Системы случайных уравнений над конечными полями

В.Н. Сачков

1. Введение

Исследованиям систем случайных линейных уравнений над конечными полями посвящен ряд работ, включающий статьи [2], [3], [4], [8], [9]. В данной статье при равновероятном и независимом выборе коэффициентов и свободных членов находятся выраженные через ряды Эйлерова типа предельные распределения числа решений однородной системы при стремлении отдельно числа неизвестных и числа уравнений к бесконечности. Для соответствующих неоднородных систем с использованием аналогичных рядов находится асимптотика вероятности совместности и предельное выражение для условного распределения числа решений при условии, что система совместна. В качестве следствия получено простое доказательство тождества Эйлера.

Для исследования систем случайных нелинейных уравнений с использованием модели, в которой порядок уравнений несущественен, используется предложенный в статье автора [7] и развитый в работе [8] подход, использующий случайные покрытия и метод биномиальных моментов. Для данной модели получены точные формулы и дано полное описание всех предельных распределений числа решений случайной системы уравнений.

2. Системы случайных линейных уравнений

Рассмотрим систему случайных линейных уравнений

$$a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{im}x_m = b_i, \quad i = 1, 2, \ldots, k, \tag{2.1}$$

где a_{ij}, b_i, $i = 1, 2, \ldots, k$, $j = 1, 2, \ldots, m$, случайно и независимо принимают значения из поля Галуа $GF(q)$, причем

$$\mathbf{P}(a_{ij} = \mu) = \frac{1}{q}, \quad \mathbf{P}(b_i = \nu) = \frac{1}{q},$$

$$\mu, \nu = 0, 1, \ldots, q-1.$$

Пусть $A = (a_{ij})$, $i = 1, 2, \ldots, k$, $j = 1, 2, \ldots, m$ - матрица системы (2.1) и r - ранг матрицы A. Множество решений случайной однородной системы

$$a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{im}x_m = 0, \quad i = 1, 2, \ldots, k, \tag{2.2}$$

соответствующей системе (2.1), образуют подпространство W_{m-r} размерности $m-r$ в m-мерном векторном пространстве V_m размерности m над полем $GF(q)$. Если $x^0 = (x_1^0, x_2^0, \ldots, x_m^0)$ есть некоторое частное решение системы (2.1), то множество решений этой системы представляет собой аффинное многообразие $\widetilde{W}_{m-r} = x^0 + W_{m-r}$, полученное из W_{m-r} параллельным переносом на вектор x^0. Таким образом, если система (2.1) совместна, то число ее решений совпадает с числом решений соответствующей однородной системы. Пусть η_{km} - число решений однородной системы случайных линейных уравнений вида (2.2) над полем $GF(q)$. Тогда вероятностные распределения η_{km} и ранг ρ_{km} случайной матрицы $A = (a_{ij})$, $i = 1, \ldots, k$, $j = 1, \ldots, m$ связаны равенством

$$\mathbf{P}(\eta_{km} = q^{m-r}) = \mathbf{P}(\rho_{km} = r). \tag{2.3}$$

Случайная величина ρ_{km} имеет следующее распределение

$$\mathbf{P}(\rho_{km} = r) = \frac{1}{q^{(k-r)(m-r)}} \frac{\prod\limits_{j=k-r+1}^{k}(1-\frac{1}{q^j}) \prod\limits_{j=m-r+1}^{m}(1-\frac{1}{q^j})}{\prod\limits_{j=1}^{r}(1-\frac{1}{q^j})}, \tag{2.4}$$

$$r = 0, 1, \ldots, \min(k, m).$$

При $r = 0$ отношение произведений полагаем равным единице, считая, что $\prod_{j=n+1}^{n} = 1$. Действительно, число матриц $k \times m$ ранга r над полем $GF(q)$ равно

$$C(k, m, r) = \begin{bmatrix} m \\ r \end{bmatrix}_q (q^k - 1)(q^k - q) \cdots (q^k - q^{r-1}), \tag{2.5}$$

где $\begin{bmatrix} m \\ r \end{bmatrix}_q$ - числа Гаусса, определяемые формулой

$$\begin{bmatrix} m \\ r \end{bmatrix}_q = \frac{(q^m - 1)(q^{m-1} - 1) \cdots (q^{m-r+1} - 1)}{(q^r - 1)(q^{r-1} - 1) \cdots (q - 1)}. \tag{2.6}$$

Формула (2.5) вытекает из следующих соображений. Строки $k \times m$ матрицы A ранга r порождают подпространство W_r размерности r m-мерного векторного пространства V_m. Ясно, что W_r изоморфно r-мерному пространству L_r, порождаемому строками матрицы B размеров $k \times r$ и ранга r. При биекции $\psi : W_r \to L_r$ матрице A ставится в соответствие матрица B, столбцы которой линейно независимы. Отсюда следует, что $C(k, m, r)$ равно произведению числа r-мерных подпространств V_m на число способов выбора r линейно независимых векторов размерности k.

