Доклады Академии наук СССР
1975. Том 221, № 4

УДК 519.21

*МАТЕМАТИКА*

И. Н. КОВАЛЕНКО, А. А. ЛЕВИТСКАЯ

# ПРЕДЕЛЬНОЕ ПОВЕДЕНИЕ ЧИСЛА РЕШЕНИЙ СИСТЕМЫ СЛУЧАЙНЫХ ЛИНЕЙНЫХ УРАВНЕНИЙ НАД КОНЕЧНЫМ ПОЛЕМ И КОНЕЧНЫМ КОЛЬЦОМ

*(Представлено академиком В. М. Глушковым 29 VIII 1974)*

1. Рассматривается система случайных линейных уравнений над $\mathbf{R}(\mathbf{m})$ ($\mathbf{R}(\mathbf{m})$ — поле или кольцо с конечным числом элементов $m$)

$$\sum_{j=1}^{n} a_{ij}x_j=0, \quad 1\leqslant i\leqslant N, \tag{1}$$

где $a_{ij}=a_{ij}^{(n)}$ — независимые случайные величины.

В различных предположениях относительно $n$, $N$ и распределений случайных величин $a_{ij}$ в работах [1-4] исследуется предельное поведение $\mu_n$ — числа линейно независимых решений системы (1) над конечными полями при $n\to\infty$.

В настоящей заметке решается задача определения любого конечного момента распределения $\nu_n$ — числа решений (1), когда $n\to\infty$. Для случая конечного поля устанавливается предельное распределение $\mu_n$ при $n\to\infty$. Основные результаты данной работы могут быть сформулированы в виде следующих теорем.

Теорема 1. *Пусть* $\mathbf{R}(\mathbf{m})$ *— поле. Тогда, если система* (1) *такая, что*:

а) $n=N+s$, $s=\text{const}$;

б) $0<\delta\leqslant\mathbf{P}(a_{ij}=z)$, $1\leqslant i\leqslant N$, $1\leqslant j\leqslant n$, $z\in\mathbf{R}(\mathbf{m})$,

*то*

$$\lim_{n\to\infty}\mathbf{M}(\nu_n-1)(\nu_n-m)\dots(\nu_n-m^{r-1})=m^{rs}, \tag{2}$$

*где* $r$ *— некоторое целое положительное число, и*

$$\lim_{n\to\infty}\mathbf{P}(\nu_n=k)=\frac{1}{m^{k(k+s)}}\frac{\prod_{i=k+1}^{\infty}(1-1/m^i)}{\prod_{i=1}^{k+s}(1-1/m^i)}. \tag{3}$$

Теорема 2. *Пусть* $\mathbf{R}(\mathbf{m})$ *— кольцо с единицей* *. *Тогда, если выполнены условия* а), б) *предыдущей теоремы, то*

$$\lim_{n\to\infty}\mathbf{M}\nu_n^r=\sum_l\frac{k_l}{l^s}, \tag{4}$$

* Отсутствие единицы в конечном кольце влечет нильпотентность такого кольца. В этом случае с вероятностью 1 число решений системы (1) при $n\to\infty$ стремится к бесконечности.

*где* $k_l$ *— количество наборов* $(u_1, \ldots, u_l)$, *состоящих из* $l$ $r$*-мерных векторов* $\mathbf{u}_i = (u_i^1, \ldots, u_i^r)$, $1 \leqslant i \leqslant l$, *для каждого из которых группа*

$$G(\mathbf{u}_1, \ldots, \mathbf{u}_l) = G(u_1^1, \ldots, u_1^r) + \ldots + G(u_l^1, \ldots, u_l^r),$$

*где* $G(u_i^1, \ldots, u_i^r) = \{(zu_i^1, \ldots, zu_i^r), \quad z \in \mathbf{R}(\mathbf{m})\}$ *и* $A+B$ *обозначает* $\{x+y: x \in A, y \in B\}$, *содержит* $l$ *элементов.*

2. Лемма. *Пусть* $\xi_1, \ldots, \xi_n$ *— независимые случайные величины со значениями в аддитивной абелевой группе* $G$ *порядка* $m$.

*Тогда, если* $0 < \delta \leqslant \mathbf{P}(\xi_i = z)$, $1 \leqslant i \leqslant n$, $z \in G$, *то*

$$\frac{1}{m}(1 - m\rho^n) \leqslant \mathbf{P}(\xi_1 + \ldots + \xi_n = z) \leqslant \frac{1}{m}(1 + m\rho^n), \quad z \in G, \quad \rho = 1 - \delta. \tag{5}$$

Доказательство. Представим $\mathbf{P}(\xi_i = z)$ в виде $\mathbf{P}(\xi_i = z) = 1/m + \Delta_i(z)$. Тогда, принимая во внимание, что $\sum\limits_{z \in G} \Delta_i(z) = 0$, по индукции легко доказываем, что

$$\mathbf{P}(\xi_1 + \ldots + \xi_n = z) = \frac{1}{m} + \sum_{z_1, \ldots, z_{n-1} \in G} \Delta_1(z_1)\Delta_2(z_2 - z_1)\ldots\Delta_n(z - z_{n-1}). \tag{6}$$

Заимствуя схему доказательства из ([5]), легко показать, что сумма, стоящая в правой части (6), по модулю не превосходит $(1-\delta)^n$ для любого $z \in G$. Отсюда доказательство (5) не составляет труда.

