)^{\sum_{i=0}^{\min(d-1,n-k_0-1)} C_{n-k_0-1}^{i}}\right]^N;$$

$$\frac{(q-1)k_0}{q^N}\left[1-(1-q\delta_n)^{\sum_{i=0}^{\min(d-1,n-k_0)} C_{n-k_0}^{i}}\right]^N \le S_n^2 \le$$

$$\le \frac{(q-1)k_0}{q^N}\left[1+(q-1)(1-q\delta_n)^{\sum_{i=0}^{\min(d-1,n-k_0)} C_{n-k_0}^{i}}\right]^N.$$

Задача состоит в определении минимального $\delta_n$, при котором верхние и нижние оценки для $S_n^1$ и $S_n^2$ одновременно стремятся к 0, когда $n\to\infty$. Однако, поскольку при стремлении к 0 верхних оценок нижние автоматически стремятся к 0, для нахождения необходимого $\delta_n$ достаточно рассматривать только верхние оценки частичных сумм $S_n^1$ и $S_n^2$.

Наиболее простой вид эти оценки будут иметь при $d>n-k_0$. Действительно, в этом случае можно записать:

$$S_n^1 \le \frac{(q-1)(n-k_0)}{q^N}\left[1+(q-1)(1-q\delta_n)^{2^{n-k_0-1}}\right]^N, \tag{15}$$

$$S_n^2 \le \frac{(q-1)k_0}{q^N}\left[1+(q-1)(1-q\delta_n)^{2^{n-k_0}}\right]^N.$$

Отсюда получаем следующие неравенства:

$$S_n^1 \le (q-1)(n-k_0)\left[1-2^{n-k_0-1}(q-1)\delta_n+O(2^{2(n-k_0-1)}\delta_n^2)\right]^N,$$

$$S_n^2 \le (q-1)k_0\left[1-2^{n-k_0}(q-1)\delta_n+O(2^{2(n-k_0)}\delta_n^2)\right]^N.$$

Из вида верхней оценки величины $S_n^1$ следует, что она при $n \to \infty$ стремится к 0, если

$$\delta_n = \delta_n^1 = \frac{\ln c_n (n-k_0)}{2^{n-k_0-1}(q-1)n},$$

где $c_n$ — некоторая последовательность, стремящаяся к $\infty$, когда $n \to \infty$. Соответствующее значение $\delta_n$ для верхней оценки $S_n^2$ равно

$$\delta_n = \delta_n^2 = \frac{\ln c_n k_0}{2^{n-k_0}(q-1)n}.$$

Пусть теперь $d = n - k_0$. В этом случае для $S_n^1$ неравенство (15) сохраняется, а для $S_n^2$ справедливо следующее соотношение:

$$S_n^2 \le \frac{(q-1)k_0}{q^N}\left[1+(q-1)(1-q\delta_n)^{2^{n-k_0}-1}\right]^N.$$

Из вида верхней оценки для $S_n^2$ следует, что она стремится к 0 при $n \to \infty$ тогда и только тогда, когда

$$\delta_n = \delta_n^2 = \frac{\ln c_n k_0}{2^{n-k_0}(q-1)n}.$$

Итак, при $d \ge n - k_0$ искомое $\delta_n$ равно

$$\delta_n = \max\left(\delta_n^1 = \frac{\ln c_n (n-k_0)}{2^{n-k_0-1}(q-1)n}, \delta_n^2 = \frac{\ln c_n k_0}{2^{n-k_0}(q-1)n}\right).$$

Выясним условия, при которых $\delta_n^1 \ge \delta_n^2$.

**Утверждение 2.** Пусть $d \ge n - k_0$. Тогда, если $k_0 \le n + \frac{1}{2c_n} - \sqrt{\frac{n}{c_n} + \frac{1}{4c^2}}$, верхние оценки для частичных сумм $S_n^1$ и $S_n^2$ одновременно стремятся к 0, когда $n \to \infty$, при $\delta_n = \delta_n^1$; в противном случае аналогичное происходит при $\delta_n = \delta_n^2$.

