УДК 519.21

А.А. ЛЕВИТСКАЯ

ТЕОРЕМЫ ИНВАРИАНТНОСТИ ДЛЯ ОДНОГО КЛАССА СИСТЕМ СЛУЧАЙНЫХ НЕЛИНЕЙНЫХ УРАВНЕНИЙ НАД ПРОИЗВОЛЬНЫМ КОНЕЧНЫМ КОЛЬЦОМ С ЛЕВОЙ ЕДИНИЦЕЙ

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

Пусть $\boldsymbol{R}$ — произвольное конечное кольцо с левой единицей. Будем считать, что $\boldsymbol{R} \neq \mathbf{GF}(2)$. Рассмотрим над $\boldsymbol{R}$ систему уравнений

$$\sum_{k=1}^{d_i} \sum_{1 \le j_1 \le j_2 \le \ldots \le j_k \le n} a_{i, j_1 \ldots j_k} x_{j_1} \cdot \ldots \cdot x_{j_k} = 0, \; i = \overline{1, n-s}, \tag{1}$$

и дополнительно к ней, в случае некоммутативности $\boldsymbol{R}$, еще одну систему

$$\sum_{k=1}^{d_i} \sum_{1 \le j_1, j_2, \ldots, j_k \le n} a_{i, j_1 \ldots j_k} x_{j_1} \cdot \ldots \cdot x_{j_k} = 0, \; i = \overline{1, n-s}, \tag{1′}$$

где s — целочисленная константа произвольного знака, $a_{i, j_1 \ldots j_k}$ — независимые в совокупности случайные величины, d_i, $2 \le d_i \le n$; $i = \overline{1, n-s}$, — натуральные числа.

Для сокращения записи исследования систем (1) и (1′) проведем одновременно. Если при этом будут возникать различия между соответствующими понятиями и теоретическими выводами, касающимися (1) и (1′), то условимся отмечать их необходимыми комментариями.

Пусть ν_n — число решений (1) ((1′)), отличных от нулевого вектора $\mathbf{0} = (0 \ldots 0)$.

В данной работе системы (1), (1′) исследуются при условии, что распределения случайных величин $a_{i, j_1 \ldots j_k}$ удовлетворяют ограничениям

$$\frac{l_0}{m(l_0 - 1)} \cdot \frac{\ln c_n \, n}{n} = \delta_n \le \mathbf{P}\,(a_{i, j_1 \ldots j_k} = z), \; z \in \boldsymbol{R}, \tag{2}$$

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

где l_0 — число, равное наименьшей из мощностей ненулевых левых идеалов $\boldsymbol{R}$, m — мощность кольца $\boldsymbol{R}$, c_n — произвольная последовательность, стремящаяся к ∞ при $n \to \infty$. Цель работы — при данных характеристиках системы (1) ((1′)) и при условии, что $n \to \infty$, установить вид предельных факториальных моментов ν_n и на основании полученных результатов исследовать вопрос о предельном распределении ν_n, а также описать геометрическую структуру множества решений (1) ((1′)).

В работе [1] аналогичная задача решена для случая системы (1) над $\boldsymbol{R} = \mathbf{GF}(q)$, где область суммирования под знаком второй суммы (1) имеет вид $1 \le j_1 < j_2 < \ldots < j_k \le n$, $k = \overline{1, d_i}$, $i = \overline{1, n-s}$.

Как и в [1], наряду с системами (1), (1′) введем соответствующую им линейную систему

$$\sum_{j=1}^{n} a_{i,j} \, x_j = 0, \; i = \overline{1, n-s}, \tag{3}$$

где $a_{i,j}$, $i = \overline{1, n-s}$, $j = \overline{1, n}$, — независимые в совокупности случайные величины,

распределения которых удовлетворяют ограничениям, аналогичным (2), т.е.

$$\frac{l_{\mathbf{0}}}{m(l_0-1)}\cdot\frac{\ln c_n\ n}{n}=\delta_n\le\mathbf{P}(a_{i,j}=z),\ z\in\boldsymbol{R},\ \ i=\overline{1,n-s},\ \ j=\overline{1,n}. \tag{4}$$

В дальнейшем будем использовать следующие обозначения: ν_{0n} — число ненулевых решений (3); $\boldsymbol{R}^r=\underbrace{\boldsymbol{R}\times\ldots\times\boldsymbol{R}}_{r}$ — векторное пространство над $\boldsymbol{R}$, элементами которого являются r-мерные векторы-столбцы; $\boldsymbol{u}=\begin{pmatrix}u_1\\.\\.\\.\\u_r\end{pmatrix}$ (возможны индексы вверху) — элемент $\boldsymbol{R}^r$; $\mathbf{0}$ — единица аддитивной группы $\boldsymbol{R}^r$; $\boldsymbol{I}$ (возможны индексы внизу) — некоторый левый идеал $\boldsymbol{R}$; $\boldsymbol{I}^r=\left\{\begin{pmatrix}z_1\\.\\.\\.\\z_r\end{pmatrix},z_i\in\boldsymbol{I},i=\overline{1,r}\right\}$ — r-мерное векторное пространство над $\boldsymbol{I}$; $\boldsymbol{I}_1\times\boldsymbol{I}_2\times\ldots\times\boldsymbol{I}_t=\left\{\begin{pmatrix}z_1\\.\\.\\.\\z_t\end{pmatrix},z_i\in\boldsymbol{I_i},i=\overline{1,t}\right\}$; $\boldsymbol{I}\cdot\boldsymbol{I}=\{z_1\cdot z_2:$ $z_1,z_2\in\boldsymbol{I}\}$; $\boldsymbol{M}_r$ (возможны индексы вверху) — некоторый левый подмодуль $\boldsymbol{R}^r$; $\boldsymbol{u}^1\cdot\boldsymbol{u}^2=\begin{pmatrix}u_1^1\ u_1^2\\.\\.\\.\\u_r^1\ u_r^2\end{pmatrix}$, $\boldsymbol{u}^1,\boldsymbol{u}^2\in\boldsymbol{R}^r$; $z\boldsymbol{u}^2=\begin{pmatrix}z\ u_1\\.\\.\\.\\z\ u_r\end{pmatrix}$, $\boldsymbol{u}\in\boldsymbol{R}^r$; $(\boldsymbol{M}_r)^2=\{u\cdot v:\ u,v\in\boldsymbol{M}_r\}$; $\boldsymbol{x}=(x_1,\ldots,x_n)$ (возможны индексы вверху) — n-мерный вектор, координаты которого являются элементами $\boldsymbol{R}$; $\boldsymbol{X}_r=\begin{pmatrix}\boldsymbol{x}^1\\.\\.\\.\\\boldsymbol{x}^r\end{pmatrix}=\begin{pmatrix}x_1^1&.&.&.&x_n^1\\.&.&.&.&.\\.&.&.&.&.\\.&.&.&.&.\\x_r^1&.&.&.&x_n^r\end{pmatrix}$;