Из формул (2.3) и (2.4) имеем точное распределение для

$$\mathbf{P}(\eta_{km} = q^\mu) = \frac{1}{q^{\mu(\mu+k-m)}} \frac{\prod_{j=k-m+\mu+1}^{k} (1 - \frac{1}{q^j}) \prod_{j=\mu+1}^{m} (1 - \frac{1}{q^j})}{\prod_{j=1}^{m-\mu} (1 - \frac{1}{q^j})}, \tag{2.7}$$
$$\mu = m - \min(m, k), \ldots, m.$$

Для представления предельного распределения η_{km} введем обозначения. Обозначим

$$\theta = \prod_{j=1}^{\infty} \left(1 - \frac{1}{q^j}\right), \tag{2.8}$$

сходящееся при $q \geq 2$ бесконечное произведение, которое, согласно пентагональной теореме Эйлера, можно представить в виде сходящегося ряда [5]:

$$\theta = \sum_{j=-\infty}^{\infty} (-1)^j \left(\frac{1}{q}\right)^{\frac{1}{2}j(3j-1)}.$$

Далее положим

$$C_0(0)=\theta,\quad C_\nu(0)=\frac{\theta}{\prod\limits_{j=1}^{\nu}(1-\frac{1}{q^j})^2},\quad C_0(\alpha)=\frac{\theta}{\prod\limits_{j=1}^{\alpha}(1-\frac{1}{q^j})},\tag{2.9}$$

$$C_\nu(\alpha)=\frac{\theta}{\prod\limits_{j=1}^{\nu}(1-\frac{1}{q^j})\prod\limits_{j=1}^{\nu+\alpha}(1-\frac{1}{q^j})}.\tag{2.10}$$

Отметим, что $C_\nu(\alpha)$ является возрастающей функцией от ν и

$$\theta\le C_\nu(\alpha)\le\frac{1}{\theta},\quad \nu=0,1,\dots$$

для любых $\alpha=0,1,\dots$.

Предельные распределения η_{km} описываются следующей теоремой.

Теорема 1. *Предельные распределения числа решений однородной системы случайных линейных уравнений η_{km} имеют следующий вид:*

а) если $\gamma=k-m\ge 0$, то

$$\lim_{m\to\infty}\mathbf{P}(\eta_{km}=q^\mu)=\begin{cases}\frac{C_\mu(\gamma)}{q^{\mu(\mu+\gamma)}}, & 0\le\mu<\infty\\ 0, & \mu\to\infty\end{cases},\tag{2.11}$$

$$\lim_{\substack{m\to\infty\\ \gamma\to\infty}}\mathbf{P}(\eta_{km}=1)=1;\tag{2.12}$$

б) если $\delta=m-k\ge 0$, то

$$\lim_{k\to\infty}\mathbf{P}(\eta_{km}=q^{\delta+\mu})=\begin{cases}\frac{C_\mu(\delta)}{q^{\mu(\mu+\delta)}}, & 0\le\mu<\infty\\ 0, & \mu\to\infty\end{cases},\tag{2.13}$$

$$\lim_{\substack{k\to\infty\\ \delta\to\infty}}\mathbf{P}(\eta_{km}=q^{\delta})=1.\tag{2.14}$$

Доказательство теоремы 1 следует непосредственно из выражения для точного распределения (2.7).

Для $\gamma=k-m$ отношение $(\mu+1)$-го члена распределения к μ-му равно

$$\frac{q}{(q^{\mu+1}-1)(q^{\mu+\gamma+1}-1)}.$$

Отсюда следует, что при $\gamma \geq 1$ для всех $q \geq 2$ распределение унимодально с модой при $\mu = 0$, и вероятности монотонно убывают с ростом μ. Точно такая же ситуация и при $\gamma = 0$ для $q > 2$. Если же $\gamma = 0$ и $q = 2$, то мода смещается в точку $\mu = 1$, и все вероятности значений $\mu > 1$ монотонно убывают с ростом μ. Отсюда следует интересный факт: если $k = m$, то при $q > 2$ наиболее вероятно, что система имеет единственное решение, а при $q = 2$ максимальную вероятность имеет событие, состоящее в том, что система имеет $q = 2$ решений. С ростом γ распределение η_{km} "сжимается" к точке $\mu = 0$ и в пределе становится вырожденным.

Аналогичная картина имеет место и при $\delta = m - k$, но со сдвигом значений μ на величину δ вправо.