**Доказательство**. Утверждение непосредственно следует из решения неравенства

$$\frac{\ln c_n^2 (n-k_0)^2}{2^{n-k_0}(q-1)n} - \frac{\ln c_n k_0}{2^{n-k_0}(q-1)n} \ge 0.$$

Это неравенство равносильно $c_n (n-k_0)^2 \ge k_0$ или $k_0^2 - \left(2n + \frac{1}{c_n}\right)k_0 + n^2 \ge 0$. Отсюда получаем, что при $k_0 \le n + \frac{1}{2c_n} - \sqrt{\frac{n}{c_n} + \frac{1}{4c_n^2}}$ величина $\delta_n^1 \ge \delta_n^2$.

Следовательно, если $k_0 \le n + \frac{1}{2c_n} - \sqrt{\frac{n}{c_n} + \frac{1}{4c_n^2}}$ и $n \to \infty$, верхние оценки для частичных сумм $S_n^1$ и $S_n^2$ стремятся к 0 при $\delta_n = \delta_n^1 = \frac{\ln c_n (n-k_0)}{2^{n-k_0-1}(q-1)n}$; если же $k_0 > n + \frac{1}{2c_n} - \sqrt{\frac{n}{c_n} + \frac{1}{4c_n^2}}$ и $n \to \infty$, то аналогичное будет происходить, когда $\delta_n = \delta_n^2 = \frac{\ln c_n k_0}{2^{n-k_0}(q-1)n}$, что и требовалось доказать.

Пусть теперь $d < n - k_0$. Тогда соответствующие неравенства для $S_n^1$ и $S_n^2$ имеют вид

$$S_n^1 \le \frac{(q-1)(n-k_0)}{q^N}\left[1+(q-1)(1-q\delta_n)^{\sum_{i=0}^{d} C_{n-k_0-1}^i}\right]^N,$$

$$S_n^2 \le \frac{(q-1)k_0}{q^N}\left[1+(q-1)(1-q\delta_n)^{\sum_{i=0}^{d} C_{n-k_0}^i}\right]^N.$$

Как и в случае $d \ge n-k_0$, устанавливаем $\delta_n^1$ и $\delta_n^2$, при которых верхние оценки для $S_n^1$ и $S_n^2$, когда $n \to \infty$, соответственно стремятся к 0. Нетрудно показать, что в случае $d < n - k_0$

$$\delta_n^1 = \frac{\ln c_n(n-k_0)}{\sum_{i=0}^{d} C_{n-k_0-1}^i (q-1)n}, \quad \delta_n^2 = \frac{\ln c_n k_0}{\sum_{i=0}^{d} C_{n-k_0}^i (q-1)n}.$$

Выясним, при каких $k_0$ справедливы неравенства $\delta_n^1 \ge \delta_n^2$ и $\delta_n^1 \le \delta_n^2$ соответственно.

Поскольку $C_{n+1}^i = C_n^i + C_n^{i-1}$, $\delta_n^2$ можно представить в виде

$$\delta_n^2 = \frac{\ln c_n k_0}{2\sum_{i=0}^{d} C_{n-k_0-1}^i - C_{n-k_0-1}^d}.$$

Установим, при каких $k_0$ выполняется неравенство

$$\frac{\ln c_n(n-k_0)}{\sum_{i=0}^{d} C_{n-k_0-1}^i} \le \frac{\ln c_n k_0}{2\sum_{i=0}^{d} C_{n-k_0-1}^i - C_{n-k_0-1}^d}. \tag{16}$$

Отсюда

$$(c_n(n-k_0))^{2\sum_{i=0}^{d} C_{n-k_0-1}^i - C_{n-k_0-1}^d} \le (c_n k_0)^{\sum_{i=0}^{d} C_{n-k_0-1}^i}$$

и, следовательно,

$$(c_n(n-k_0))^{2 - \frac{C_{n-k_0-1}^d}{2\sum_{i=0}^{d} C_{n-k_0-1}^i}} \le c_n k_0. \tag{17}$$