$\boldsymbol{a}_i\boldsymbol{X}_r=\sum\limits_{k=1}^{d_i}\sum\limits_{\Im}a_{i,j_1\ldots j_k}\begin{pmatrix}x_{j_1}^1&x_{j_2}^1&.&.&.&x_{j_k}^1\\.&.&.&.&.&.\\x_{j_1}^r&x_{j_2}^r&.&.&.&x_{j_k}^r\end{pmatrix}$, $i=\overline{1,n-s}$, где область суммирования $\Im=\{1\le j_1\le..\le j_k\le n\}$ в случае системы (1) и $\Im=\{1\le j_1,\ldots,j_k\le n\}$ для системы (1′); $\boldsymbol{a}_i^0\boldsymbol{X}_r=\sum\limits_{j=1}^{n}a_{i,j}\begin{pmatrix}x_j^1\\.\\.\\.\\x_j^r\end{pmatrix}$, $i=\overline{1,n-s}$;

$$\boldsymbol{N}_{\boldsymbol{M}_r}=\left\{\boldsymbol{X}_r\colon \left\{\sum_{j=1}^{n}\alpha_j\begin{pmatrix}x_j^1\\ .\\ .\\ .\\ x_j^r\end{pmatrix}+\sum_{j=1}^{n}n_j\begin{pmatrix}x_j^1\\ .\\ .\\ .\\ x_j^r\end{pmatrix},\ \alpha_j\in\boldsymbol{R},\ n_j\in\boldsymbol{Z}^+,\ j=\overline{1,n}\right\}\right\}=\boldsymbol{M}_r,\quad \text{т.е.}$$

$\boldsymbol{N}_{\boldsymbol{M}_r}$ — множество матриц $\boldsymbol{X}_r$, столбцы каждой из которых порождают модуль $\boldsymbol{M}_r$ (отметим, что в последних трех выражениях сложение и умножение под знаком суммы производится покомпонентно по модулю m); $\xi_i(\boldsymbol{X}_r)\cdot(\xi_i^{(0)}(\boldsymbol{X}_r))$ — индикатор события $\{\boldsymbol{a}_i\boldsymbol{X}_r=\boldsymbol{0}\}$ ($\{\boldsymbol{a}_i^{(0)}\boldsymbol{X}_r=\boldsymbol{0}\}$), $i=\overline{1,n-s}$, $|\boldsymbol{T}|$ — мощность множества $\boldsymbol{T}$; $k_{\boldsymbol{u}}(\boldsymbol{X}_r)=\left|\left\{j\colon\begin{pmatrix}x_j^1\\ .\\ .\\ .\\ x_j^r\end{pmatrix}=\boldsymbol{u},\ j=\overline{1,n}\right\}\right|$, $\boldsymbol{u}\in\boldsymbol{R}^r$; $\nu_{n\boldsymbol{M}_r}=\left|\boldsymbol{X}_r\in\boldsymbol{N}_{\boldsymbol{M}_r}\colon\prod_{i=1}^{n-s}\xi_i(\boldsymbol{X}_r)=1\right|$;

$\nu_{0n\boldsymbol{M}_r}=\left|\boldsymbol{X}_r\in\boldsymbol{N}_{\boldsymbol{M}_r}\colon\prod_{i=1}^{n-s}\xi_i^{(0)}(\boldsymbol{X}_r)=1\right|$.

Условимся впредь считать, что все арифметические операции над элементами $\boldsymbol{R}^r$ производятся по модулю m, те же операции над величинами, не являющимися элементами $\boldsymbol{R}^r$, — это обычные операции в поле действительных чисел.

Напомним некоторые результаты из [2, гл. 9], которые предполагаем использовать существенно в наших рассуждениях относительно системы (1) ((1′)).

Итак, в [2, гл. 9] доказано, что для системы (3) условия (4) в данной терминологии являются границей области инвариантности для предельного распределения случайной величины ν_{0n} и предела любого конечного момента $\mathbf{M}\nu_{0n}^r$ (r — натуральное число), когда $n\to\infty$, причем предельное распределение ν_{0n} и $\lim\limits_{n\to\in\infty}\mathbf{M}\nu_{0n}^r$ имеют соответственно те же значения, что и в случае $\mathbf{P}(a_{i,j}^{(0)}=z)=m^{-1}$, $z\in\boldsymbol{R}$, $i=\overline{1,n-s}$, $j=\overline{1,n}$. Кроме того, здесь также установлены следующие выражения для $\mathbf{M}\nu_{0n}^r$ и $\lim\limits_{n\to\infty}\mathbf{M}\nu_{0n}^r$:

$$\mathbf{M}\nu_{0n}^r=\sum_{\boldsymbol{M}_r\subseteq\boldsymbol{R}^r}\mathbf{M}\nu_{0n\boldsymbol{M}_r}^r=\sum_{\boldsymbol{M}_r\subseteq\boldsymbol{R}^r}\sum_{\boldsymbol{X}_r\in\boldsymbol{N}_{\boldsymbol{M}_r}}\mathbf{M}\prod_{i=1}^{n-s}\xi_i^0(\boldsymbol{X}_r)\underset{n\to\infty}{\sim}$$

$$\underset{n\to\infty}{\sim}\sum_{\boldsymbol{M}_r\subseteq\boldsymbol{R}^r}\sum_{\substack{\boldsymbol{X}_r\in\boldsymbol{N}_{\boldsymbol{M}_r}\\ \boldsymbol{X}_r\colon k_{\boldsymbol{u}}(\boldsymbol{X}_r)\sim\frac{n}{\boldsymbol{M}_r},\ \boldsymbol{u}\in\boldsymbol{M}_r}}\prod_{i=1}^{n-s}\mathbf{P}(\boldsymbol{a}_i^{(0)}\boldsymbol{X}_r=\boldsymbol{0})= \tag{5}$$

$$=\sum_{\boldsymbol{M}_r\subseteq\boldsymbol{R}^r}\sum_{\substack{k_{\boldsymbol{u}}(\boldsymbol{X}_r)\sim\frac{n}{|\boldsymbol{M}_r|},\ \boldsymbol{u}\in\boldsymbol{M}_r\\ \sum_{\boldsymbol{u}\in\boldsymbol{M}_r}k_{\boldsymbol{u}}=n}}\frac{n!}{\prod_{\boldsymbol{u}\in\boldsymbol{M}_r}k_{\boldsymbol{u}}}\cdot|\boldsymbol{M}_r|^{-(n-s)}[1+o(c_n^{-1})]\xrightarrow[n\to\infty]{}$$

$$\xrightarrow[n\to\infty]{}\sum_{\boldsymbol{M}_r\subseteq\boldsymbol{R}^r}|\boldsymbol{M}_r|^s=\lim_{n\to\infty}\mathbf{M}\nu_{0n}^r,$$

где суммирование ведется по всем левым подмодулям $\boldsymbol{M}_r$ модуля $\boldsymbol{R}^r$ и по всем матрицам $\boldsymbol{X}_r\in\boldsymbol{N}_{\boldsymbol{M}_r}$.

Как и в [1], вероятностный анализ системы (1) ((Г)) 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

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

где суммирование ведется по различным матрицам $\boldsymbol{X}_r$, все строки которых отличны от нулевого вектора и друг от друга.

Для вычисления $\mathbf{M}(\nu_n)_r$ используем подход, предложенный в [2, гл. 9] для вычисления $\mathbf{M}\nu_{0n}^r$.

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

$\overset{\text{def}}{=}\begin{pmatrix} u_1^1 & \ldots & u_1^{|\boldsymbol{M}_r|} \\ \ldots & \ldots & \ldots \\ u_r^1 & \ldots & u_r^{|\boldsymbol{M}_r|} \end{pmatrix}$ которых все строки различны и отличны от (0…0).

Теперь перепишем правую часть (6):

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

$$= \sum_{\boldsymbol{M}_r\in\boldsymbol{K}_r}\sum_{\boldsymbol{X}_r\in\boldsymbol{N}_{\boldsymbol{M}_r}}\mathbf{M}\prod_{i=1}^{n-s}\mathbf{P}(\boldsymbol{a}_i\boldsymbol{X}_r=\boldsymbol{0}). \tag{7}$$

Для модулей из $\boldsymbol{K}_r$ введем понятия расширяемости и нерасширяемости.

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

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

Примерами нерасширяемых модулей в $\boldsymbol{K}_r$ являются все модули вида $\boldsymbol{I}_1\times\boldsymbol{I}_2\times\ldots\times\boldsymbol{I}_k$, где $\boldsymbol{I}_j$, $j=\overline{1,k}$, — левые идеалы кольца, $\boldsymbol{R}$ среди последних могут встречаться как одинаковые, так и совпадающие с самим кольцом $\boldsymbol{R}$. Однако, помимо нерасширяемых модулей указанного вида в случае $\boldsymbol{R}\neq\mathbf{GF}(q)$, в $\boldsymbol{R}^r$ существуют и другие нерасширяемые модули.

Пример 1. Рассмотрим в качестве $\boldsymbol{R}$ кольцо $\boldsymbol{Z}_4=\{0,1,2,3\}$ вычетов по модулю 4. $\boldsymbol{R}$ имеет единственный, отличный от самого $\boldsymbol{R}$, ненулевой идеал $\boldsymbol{I}=\{0,2\}$. Легко проверить, что нерасширяемыми собственными подмодулями модуля $\boldsymbol{Z}_4^2$ являются следующие элементы из $\boldsymbol{K}_2$:

$$\boldsymbol{M}_1=\left\{\begin{pmatrix}1\\3\end{pmatrix},\begin{pmatrix}2\\2\end{pmatrix},\begin{pmatrix}3\\1\end{pmatrix},\begin{pmatrix}3\\3\end{pmatrix},\begin{pmatrix}0\\2\end{pmatrix},\begin{pmatrix}1\\1\end{pmatrix}\begin{pmatrix}2\\0\end{pmatrix},\begin{pmatrix}0\\0\end{pmatrix}\right\},\ \boldsymbol{M}_2=\boldsymbol{I}^2,\ \boldsymbol{M}_3=\boldsymbol{I}\times\boldsymbol{Z}_4,\ \boldsymbol{M}_4=\boldsymbol{Z}_4\times\boldsymbol{I}.$$

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

На основании леммы 1 [1] справедливо следующее утверждение.