Введем следующие обозначения: $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{x}_i \in \mathbf{R}(\mathbf{m})$, $1 \leqslant i \leqslant n$; $\xi(\mathbf{x})$ — индикатор события, состоящего в том, что $\mathbf{x}$ удовлетворяет (1); $|A|$ — мощность любого множества $A$.

3. Доказательство теоремы 1. Нетрудно видеть, что

$$\mathbf{M} \sum_{\text{л.н.}\mathbf{x}^1, \ldots, \mathbf{x}^r} \xi(\mathbf{x}^1)\ldots\xi(\mathbf{x}^r) = \mathbf{M}(\nu_n - 1)(\nu_n - m)\ldots(\nu_n - m^{r-1}),$$

где запись л.н. $\mathbf{x}^1, \ldots, \mathbf{x}^r$ обозначает, что сумма берется по всевозможным наборам линейно независимых векторов $\mathbf{x}^i$, $1 \leqslant i \leqslant r$.

Рассмотрим произвольный набор л.н. $\mathbf{x}^1, \ldots, \mathbf{x}^r$ и набор переменных $u^i \in \mathbf{R}(\mathbf{m})$, $1 \leqslant i \leqslant r$. Обозначим

$$I_{u^1 \ldots u^r}(x^1, \ldots, x^r) = \{j: 1 \leqslant j \leqslant n, x_j^k = u^k, 1 \leqslant k \leqslant r\}.$$

Пусть $U(\mathbf{x}^1, \ldots, \mathbf{x}^r) = \|u_j^i\|_{j=1,\ldots,n}^{i=1,\ldots,r}$ — матрица, $i$-я строка которой есть вектор $\mathbf{x}^i$. Обозначим через $\Delta_t$ некоторую матрицу, составленную из элементов, стоящих на пересечении произвольных $t$ строк и $t$ столбцов $U(\mathbf{x}^1, \ldots, \mathbf{x}^r)$, а через $R(\Delta_t)$ — ранг $\Delta_t$. Пусть

$$k_t(\mathbf{x}^1, \ldots, \mathbf{x}^r) = \max_{\Delta_t:\ R(\Delta_t) = t} \min_{1 \leqslant j \leqslant t} \{|I_{u_{k_j}^{l_1} \ldots u_{k_j}^{l_t}}(\mathbf{x}^1, \ldots, \mathbf{x}^r)|\}.$$

Рассмотрим $\Delta_t$, на которой

$$k_t(\mathbf{x}^1, \ldots, \mathbf{x}^r) = \min_{1 \leqslant j \leqslant t} \{|I_{u_{k_j}^{l_1} \ldots u_{k_j}^{l_t}}(\mathbf{x}^1, \ldots, \mathbf{x}^r)|\},$$

и матрицу $\Delta_r$, $R(\Delta_r)=r$, содержащую $\Delta_t$. Введем случайные величины

$$\gamma^{(i)}_{u^1\dots u^r}=\sum_{j\in I_{u^1\dots u^r}(\mathbf{x}^1,\dots,\mathbf{x}^r)} a_{ij}.$$

Тогда л.н. $\mathbf{x}^1,\dots,\mathbf{x}^r$ удовлетворяют (1) в том и только том случае, если

$$\sum_{j=1}^{r}\gamma^{(i)}_{u^1_{k_j}\dots u^r_{k_j}}u^l_{k_j}+\Psi_{li}=0,\quad 1\leqslant l\leqslant r,\ 1\leqslant i\leqslant N, \tag{7}$$

где $(u^1_{k_j}\dots u^r_{k_j})$, $1\leqslant j\leqslant r$, — $j$-й столбец $\Delta_r$, а $\Psi_{li}$ — сумма по наборам $(u^1\dots u^r)$, не входящим в число столбцов $\Delta_r$.