Однако, как вытекает из доказательства утверждения 2, $c_n^2(n-k_0)^2 \le c_n^2 k_0$, если $k_0 \ge n + \frac{1}{2c_n} - \sqrt{\frac{n}{c_n} + \frac{1}{4c_n^2}}$. Таким образом, при $k_0 \ge n + \frac{1}{2c_n} - \sqrt{\frac{n}{c_n} + \frac{1}{4c_n^2}}$ тем более выполняется неравенство (17), в силу которого $\delta_n^2 \ge \delta_n^1$. Кроме того, очевидно, если $k_0 \le \frac{n}{2}$, то $\delta_n^1 > \delta_n^2$. Остается выяснить, при каких $k_0$ выполняется (16), если известно, что

$$\frac{n}{2} < k_0 \le n + \frac{1}{2c_n} - \sqrt{\frac{n}{c_n} + \frac{1}{4c_n^2}}. \tag{18}$$

Решение последней задачи достаточно трудоемко. Поэтому для $k_0$, удовлетворяющих неравенствам (18), проще проверять выполнение либо неравенства (17), либо равносильного неравенства (16). Если выполняется (16) ((17)), то $\delta_n = \delta_n^2$, в противном случае $\delta_n = \delta_n^1$.

Таким образом, доказано следующее утверждение.

**Утверждение 3.** Пусть $d < n - k_0$. Тогда искомое $\delta_n$ принимает следующие значения:

а) $\delta_n = \delta_n^2 = \dfrac{\ln c_n k_0}{\sum\limits_{i=0}^{d} C_{n-k_0}^{i} (q-1)n}$, если $k_0 \ge n + \dfrac{1}{2c_n} - \sqrt{\dfrac{n}{c_n} + \dfrac{1}{4c_n^2}}$;

б) $\delta_n = \delta_n^1 = \dfrac{\ln c_n (n-k_0)}{\sum\limits_{i=0}^{d} C_{n-k_0-1}^{i} (q-1)n}$, если $k_0 \le \dfrac{n}{2}$;

в) $\delta_n = \max(\delta_n^1, \delta_n^2)$, если $\dfrac{n}{2} < k_0 < n + \dfrac{1}{2c_n} - \sqrt{\dfrac{n}{c_n} + \dfrac{1}{4c_n^2}}$.

Далее, используя лемму 1 из [5, § 8.3], нетрудно убедиться, что для системы (1) над произвольным коммутативным кольцом $\mathbf{R}$ с единицей в случае, когда ненулевые координаты $\mathbf{x}^0$ не являются делителями 0, аналогом утверждений 2, 3 будут следующие утверждения.

**Утверждение 4.** Пусть $d \ge n - k_0$. Тогда, если $k_0 \le n + \dfrac{1}{2c_n} - \sqrt{\dfrac{n}{c_n} + \dfrac{1}{4c_n^2}}$, искомое $\delta_n = \dfrac{l_0}{m(l_0 - 1)} \dfrac{\ln c_n (n-k_0)}{2^{n-k_0-1} n}$, в противном случае $\delta_n = \dfrac{l_0}{m(l_0-1)} \dfrac{\ln c_n k_0}{2^{n-k_0} k_0}$.

**Утверждение 5.** Пусть $d < n - k_0$. Тогда:

а) искомое $\delta_n = \delta_n^1 = \dfrac{l_0}{m(l_0-1)} \dfrac{\ln c_n k_0}{\sum\limits_{i=0}^{d} C_{n-k_0}^{i} n}$, если $k_0 \ge n + \dfrac{1}{2c_n} - \sqrt{\dfrac{n}{c_n} + \dfrac{1}{4c_n^2}}$;

б) искомое $\delta_n = \delta_n^2 = \dfrac{l_0}{m(l_0-1)} \dfrac{\ln c_n (n-k_0)}{\sum\limits_{i=0}^{d} C_{n-k_0}^{i} n}$, если $k_0 \le \dfrac{n}{2}$;

в) искомое $\delta_n = \max(\delta_n^1, \delta_n^2)$, если $\dfrac{n}{2} < k_0 < n + \dfrac{1}{2c_n} - \sqrt{\dfrac{n}{c_n} + \dfrac{1}{4c_n^2}}$.