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

В [1] последнее утверждение играет ключевую роль при обосновании сходимости распределения числа ν_n ненулевых решений системы (1) над $\boldsymbol{R}=\mathbf{GF}(q)$, где

область суммирования под знаком второй суммы в (1) имеет вид $1 \le j_1 < j_2 < \ldots$ $\ldots < j_k \le n$, $k = \overline{1, d_i}$, $i = \overline{1, n-s}$, к закону Пуассона, когда $n \to \infty$. Для конечных колец $\boldsymbol{R} \ne \mathbf{GF}(2)$, как показывает пример 1, утверждение 1 не имеет места, поэтому здесь следует ожидать иных результатов, отличных от установленых в [1].

Зафиксируем некоторую матрицу $\boldsymbol{X}_r \in \boldsymbol{N}_{\boldsymbol{M}_r}$, $\boldsymbol{M}_r \in \boldsymbol{K}_r^0$. Обозначим $\boldsymbol{X}'_{ri}$ матрицу, полученную из $\boldsymbol{X}_r$ добавлением столбцов вида

$$\begin{matrix} x^1_{j_1} & \cdot & \cdot & \cdot & \cdot & x^1_{j_k} \\ \cdot & & \cdot & \cdot & \cdot & \cdot \\ \cdot & & \cdot & \cdot & \cdot & \cdot \\ \cdot & & \cdot & \cdot & \cdot & \cdot \\ x^r_{j_1} & \cdot & \cdot & \cdot & \cdot & x^r_{j_k} \end{matrix},$$

где $1 \le j_1 \le .. \le j_k \le n$, $k = \overline{1, d_i}$, если речь идет о системе (1), и $1 \le j_1, \ldots, j_k \le n$, $i = \overline{k, d_i}$, в случае системы (1'), $i = \overline{1, n-s}$. Поскольку $\boldsymbol{M}_r \in \boldsymbol{K}_r^0$, то $\boldsymbol{X}'_r \in \boldsymbol{N}_{\boldsymbol{M}_r}$, $i = \overline{1, n-s}$.

Если же $\boldsymbol{X}_r \in \boldsymbol{N}_{\boldsymbol{M}_r}$, где $\boldsymbol{M}_r \notin \boldsymbol{K}_r^0$, то, очевидно, $\boldsymbol{X}'_{ri} \in \boldsymbol{N}_{\boldsymbol{M}'_{ri}}$, где $\boldsymbol{M}'_{ri}$ — некоторый подмодуль $\boldsymbol{R}^r$, порождаемый столбцами матрицы $\boldsymbol{X}'_{ri} \in \boldsymbol{N}_{\boldsymbol{M}'_r}$, для которого $\boldsymbol{M}_r$ является собственным подмодулем, т.е. $\boldsymbol{M}_{ri} \subset \boldsymbol{M}'_r$, $i = \overline{1, n-s}$.

Принимая во внимание только что сказанное, не представляет труда доказать следующие леммы.

Лемма 1. Если $\boldsymbol{M}_r \in \boldsymbol{K}_r^0$, то

$$\lim_{n \to \infty} \mathbf{M} \nu_{n \boldsymbol{M}_r} = \left| \boldsymbol{M}_r \right|^s.$$

Доказательство. Пусть $\boldsymbol{M}_r \in \boldsymbol{K}_r^0$. На основании теоремы 1 и примеров, приведенных в [2] (гл. 8, §§ 8.2, 8.3), для $\mathbf{P}(\boldsymbol{a}_i \boldsymbol{X}_r = \mathbf{0})$, $i = \overline{1, n-s}$, где $\boldsymbol{X}_r \in \boldsymbol{N}_{\boldsymbol{M}_r}$ и $\boldsymbol{X}'_{ri} \in \boldsymbol{N}_{\boldsymbol{M}_r}$, $i = \overline{1, n-s}$, справедливы следующие оценки:

$$\min_{\{\mathbf{P}(a_{ij} = z)\}} \mathbf{P}(\boldsymbol{a}_i^{(0)} \boldsymbol{X}_r = \mathbf{0}) \le \mathbf{P}(\boldsymbol{a}_i \boldsymbol{X}_r = \mathbf{0}) \le \max_{\{\mathbf{P}(a_{ij} = z)\}} \mathbf{P}(\boldsymbol{a}_i^{(0)} \boldsymbol{X}_r = \mathbf{0}), \qquad (8)$$

где min и max берутся по всем распределениям случайных величин a_{ij}, $i = \overline{1, n-s}$, $j = \overline{1, n-s}$, удовлетворяющим условиям (4). В силу (5), (7), (8)

$$\mathbf{M}\nu_{n\boldsymbol{M}_r} = \sum_{\boldsymbol{X}_r \in \boldsymbol{N}_{\boldsymbol{M}_r}} \prod_{i=1}^{n-s} \mathbf{P}\left(a_i \boldsymbol{X}_r = \mathbf{0}\right)_{n \tilde{\to} \infty}$$

$$n \tilde{\to} \infty \qquad \sum_{\boldsymbol{X}_r \in \boldsymbol{N}_{\mathbf{M}_r}} \prod_{i=1}^{n-s} \mathbf{P}(\boldsymbol{a}_i^{(0)} \boldsymbol{X}_r = \mathbf{0})_{n \tilde{\to} \infty} \left| \boldsymbol{M}_r \right|^s, \qquad (9)$$

$$\boldsymbol{X}_r : k_{\boldsymbol{u}}(\boldsymbol{X}_r) \sim \frac{n}{\boldsymbol{M}_r},\ \boldsymbol{u} \in \boldsymbol{M}_r$$

что и требовалось доказать.

Лемма 2. Для любого расширяемого модуля $\boldsymbol{M}_r \in \boldsymbol{K}_r \setminus \boldsymbol{K}_r^0$ имеет место соотношение $\lim_{n \to \infty} \mathbf{M} \nu_{n \boldsymbol{M}_r} = 0$.