Зафиксировав $\Psi_{li}$, можно однозначно разрешить (7) относительно $\gamma^{(i)}_{u^1_{k_j}\dots u^r_{k_j}}$, $1\leqslant j\leqslant r$. Отсюда, учитывая (5), легко показать, что

$$\frac{1}{m^{Nr}}[1-mNr\rho^{k_r(\mathbf{x}^1,\dots,\mathbf{x}^r)}]\leqslant M\xi(\mathbf{x}^1)\dots\xi(\mathbf{x}^r)\leqslant\frac{1}{m^{Nr}}\exp\{mNr\rho^{k_r(\mathbf{x}^1,\dots,\mathbf{x}^r)}\}; \tag{8}$$

$$0<\mathbf{M}\xi(\mathbf{x}^1)\dots\xi(\mathbf{x}^r)\leqslant(1-(m-1)\delta)^{(r-1)N}\frac{1}{m^{Nt}}\exp\{mNt\rho^{k_t(\mathbf{x}^1,\dots,\mathbf{x}^r)}\}, \tag{9}$$

$$1\leqslant t\leqslant r-1.$$

Фиксируем некоторое $k_0>0$ и разобьем все наборы л.н. $\mathbf{x}^1,\dots,\mathbf{x}^r$ на множества:

$$A_0=\{\text{л.н. }\mathbf{x}^1,\dots,\mathbf{x}^r\colon\ k_1(\mathbf{x}^1,\dots,\mathbf{x}^r)\leqslant k_0\},$$

$$A_t=\{\text{л.н. }\mathbf{x}^1,\dots\mathbf{x}^r\colon\ k_t(\mathbf{x}^1,\dots,\mathbf{x}^r)>k_0,\ k_{t+1}(\mathbf{x}^1,\dots,\mathbf{x}^r)\leqslant k_0\},\quad 0<t<r,$$

$$A_r=\{\text{л.н. }\mathbf{x}^1,\dots,\mathbf{x}^r\colon\ k_r(\mathbf{x}^1,\dots,\mathbf{x}^r)>k_0\}.$$

Теперь, оценивая $|A_t|$, $0\leqslant t\leqslant r$, и принимая во внимание (8), (9), нетрудно доказать (2).

Формула (3) следует из рассуждений, вполне аналогичных использованным в [2].

4. Доказательство теоремы 2. Очевидно, что

$$\mathbf{M}\nu_n{}^r=\sum_{\mathbf{x}^1,\dots,\mathbf{x}^r}\mathbf{M}\xi(\mathbf{x}^1)\dots\xi(\mathbf{x}^r).$$

Зададим некоторое $k_0$ и рассмотрим

$$R(\Theta)=\{(\mathbf{x}^1,\dots,\mathbf{x}^r)\colon\ |I_{u^1\dots u^r}(\mathbf{x}^1,\dots,\mathbf{x}^r)|<k_0\ \text{при}\ \Theta(u^1,\dots,u^r)=0,$$

$$|I_{u^1\dots u^r}(\mathbf{x}^1,\dots,\mathbf{x}^r)|>k_0\ \text{при}\ \Theta(u^1,\dots,u^r)=1\},$$

где $\Theta=\Theta(u^1,\dots,u^r)$ — произвольная функция со значениями 0 и 1. Обозначим $S=\{(u_1,\dots,u_l)\colon\ |G(u_{i_1},\dots,u_{i_l})|=l\}$ (см. формулировку теоремы 2). Тогда

$$\mathbf{M}\nu_n{}^r=\sum_{\Theta\colon\{(u^1,\dots,u^r)\colon\Theta(u^1,\dots,u^r)=1\}\in S}\mathbf{M}\sum_{(\mathbf{x}^1,\dots,\mathbf{x}^r)\in R(\Theta)}\xi(\mathbf{x}^1)\dots\xi(\mathbf{x}^r)+$$

$$+\sum_{\Theta\colon\{(u^1,\dots,u^r)\colon\Theta(u^1,\dots,u^r)=1\}\notin S}\mathbf{M}\sum_{(\mathbf{x}^1,\dots,\mathbf{x}^r)\in R(\Theta)}\xi(\mathbf{x}^1)\dots\xi(\mathbf{x}^r). \tag{10}$$

Рассмотрим произвольное $\Theta$, соответствующее первой сумме в (10). Учитывая (5), нетрудно доказать, что

$$\mathbf{M}\sum_{(\mathbf{x}^1,\dots,\mathbf{x}^r)\in R(\Theta)}\xi(\mathbf{x}^1)\dots\xi(\mathbf{x}^r)\to\frac{1}{l^s}.$$

Из того, что второй суммой в (10) при достаточно большом $n$ можно пренебречь, следует (4).

Институт кибернетики
Академии наук УССР
Киев

Поступило
7 VI 1974

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] *И. Н. Коваленко,* ДАН, т. 161, № 3, 517 (1965). [2] *М. В. Козлов,* ДАН, т. 169, № 5, 1013 (1966). [3] *И. Н. Коваленко,* Теория вероятн. и ее примен., т. 12, 1, 51 (1967). [4] *Г. В. Балакин,* Там же, т. 13, 4, 631 (1968). [5] *Б. В. Гнеденко,* Курс теории вероятностей, М., 1965.