2. Рассмотрим систему (2) над полем $\mathbf{GF}(q)$, в которой $d_i = d$, $i = \overline{1, n-s}$,

$$\sum_{k=1}^{d} \sum_{1 \le j_1 \le j_2 \le \ldots \le j_k \le n} a_{i, j_1 \ldots j_k} x_{j_1} \ldots x_{j_k} = \sum_{k=1}^{d} \sum_{1 \le j_1 \le j_2 \le \ldots \le j_k \le n} a_{i, j_1 \ldots j_k} x_{j_1}^0 \ldots x_{j_k}^0$$

и соответствующее ей выражение для $\mathbf{M}\nu_n$

$$\mathbf{M}\nu_n = \sum_{\mathbf{x} \ne 0} \prod_{i=1}^{n-s} \mathbf{P}(a_i(\mathbf{x}^0 + \mathbf{x}) - a_i(\mathbf{x}^0) = 0).$$

Здесь $\mathbf{x}^0$ то же, что и в п. 1.

Как и в п. 1, в зависимости от величины $k_0$ в выражении для $\mathbf{M}\nu_n$ выделим следующие частичные суммы:

а) если $k_0 \ne 0$, рассмотрим две частичные суммы: сумму $S_n^1$ по множеству векторов $\mathbf{x}$, у которых одна из первых $n - k_0$ координат отлична от 0, а остальные равны 0, и сумму $S_n^2$ по множеству векторов $\mathbf{x}$, у которых одна из последних $n - k_0$ координат отлична от 0, а остальные равны 0;

б) если $k_0 = 0$, рассматриваем одну сумму $S_n^1$, определенную в п. а).

**Подсчет числа ненулевых слагаемых в выражении $\mathbf{a}_i(\mathbf{x}^0 + \mathbf{x}) - \mathbf{a}_i(\mathbf{x}^0)$ для суммы $S_n^1$ при фиксированном $\mathbf{x}$.** Не ограничивая общности, полагаем, что первая координата $x_1$ в векторе $\mathbf{x}$ отлична от 0, а остальные $x_i = 0$, $i = \overline{2, n}$.

Поскольку в векторе $\mathbf{x}^0$ координаты $x^0_{n-k_0+1}=\ldots=x^0_n=0$, ненулевыми слагаемыми в $\mathbf{a}_i(\mathbf{x}^0+\mathbf{x})-\mathbf{a}_i(\mathbf{x}^0)$ в данном случае являются слагаемые вида $x_1^j(x_1^0)^{t_1-j}(x_2^0)^{t_2}\ldots(x^0_{n-k_0})^{t_{n-k_0}}$, где $j, t_1, \ldots, t_{n-k_0}$ — целые неотрицательные числа, при этом $1\le j\le t_1\le d$, $t_2+\ldots+t_{n-k_0}\le d-t_1$.

Поэтому выражение $\mathbf{a}_i(\mathbf{x}^0+\mathbf{x})-\mathbf{a}_i(\mathbf{x}^0)$ будет иметь вид

$$\mathbf{a}_i(\mathbf{x}^0+\mathbf{x})-\mathbf{a}_i(\mathbf{x}^0)=\sum_{t=1}^{d}\sum_{j,t_1,\ldots,t_{n-k_0}} x_1^j(x_1^0)^{t_1-j}(x_2^0)^{t_2}\ldots(x^0_{n-k_0})^{t_{n-k_0}}, \qquad (19)$$

где суммирование ведется по целым неотрицательным числам $j, t_1, \ldots, t_{n-k_0}$, удовлетворяющим условиям $1\le j\le t_1\le d$, $t_2+\ldots t_{n-k_0}=t\le d$.