Доказательство. В силу (7), (8) для $\mathbf{M}\nu_{n\boldsymbol{M}_r}$ имеют место следующие оценки:

$$0 \le \mathbf{M}\nu_{n\boldsymbol{M}_r} = \sum_{\boldsymbol{X}_r \in \boldsymbol{N}_{\boldsymbol{M}_r}} \mathbf{M} \prod_{i=1}^{n-s} \mathbf{P}\left(\boldsymbol{a}_i \boldsymbol{X}_r = \mathbf{0}\right) \underset{n \to \infty}{\lesssim}$$

$$\lesssim_{n\to\infty} \sum_{\boldsymbol{X}_r \in \boldsymbol{N}_{\boldsymbol{M}_r}} \prod_{i=1}^{n-s} \mathbf{P}(\boldsymbol{a}_i^{(0)} \boldsymbol{X}_r = \mathbf{0}) +$$

$$\boldsymbol{X}_r : \exists (\boldsymbol{u} \in \boldsymbol{M}_r) k_{\boldsymbol{u}}(\boldsymbol{X}_r) \not\sim_{n\to\infty} \frac{n}{|\boldsymbol{M}_r|}$$

$$+ \sum_{\boldsymbol{X}_r \in \boldsymbol{N}_{\boldsymbol{M}_r}} \prod_{i=1}^{n-s} \mathbf{P}(\boldsymbol{a}_i \boldsymbol{X}_r = \mathbf{0}). \qquad (10)$$

$$\boldsymbol{X}_r : k_u(\boldsymbol{X}_r) \sim_{n\to\infty} \frac{n}{|\boldsymbol{M}_r|},\ \boldsymbol{u} \in \boldsymbol{M}_r$$

Согласно (5) первая сумма в правой части выражения (10) при $n \to \infty$ стремится к 0, а что касается второй, то, поскольку для любого $i = \overline{1, n-s}$ $\boldsymbol{X}'_{ri} \in \boldsymbol{N}_{\boldsymbol{M}'_{ri}}$, где $\boldsymbol{M}'_{ri}$ — некоторый модуль, для которого модуль $\boldsymbol{M}_r$ является собственным подмодулем, вероятность $\mathbf{P}(\boldsymbol{a}_i \boldsymbol{X}_r = \mathbf{0}) \sim_{n\to\infty} |\boldsymbol{M}'_{ri}|^{-1} [1 + O(c_n^{-1} n^{-1})]$. Поэтому и в силу неравенства $|\boldsymbol{M}_r| < |\boldsymbol{M}'_{ri}|$ вторая сумма при $n \to \infty$ стремится к значению $\left(|\boldsymbol{M}_r|^n \cdot \prod_{i=1}^{n-s} |\boldsymbol{M}'_{ri}|^{-1} \right) [1 + O(c_n^{-1})] \xrightarrow[n\to\infty]{} 0$. Таким образом, утверждение доказано.

Леммы 1 и 2 позволяют перейти к доказательству следующих основных результатов данной работы.

Теорема 1. При выполнении условий (2) для любого натурального r

$$\lim_{n\to\infty} \mathbf{M}(\nu_n)_r = \sum_{\boldsymbol{M}_r \in \boldsymbol{K}_r^0} |\boldsymbol{M}_r|^s. \qquad (11)$$

Доказательство. Согласно (7)

$$\mathbf{M}(\nu_n)_r = \sum_{\boldsymbol{M}_r \in \boldsymbol{K}_r^0} \mathbf{M}\nu_{n\boldsymbol{M}_r} + \sum_{\boldsymbol{M}_r \in \boldsymbol{K}_r \setminus \boldsymbol{K}_r^0} \mathbf{M}\nu_{n\boldsymbol{M}_r}. \qquad (12)$$

На основании леммы 2 вторая сумма в (12) при $n \to \infty$ стремится к 0, а в силу леммы 1 сумма $\sum_{\boldsymbol{M}_r \in \boldsymbol{K}_r^0} \mathbf{M}\nu_{n\boldsymbol{M}_r} \xrightarrow[n\to\infty]{} \sum_{\boldsymbol{M}_r \in \boldsymbol{K}_r^0} |\boldsymbol{M}_r|^s$, что и доказывает (11).

Следствие 1. При выполнении условий (2) для любого набора $\boldsymbol{x}^1, \ldots, \boldsymbol{x}^r$ нетривиальных и отличных друг от друга решений системы (1) ((1′)) с вероятностью, стремящейся к 1 при $n \to \infty$, существует модуль $\boldsymbol{M}_r \in \boldsymbol{K}_r^0$ такой, что соответствующая матрица $\boldsymbol{X}_r = \begin{pmatrix} \boldsymbol{x}^1 \\ \cdot \\ \cdot \\ \cdot \\ \boldsymbol{x}^r \end{pmatrix} \in \boldsymbol{N}_{\boldsymbol{M}_r}$ и при этом $\mathbf{k}_{\boldsymbol{u}}(\boldsymbol{X}_r) \sim_{n\to\infty} \frac{n}{|\boldsymbol{M}_r|}$, $\boldsymbol{u} \in \boldsymbol{M}_r$.