Из формул (2.11) и (2.13) при $\gamma = 0$ с учетом равенства единице суммы вероятностей предельных распределений получаем тождество

$$\sum_{\mu=0}^{\infty} q^{-\mu^2} \left[\left(1 - \frac{1}{q}\right) \left(1 - \frac{1}{q^2}\right) \cdots \left(1 - \frac{1}{q^\mu}\right) \right]^{-2} = \prod_{j=1}^{\infty} \left(1 - \frac{1}{q^j}\right)^{-1}, \quad (2.15)$$

где полагаем $\prod\limits_{j=1}^{0} (1 - \frac{1}{q^j}) = 1$.

Это тождество является известным тождеством Эйлера [5, стр .34].

Из точного распределения получаем предельные выражения для среднего значения $\mathbf{M}\eta_{km}$:

$$\mathbf{M}\eta_{km} \sim \begin{cases} E(\gamma), & k = m + \gamma, \quad \gamma \geq 0, \quad m \to \infty, \\ q^\delta E(\delta), & m = k + \delta, \quad \delta \geq 0, \quad k \to \infty, \end{cases} \quad (2.16)$$

где

$$E(\alpha) = \sum_{\mu=0}^{\infty} \frac{C_\mu(\alpha)}{q^{\mu(\mu+\alpha)}}, \quad (2.17)$$

причем $E(\alpha)$ можно представить в следующем виде

$$E(\alpha) = \prod_{j=\alpha+1}^{\infty} \left(1 - \tfrac{1}{q^j}\right) \left[1 + \sum_{\mu=1}^{\infty} \frac{q^{2\mu}}{(q-1)(q^2-1)\cdots(q^\mu-1)(q^{\alpha+1}-1)\cdots(q^{\alpha+\mu}-1)} \right]. \quad (2.18)$$

Из формул (2.16) и (2.18) имеем

$$\mathbf{M}\eta_{km} \sim \begin{cases} 1, & k = m + \gamma, \quad \gamma \to \infty, \quad m \to \infty, \\ q^\delta, & m = k + \delta, \quad \delta \to \infty, \quad k \to \infty. \end{cases} \quad (2.19)$$

Перейдем теперь к изучению неоднородных систем случайных линейных уравнений вида (2.1). Обозначим через $\mathbf{P}(k,m)$ вероятность совместности этой ситемы. Для вероятности $\mathbf{P}(k,m)$ имеем следующую формулу:

$$\mathbf{P}(k,m) = \sum_{r=0}^{\min(k,m)} \frac{D_{km}(r)}{q^{(k-r)(m-r+1)}}, \tag{2.20}$$

где

$$D_{km}(r) = \frac{\prod\limits_{j=k-r+1}^{k}(1-\frac{1}{q^j}) \prod\limits_{j=m-r+1}^{m}(1-\frac{1}{q^j})}{\prod\limits_{j=1}^{r}(1-\frac{1}{q^j})}, \ 1 \le r \le \min(m,k), \tag{2.21}$$
$$D_{km}(0) = 1.$$

Действительно, если матрица системы (2.1) имеет ранг r, то условие совместности системы заключается в том, чтобы k-мерный вектор-столбец из свободных членов принадлежал r-мерному подпространству столбцов матрицы. Вероятность этого события равна $1/q^{k-r}$, $0 \le r \le \min(k,m)$. Таким образом,

$$\mathbf{P}(k,m) = \sum_{r=0}^{\min(k,m)} \frac{1}{q^{k-r}} \mathbf{P}(\rho_{km} = r). \tag{2.22}$$

Теперь формула (2.20) следует из формулы (2.4).

Предельные выражения для вероятности $\mathbf{P}(k,m)$ определяются следующей теоремой.

Теорема 2. *Для вероятности совместности системы из k случайных линейных уравнений с m неизвестными $\mathbf{P}(k,m)$ имеют место следующие предельные равенства:*

$$\lim_{m\to\infty} \mathbf{P}(m+\gamma,m) = \begin{cases} \sum\limits_{\nu=0}^{\infty} \frac{C_\nu(\gamma)}{q^{(\nu+1)(\nu+\gamma)}}, & 0 \le \gamma < \infty, \\ 0, & \gamma \to \infty, \end{cases} \tag{2.23}$$

$$\lim_{k\to\infty} \mathbf{P}(k,k+\gamma) = \begin{cases} \sum\limits_{\nu=0}^{\infty} \frac{C_\nu(\delta)}{q^{\nu(\nu+\delta+1)}}, & 0 \le \delta < \infty, \\ 1, & \delta \to \infty, \end{cases} \tag{2.24}$$

где ряды сходятся и величины $C_\nu(\alpha)$ определяются формулами (2.9) и (2.10).