Для подсчета числа слагаемых в последнем выражении для $\mathbf{a}_i(\mathbf{x}^0+\mathbf{x})-\mathbf{a}_i(\mathbf{x}^0)$ используем известную задачу о вычислении числа способов, посредством которых $t$ элементов можно разделить на $k$ групп, из которых первая содержит $t_1\ge 1$ элементов, вторая — $t_2$ элементов и т.д.

Очевидно, что число слагаемых в (19) равно

$$\alpha=\sum_{t=1}^{d}\sum_{\substack{t_1,\ldots,t_{n-k_0}\\ t_1\ge 1,\, t_1+\ldots+t_{n-k_0}=t}}\frac{t}{t_1\ \ldots\ t_{n-k_0}}\sum_{j=1}^{t_1}C_{t_1}^{j}=$$

$$=\sum_{t=1}^{d}\left[\sum_{\substack{t_1,\ldots,t_{n-k_0}\\ t_1\ge 1,\, t_1+\ldots+t_{n-k_0}=t}}2^{t_1}\frac{t}{t_1\ \ldots\ t_{n-k_0}}-\sum_{\substack{t_1,\ldots,t_{n-k_0}\\ t_1\ge 1,\, t_1+\ldots+t_{n-k_0}=t}}\frac{t}{t_1\ \ldots\ t_{n-k_0}}\right]=$$

$$=\sum_{t=1}^{d}[(n-k_0+1)^t-(n-k_0)^t]=$$

$$=\frac{(n-k_0+1)[(n-k_0+1)^d-1]}{n-k_0}-\frac{(n-k_0)[(n-k_0)^d-1]}{n-k_0-1}. \qquad (20)$$

**Подсчет числа ненулевых слагаемых в выражении $\mathbf{a}_i(\mathbf{x}^0+\mathbf{x})-\mathbf{a}_i(\mathbf{x}^0)$ для суммы $S_n^2$ при фиксированном x**. Не ограничивая общности, полагаем, что в векторе $\mathbf{x}$ координаты $x_1=\ldots=x_{n-k_0}=x_{n-k_0+2}=\ldots=x_n=0$ , а $x_{n-k_0+1}\ne 0$.

Тогда

$$\mathbf{a}_i(\mathbf{x}^0+\mathbf{x})-\mathbf{a}_i(\mathbf{x}^0)=\sum_{t=1}^{d}\sum_{t_1,\ldots,t_{n-k_0+1}}(x_1^0)^{t_1}\ldots(x^0_{n-k_0})^{n-k_0}x_{n-k_0+1}^{t_{n-k_0+1}}, \qquad (21)$$

где суммирование во второй сумме ведется по всем неотрицательным целым $t_1,\ldots,t_{n-k_0+1}$, причем $t_{n-k_0+1}\ge 1$, $t_1+\ldots+t_{n-k_0+1}=t$.

По построению все слагаемые в (21) ненулевые. Теперь нетрудно подсчитать их число. Действительно, используя задачу о разделении $t$ предметов на $n-k_0+1$ групп, из которых первая содержит $t_1$ элементов, вторая — $t_2$ и т.д., причем последняя $n-k_0+1$-я группа содержит $t_{n-k_0+1}\ge 1$ элементов, можно утверждать, что число слагаемых в сумме (21) равно

$$\sum_{t=1}^{d}\sum_{\substack{t_1,\ldots,t_{n-k_0}\\ t_{n-k_0+1}\ge 1,\, t_1+\ldots+t_{n-k_0+1}=t}}\frac{t}{t_1\ \ldots\ t_{n-k_0+1}}=$$

$$=\sum_{t=1}^{d}\left[\sum_{\substack{t_1,\ldots,t_{n-k_0}\\ t_1+\ldots+t_{n-k_0+1}=t}}\frac{t!}{t_1!\ldots t_{n-k_0+1}!}-\sum_{\substack{t_1,\ldots,t_{n-k_0}\\ t_1+\ldots+t_{n-k_0}=t}}\frac{t!}{t_1!\ldots t_{n-k_0}!}\right]=\sum_{t=1}^{d}[(n-k_0+1)^t-(n-k_0)^t],$$

что совпадает с числом ненулевых слагаемых в выражении $\mathbf{a}_i(\mathbf{x}^0+\mathbf{x})-\mathbf{a}_i(\mathbf{x}^0)$ для суммы $S_n^1$.