Замечание. Для случая $\boldsymbol{R} = \mathbf{GF}(q)$ в [1] доказано, что при $n \to \infty$ распределение случайной величины ν_n стремится к закону Пуассона с параметром q^s. Данный результат следует из того, что $\lim_{n\to\infty} \mathbf{M}(\nu_n)_r = q^{sr}$, где r — фиксированное натуральное число. Если же $\boldsymbol{R} \neq \mathbf{GF}(q)$, то в $\boldsymbol{R}$ существует хотя бы один левый идеал, отличный от $\boldsymbol{R}$ и $\{0\}$. В силу своего определения идеалы $\boldsymbol{R}$ (и только они!) являются нерасширяемыми подмодулями $\boldsymbol{R}$. Поэтому $\lim_{n\to\infty} \mathbf{M}(\nu_n)_{\mathbf{1}} = \lim_{n\to\infty} \mathbf{M}\nu_n = \sum_{\boldsymbol{I} \subseteq \boldsymbol{R}} |\boldsymbol{I}|^s$, где суммирование ведется по всем левым идеалам кольца $\boldsymbol{R}$. Далее, на основании (11)

$\lim\limits_{n\to\infty} \mathbf{M}(\nu_n)_2 = \sum\limits_{M_2\subseteq K_2^0} |M_2|^s$. Однако $\sum\limits_{M_2\subseteq K_2^0} |M_2|^s \neq \left(\sum\limits_{I\subseteq R} |I|^s\right)^2$, поскольку R — кольцо и, как видно из примера 1, K_2^0 помимо модулей вида $I_1 \times I_2$, где I_1, I_2 пробегают множество левых идеалов R, отличных от $\{0\}$, содержит нерасширяемые модули и иного вида. Отсюда следует, что для $R \neq \mathbf{GF}(q)$ распределение случайной величины ν_n при $n\to\infty$ не может стремиться к закону Пуассона. Тем не менее для решений определенного вида закон Пуассона имеет место и в случае $R \neq GF(q)$.

Предположим, что в R существуют идеалы, изоморфные полям. Выделим их: $\{I_{01},\ldots,I_{0t}\} = D_0$. Относительно таких идеалов справедливы следующие теоремы.

Теорема 2. Если выполнены условия (2), то для любого конечного r

$$\lim_{n\to\infty} \mathbf{M}(\nu_{n I_{0i}})_r = |I_{0i}|^{rs}, \quad i=\overline{1,t}. \tag{13}$$

Доказательство. Доказательство теоремы 2 аналогично доказательству соответствующего утверждения для случая $R = \mathbf{GF}(q)$, приведенного в [1].

Следствие 2. Для каждого фиксированного $i, i=\overline{1,t}$, при выполнении условий (2) для любого набора $x^1,\ldots, x^r$ ненулевых и отличных друг от друга решений $x^j \in N_{I_{0i}}$, $j=\overline{1,r}$, с вероятностью, стремящейся к 1, когда $n\to\infty$, имеют место соотношения: $k_u(X_r) \underset{n\to\infty}{\sim} \dfrac{n}{|I_{0i}|^r}$, $u \in I_{0i}^r$, где $X_r = \begin{pmatrix} x^1 \\ \cdot \\ \cdot \\ \cdot \\ x^r \end{pmatrix}$.

Теорема 3. Пусть выполнены условия (2). Тогда для каждого фиксированного $i, i=\overline{1,t}$, случайная величина $\nu_{n I_{0i}}$ при $n\to\infty$ распределена по закону Пуассона с параметром $|I_{0i}|^s$.

Доказательство. На основании теоремы 1 из [3, с. 26] теорема 2 обеспечивает выполнение условий $\lim\limits_{n\to\infty} \mathbf{M}(\nu_{n I_{0i}})_r / r! = |I_{0i}|^{rs} / r!$, $r=1,2,\ldots$, при которых распределение случайной величины $\nu_{n I_{0i}}$ при $n\to\infty$ стремится к закону Пуассона с параметром $|I_{0i}|^s$, что и требовалось доказать.

На основании теорем 2 и 3 сформулируем более общее утверждение.

Теорема 4. Пусть выполнены условия (2), и пусть для кольца $\mathbf{R}$ множество $D_0 \neq \varnothing$. Тогда случайная величина $\nu_{n D_0}$, равная числу решений системы (1) ((1′)), каждое из которых принадлежит одному из множеств N_I, $I \in D_0$, при $n\to\infty$ распределена по закону Пуассона с параметром $\sum\limits_{i=1}^{k} |I_{0i}|^s$. При этом для любого набора ненулевых и отличных друг от друга решений $x^1,\ldots, x^r$ системы (1) ((1′)), для которого соответствующая матрица

$$X_r = \begin{pmatrix} x^1 \\ \cdot \\ \cdot \\ \cdot \\ x^r \end{pmatrix} \in N_{I_{0i_1}\times\ldots\times I_{0i_r}}, \text{ где } I_{0i_j} \in D_0, \ j=\overline{1,r},$$

$\boldsymbol{r}$ — некоторое натуральное число, с вероятностью, стремящейся к 1, когда $n \to \infty$, имеют место соотношения

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

Пример 2. Рассмотрим кольцо $\boldsymbol{R} = \boldsymbol{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ вычетов по модулю 6. $\boldsymbol{R}$ содержит два идеала: $\boldsymbol{I}_1 = \{3, 0\}$ и $\boldsymbol{I}_2 = \{2, 4, 0\}$. Нетрудно проверить, что эти идеалы изоморфны соответственно **GF**(2) и **GF**(3). Таким образом, $\boldsymbol{D}_0 = \{\boldsymbol{I}_1, \boldsymbol{I}_2\}$. На основании теорем 3, 4 можно сделать следующий вывод: при выполнении условий (2) распределение каждой из случайных величин $\nu_{n\boldsymbol{I}_1}$, $\nu_{n\boldsymbol{I}_2}$, $\nu_{n\boldsymbol{D}_0}$ при $n \to \infty$ стремится к закону Пуассона соответственно с параметром 2^s, 3^s, $2^s + 3^s$.

Заметим, что в отличие от теорем 1–3 статьи [1] в формулировках, аналогичных теорем 1–4 настоящей работы, не говорится, что условия (2) определяют границу области инвариантности соответствующих вероятностных характеристик системы (1) ((1′)). Здесь условия (2) выступают в роли достаточных. Будут ли они и необходимыми, т.е. определяют ли они (в данной терминологии) границу области инвариантности $\mathbf{M}(\nu_n)_r$ и распределений случайных величин $\nu_{n\boldsymbol{I}_{0i}}, i = \overline{1, t}$, $\nu_{n\,\boldsymbol{D}_0}$, когда $n \to \infty$, зависит, вообще говоря, от вида самой нелинейной системы (1) ((1′)) и от структурных особенностей кольца $\boldsymbol{R}$.

Действительно, имеют место следующие теоремы.

Теорема 5. Если в уравнениях системы (1) ((1′)) отсутствуют слагаемые вида ax^k, $k = \overline{2, d_i}$, $i = \overline{1, n-s}$, и для распределений коэффициентов системы выполняются условия, аналогичные (2), то последние (в данной терминологии) являются необходимыми и достаточными для справедливости утверждений теоремы 1–4.

Доказательство. Для доказательства утверждения теоремы достаточно показать, что условия (2) в данной терминологии определяют границу области инвариантности $\lim\limits_{n \to \infty} \mathbf{M}\nu_{n\boldsymbol{I}_0}$, где $\boldsymbol{I}_0$ — минимальный по мощности ненулевой левый идеал $\boldsymbol{R}$, т.е. $|\boldsymbol{I}_0| = l_0$.

На основании (9) можно записать

$$\mathbf{M}\nu_{n\boldsymbol{I}_0} = \sum_{\boldsymbol{x} \in \boldsymbol{N}_{\boldsymbol{I}_0}} \prod_{i=1}^{n-s} \mathbf{P}(\boldsymbol{a}_i\, x = \boldsymbol{0}). \tag{14}$$

Рассмотрим часть суммы (14), которая соответствует векторам $\boldsymbol{x} \in \boldsymbol{N}_{\boldsymbol{I}_0}$ у которых одна из координат фиксирована и равна $z_0 \in \boldsymbol{I}_0 \setminus 0$, а остальные равны 0. Обозначим эту часть s_n. В силу результатов § 8.3 [2] для s_n справедлива точная верхняя оценка

$$s_n \le n \cdot l_0^{-(n-s)} [1 + (l_0 - 1)(1 - m\delta_n)]^{n-s} = n\left[1 - \frac{\ln c_n\, n}{n}\right]^{n-s} \underset{n \to \infty}{\sim}$$

$$\underset{n \to \infty}{\sim} ne^{-\ln c_n n} = c_n^{-1}.$$

Отсюда получаем, если $c_n \underset{n \to \infty}{\not\to} \infty$, то верхняя оценка для s_n не стремится к 0, т.е. условия (2), где $c_n \underset{n \to \infty}{\not\to} \infty$, не могут определять границу области инвариантности для $\lim\limits_{n \to \infty} \mathbf{M}\nu_{n\boldsymbol{I}_0}$, что и требовалось доказать.

Теорему 5 можно переформулировать в таком виде.

Теорема 5′. Если в системе (1) ((1′)) область суммирования под знаком второй суммы имеет вид $1 \le j_1 < \ldots < j_k \le n$, $(1 \le j_1, \ldots, j_k \le n;\ j_i \ne j_t, i \ne t)$, то условия (2) (в данной терминологии) являются необходимыми и достаточными для справедливости утверждений теорем 1–4.

Теорема 6. Если в кольце $\boldsymbol{R}$ среди минимальных по мощности ненулевых левых идеалов существует идеал $\boldsymbol{I}_0$, для которого $\boldsymbol{I}_0 \cdot \boldsymbol{I}_0 = \{0\}$, то условия (2) (в данной терминологии) являются необходимыми и достаточными для справедливости утверждений теорем 1–4.

Доказательство. Из условия теоремы 6 следует, что $\left|\boldsymbol{I}_0\right| = l_0$ и $z^2 = 0$ для любого $z \in \boldsymbol{I}_0$. Теперь, используя последнее и полностью повторяя рассуждения доказательства теоремы 5, можно показать, что условия (2) в данной терминологии определяют границу области инвариантности для $\lim\limits_{n\to\infty} \mathbf{M}\nu_{n\boldsymbol{I}_0}$, что и доказывает справедливость утверждения теоремы.

Теорема 7. Пусть в кольце $\boldsymbol{R}$ не существует левого идеала $\boldsymbol{I}$, для которого $\boldsymbol{I}\cdot\boldsymbol{I} = \{0\}$, и пусть в системе (1) $((1'))d_i = d, i = \overline{1,n-s}$, а коэффициенты удовлетворяют условиям

$$\frac{l_0}{m(l_0-1)} \cdot \frac{\ln c_n\, n}{dn} = \delta_n \le \mathbf{P}(a_{i,j_1,\dots,j_k} = z),\ z \in \boldsymbol{R}, \tag{15}$$

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

где l_0, m, c_n те же, что и в (2). Тогда условия (15) (в данной терминологии) являются необходимыми и достаточными для справедливости утверждений, аналогичных утверждениям теорем 1–4.

Доказательство. Пусть $\boldsymbol{I}_0$ — отличный от $\{0\}$ минимальный по мощности левый идеал $\boldsymbol{R}$, т.е. $\left|\boldsymbol{I}_0\right| = l_0$. Для доказательства теоремы 7, как и в аналогичном случае при $d = 1$ в [2], достаточно показать, что условия (15) в данной терминологии определяют границу области инвариантности для $\lim\limits_{n\to\infty} \mathbf{M}\nu_{n\boldsymbol{I}_0}$.