Таким образом, доказано следующее утверждение.

**Утверждение 6.** Для любого вектора **x**, у которого только одна ненулевая координата, число ненулевых слагаемых в соответствующем выражении $\mathbf{a}_i(\mathbf{x}^0+\mathbf{x})-\mathbf{a}_i(\mathbf{x}^0)$ — величина постоянная и вычисляется по формуле (20).

Нетрудно доказать следующее утверждение.

**Утверждение 7.** Частичная сумма по векторам **x**, у которых одна координата ненулевая, а остальные равны 0, в выражении для $\mathbf{M}\nu_n$ стремится к 0 при $n\to\infty$ тогда и только тогда, когда $\delta_n=\dfrac{\ln c_n n}{(q-1)\alpha n}$, где $\alpha$ определяется формулой (20).

Для системы (2) над коммутативным кольцом **R** с единицей в случае, когда $(\mathbf{I}_0)^2=\mathbf{I}_0\ \forall(\mathbf{I}_0)$ и ненулевые координаты вектора $\mathbf{x}^0$ не являются делителями 0, аналогом утверждения 7 является следующее утверждение.

**Утверждение 8.** Частичная сумма по векторам **x**, у которых одна координата ненулевая, а остальные равны 0, в выражении для $\mathbf{M}\nu_n$ стремится к 0 при $n\to\infty$ тогда и только тогда, когда $\delta_n=\dfrac{l_0}{m(l_0-1)}\dfrac{\ln c_n n}{\alpha n}$, где $\alpha$ определяется формулами (20).

На основании результатов, полученных в пп. 1, 2 для системы (1) ((2)) над коммутативным кольцом с единицей в случае, когда $(\mathbf{I}_0)^2=\mathbf{I}_0\ \forall(\mathbf{I}_0)$ и ненулевые координаты вектора $\mathbf{x}^0$ не являются делителями 0, справедливы следующие теоремы.

**Теорема 8.** Для системы (1) границей области инвариантности $\lim\limits_{n\to\infty}\mathbf{M}(\nu_n)_r$ для любого натурального $r$ является величина $\delta_n$, определяемая в утверждениях 4, 5.

**Теорема 9.** Для системы (2) границей области инвариантности $\lim\limits_{n\to\infty}\mathbf{M}(\nu_n)_r$ для любого натурального $r$ является величина $\delta_n$, определяемая в утверждении 8.

Поскольку для биномиальных моментов случайной величины $\nu_n$ выполняются условия теоремы 2 [10, с. 261], справедливы следующие теоремы.

**Теорема 10.** Для системы (1) величина $\delta_n$, определяемая в утверждении теоремы 8, в данной терминологии, является границей области инвариантности предельного распределения случайной величины $\nu_n$, когда $n\to\infty$.

**Теорема 11.** Для системы (2) величина $\delta_n$, определяемая в утверждении теоремы 9, в данной терминологии, является границей области инвариантности предельного распределения случайной величины $\nu_n$, когда $n\to\infty$.

И наконец, в силу полученных результатов имеет место следующая теорема.

**Теорема 12.** Условия (11), в которых $\delta_n$ определяется теоремами 8, 9, являются необходимыми и достаточными для справедливости теорем 1–4 и их следствий.