Поскольку в силу определения $\boldsymbol{I}_0$ все элементы $z \in \boldsymbol{I}_0 \setminus 0$ таковы, что $\boldsymbol{R}\, z = \boldsymbol{I}_0$, точная нижняя и точная верхняя оценки для $\mathbf{M}\nu_{n\boldsymbol{I}_0}$ имеют соответственно вид

$$L_* = \sum_{\substack{k_z,\ z\in\boldsymbol{I}_0 \\ \sum\limits_{z\in\boldsymbol{I}_0} k_z = n,\ k_0 \ne n}} \frac{n!}{\prod\limits_{z\in\boldsymbol{I}_0} k_z!} \cdot l_0^{-(n-s)} [1-(1-m\delta_n)^k]^{n-s},$$

$$L^* = \sum_{\substack{k_z,\ z\in\boldsymbol{I}_0 \\ \sum\limits_{z\in\boldsymbol{I}_0} k_z = n,\ k_0 \ne n}} \frac{n!}{\prod\limits_{z\in\boldsymbol{I}_0} k_z!} \cdot l_0^{-(n-s)} [1+(l_0-1)(1-m\delta_n)^k]^{n-s},$$

где $k_0 = k_0(\boldsymbol{x})$ — число нулевых координат в векторе $\boldsymbol{x} \in \boldsymbol{N}_{\boldsymbol{I}_0}$,

$$k = \sum_{t=1}^{d} \left(\sum_{z\in\boldsymbol{I}_0\setminus 0} k_z \right)^t = \frac{\left[\left(\sum\limits_{z\in\boldsymbol{I}_0\setminus 0} k_z \right)^d - 1 \right]}{\sum\limits_{z\in\boldsymbol{I}_0\setminus 0} k_z - 1}.$$

Из вида нижней оценки L_* следует, что

$$L_* \underset{n\to\infty}{\sim} \sum_{\substack{k_z \underset{n\to\infty}{\sim} \frac{n}{l_0},\ z\in\boldsymbol{I}_0 \\ \sum\limits_{z\in\boldsymbol{I}_0} k_z = n}} \frac{n!}{\prod\limits_{z\in\boldsymbol{I}_0} k_z!} \cdot l_0^{-(n-s)} \left[1-\left[1-\frac{l_0 \ln c_n\, n}{(l_0-1)dn} \right]^k \right]^{n-s} \underset{n\to\infty}{\sim}$$

$$\underset{n\to\infty}{\sim} l_0^s [1-(c_n n)^{-\theta_{nd}}]^{n-s} = l_0^s + O\left(c_n^{-\theta_{nd}} n^{-\theta_{nd}} \right) \xrightarrow[n\to\infty]{} l_0^s,$$

где

$$\theta_{nd} = \frac{((l_0-1)n/l_0)^d - 1}{((l_0-1)n/l_0 - 1)d}. \tag{16}$$

Приступим к анализу L^*.

Фиксируем некоторый элемент $z_0 \in \boldsymbol{I}_0 \setminus 0$ и выделим в L^* ту часть s_n суммы, в слагаемых которой $k_{z_0} = 1$, $k_z = 0$, $z \in \boldsymbol{I}_0 \setminus \{z_0 \cup 0\}$, т.е. $s_n = n \cdot l_0^{-(n-s)} \times$ $\times [1 + (l_0 - 1)(1 - m\delta_n)^d]^{n-s}$. В результате асимптотического анализа s_n имеем

$$s_n \underset{n\to\infty}{\sim}{}_{k_z} l_0^{-(n-s)} \left[1 + (l_0 - 1)\left(1 - \frac{l_0}{l_0 - 1} \cdot \frac{\ln c_n\, n}{n}\right)\right]^{n-s} = n\left(1 - \frac{\ln c_n\, n}{n}\right)^{n-s} \underset{n\to\infty}{\sim} c_n^{-1}. \tag{17}$$

Что касается оставшейся части оценки L^*, т.е. суммы $L^* - s_n$, то

$$L^* - s_n \underset{n\to\infty}{\sim} \sum_{\substack{k_z \underset{n\to\infty}{\sim} \frac{n}{l_0}, z\in \boldsymbol{I}_0 \\ \sum_{z\in \boldsymbol{I}_0} k_z = n}} \frac{n!}{\prod_{z\in \boldsymbol{I}_0} k_z!} \cdot l_0^{-(n-s)} \, [1 + (l_0 - 1)(1 - m\delta_n)^k]^{n-s} \underset{n\to\infty}{\sim}$$

$$\underset{n\to\infty}{\sim} l_0^s \left[1 + O\left(c_n^{-\theta_{nd}}\, n^{-\theta_{nd}}\right)\right] \xrightarrow[n\to\infty]{\sim} l_0^s,$$

где θ_{nd} определяется формулой (16).

Итак, на основании полученных оценок для L_*, s_n и $L^* - s_n$ можно сделать следующий вывод: при $2 \le d \le n$ условия (15) (в данной терминологии) являются достаточными для того, чтобы $\lim\limits_{n\to\infty} \mathbf{M}\nu_{n\boldsymbol{I}_0} = l_0^s$. Однако в силу (17) при $c_n \underset{n\to\infty}{\not\to} \infty$ сумма s_n не стремится к 0, когда $n \to \infty$. Таким образом, условия (15) (в данной терминологии) являются не только достаточными, но и необходимыми, чтобы $\lim\limits_{n\to\infty} \mathbf{M}\nu_{n\boldsymbol{I}_0} = l_0^s$, что и требовалось доказать.

Выражаю благодарность О.А. Король за помощь в оформлении работы.

СПИСОК ЛИТЕРАТУРЫ

1. Левитская А.А. Теоремы инвариантности для одного класса нелинейных сиситем уравнений над произвольным конечным полем // Кибернетика и системный анализ. — 1996. — № 2. — С. 103–112.
2. Коваленко И.Н., Левитская А.А., Савчук М.Н. Избранные задачи вероятностной комбинаторики. — Киев: Наук. думка, 1986. — 223 с.
3. Сачков В.Н. Введение в комбинаторные методы дискретной математики. — М.: Наука, 1982. — 384 с.

Поступила 27.03.2008