Сформулированные выше теоремы касаются определенных видов **R** и $\mathbf{x}^0$. Формулировка их в общем случае, т.е. для произвольных **R** и $\mathbf{x}^0$, слишком громоздка, хотя для каждой конкретной пары $(\mathbf{R},\mathbf{x}^0)$ определить искомое $\delta_n$ в (11) для систем (1), (2) соответственно не представляет трудностей. Действительно, в силу теоремы 7 искомое $\delta_n$ соответствует некоторому ненулевому идеалу $\mathbf{I}_0^*$ минимальной мощности. При этом очевидно, что $\mathbf{I}_0^*$ должен быть таким, чтобы число ненулевых слагаемых в выражении $\mathbf{a}_i(\mathbf{x}^0+\mathbf{x})-\mathbf{a}_i(\mathbf{x}^0)$, где $\mathbf{x}^0\in\mathbf{N}_{\mathbf{I}_0^*}$ и в $\mathbf{x}^0$ все координаты кроме одной равны 0, было не больше, чем в аналогичных выражениях для других $\mathbf{I}_0$. Таким образом, выбор $\mathbf{I}_0^*$ из множества ненулевых идеалов $\mathbf{I}_0$ полностью зависит от алгебраических свойств как самого кольца **R**, так и набора ненулевых координат вектора $\mathbf{x}^0$.

Например, если в $\mathbf{R}$ найдется идеал $\mathbf{I}_0$, для которого $(\mathbf{I}_0)^2 = \mathbf{I}_0$ и при этом $\mathbf{x}^0 = (z_1^0 \ldots z_{n-k_0}^0 0 \ldots 0)$ такой, что

$$z_i y = 0, \quad y \in \mathbf{I}_0, \quad i = \overline{1, n-k_0}, \tag{22}$$

то указанный $\mathbf{I}_0$ следует выбрать в качестве $\mathbf{I}_0^*$. Легко показать, что в этом случае для системы (1) и для системы (2) искомое $\delta_n$ определяется формулой (4). Если $(\mathbf{I}_0)^2 = \mathbf{I}_0$ для любого идеала $\mathbf{I}_0$ и при этом существует $\mathbf{I}_0$, для которого выполняются соотношения (22), то последний и равен $\mathbf{I}_0^*$. В этом случае для системы (1) искомое $\delta_n$ равно (4), а для системы (2) определяется формулой (5).

СПИСОК ЛИТЕРАТУРЫ


1. Коваленко И.Н. О предельном распределении числа решений случайной системы линейных уравнений в классе булевых функций // Теория вероятностей и ее применения. — 1967. — **12**, вып. 1. — С. 51–61.
2. Левитская А.А. Системы случайных уравнений над конечными алгебраическими структурами // Кибернетика и системный анализ. — 2005. — № 4. — С. 82–116.
3. Коваленко И.Н. Об одной предельной теореме для определителей в классе булевых функций // Докл. АН СССР. — 1965. — **161**, № 3. — С. 517–519.
4. Коваленко И.Н. О распределении для случайных булевых матриц // Кибернетика. — 1975. — № 5. — С. 138–152.
5. Коваленко И.Н., Левитская А.А., Савчук М.Н. Избранные задачи вероятностной комбинаторики. — Киев: Наук. думка, 1986. — 223 с.
6. Масол В.И. Теорема о предельном распределении числа ложных решений системы нелинейных случайных булевых уравнений // Теория вероятностей и ее применения. — 1998. — **43**, вып. 1. — С. 41–56.
7. Масол В.И. Некоторые вероятностные свойства нелинейных случайных булевых уравнений // Обозрение прикл. и промышл. математики. — 1998. — **5**, вып. 2. — С. 252–253.
8. Левитская А.А. Теоремы инвариантности для одного класса нелинейных систем уравнений над произвольным конечным полем // Кибернетика и системный анализ. — 1996. — № 2. — С. 103–112.
9. Левитская А.А. Теоремы инвариантности для одного класса систем случайных нелинейных уравнений над произвольным конечным кольцом с левой единицей // Там же. — 2008. — № 6. — С. 106–115.
10. Сачков В.Н. Введение в комбинаторные методы дискретной математики. — М.: Наука, 1982. — 384 с.


*Поступила 22.12.2009*