Докажем равенство (2.23). В соответствии с формулами (2.20) и (2.21) имеем

$$\mathbf{P}(m+\gamma, m) = S_1 + S_2,$$

где

$$S_1 = \sum_{\nu=0}^{\log_q m} \frac{D_{m+\gamma,m}(m-\nu)}{q^{(\nu+1)(\nu+\gamma)}},$$

$$S_2 = \sum_{\nu=\log_q m+1}^{m} \frac{D_{m+\gamma,m}(m-\nu)}{q^{(\nu+1)(\nu+\gamma)}}.$$

Очевидна следующая равномерная оценка

$$D_{m+\gamma,m}(m-\nu) \le \frac{1}{\theta}, \quad 0 \le \nu \le m.$$

Поэтому имеем следующую равномерную оценку

$$S_2 \le \frac{1}{\theta}\,\frac{1}{(m-1)m^{\log_q m-1}}.$$

При $m \to \infty$ из очевидных неравенств

$$1 - \sum_{j=m}^{\infty} \frac{1}{q^j} \le \prod_{j=m}^{\infty} \left(1 - \frac{1}{q^j}\right) \le \mathrm{e}^{-\sum\limits_{j=m}^{\infty} \frac{1}{q^j}}$$

следует оценка, равномерная для $0 \le \nu \le \log_q m$:

$$\frac{C_\nu(\gamma)}{D_{m+\gamma,m}(m-\nu)} = 1 + O\left(\frac{1}{q^{m-\log_q m}}\right).$$

С использованием этой оценки находим, что

$$S_1 = \sum_{\nu=0}^{\log_q m} \frac{C_\nu(\gamma)}{q^{(\nu+1)(\nu+\gamma)}} + O\left(\frac{\log_q m}{q^{m-\log_q m}}\right).$$

Так как

$$\sum_{\nu=\log_q m+1}^{\infty} \frac{C_\nu(\gamma)}{q^{(\nu+1)(\nu+\gamma)}} \le \frac{1}{\theta}\,\frac{1}{m^{\log_q m-1}},$$

то собирая полученные оценки, убеждаемся в справедливости первого из равенств (2.23). Второе равенство в (2.23) очевидно ввиду ограниченности коэффициентов $C_\nu(\gamma)$. Равенства (2.24) доказываются точно таким же способом, поэтому доказательство опускается.

Пусть теперь η'_{km} - число решений неоднородной системы случайных линейных уравнений типа (2.1). Из теоремы 2 следует, что при $\gamma = k-m \to \infty$ с вероятростью близкой к единице система (2.1) несовместна, а при $\delta = m - k \to \infty$ система (2.1) совместна. Так как для совместной системы число решений совпадает с числом решений соответствующей однородной системы, то из теоремы 4 вытекает следствие.

Следствие 1. *При* $m \to \infty$

а) если $\gamma = k - m \to \infty$, *то*

$$\mathbf{P}(\eta'_{km} = 0) \to 1; \tag{2.25}$$

б) если $\delta = m - k \to \infty$, *то*

$$\mathbf{P}(\eta'_{km} = q^\delta) \to 1. \tag{2.26}$$

Доказательство следует из неравенства

$$\mathbf{P}(A \cap B) \geq \mathbf{P}(A) + \mathbf{P}(B) - 1,$$

где в качестве события A берется совместность или несовместность системы, а в качестве B - одно из событий $\{\eta'_{km} = 0\}$ или $\{\eta'_{km} = q^\delta\}$.

Утверждение б) легко доказать и непосредственно. Очевидно, что если $\delta = m - k$ и матрица системы (2.1) имеет ранг k, то система совместна. Вероятность этого события равна:

$$\left(1 - \frac{1}{q^{m-k+1}}\right) \cdots \left(1 - \frac{1}{q^m}\right) \geq 1 - \sum_{j=m-k+1}^{\infty} \frac{1}{q^j}.$$

Если $\delta = m - k \to \infty$ при $m \to \infty$, то эта вероятность стремится к единице.

Следствие 2. *При* $k = m$ *имеем следующую формулу:*

$$\lim_{m\to\infty} \mathbf{P}(m, m) = \theta \left[1 + \sum_{\nu=1}^{\infty} [(q-1)(q^2-1)\cdots(q^\nu - 1)]^{-2}\right]. \tag{2.27}$$

Формула (2.27) следует из равенств (2.23) и (2.24) при $\gamma = \delta = 0$.

Из формулы (2.27) следует неравенство

$$1 + \sum_{\nu=1}^{\infty} q^{-\nu(\nu+1)} \left[\left(1 - \frac{1}{q}\right) \cdots \left(1 - \frac{1}{q^{\nu}}\right) \right]^{-2} \leq \prod_{j=1}^{\infty} \left(1 - \frac{1}{q^j}\right)^{-1}.$$

Для системы случайных уравнений (2.1) рассмотрим случайную величину $\widetilde{\eta}_{km}$ - число решений этой системы при условии, что она совместна. Условное распределение $\widetilde{\eta}_{km}$ фактически получается сосредоточением вероятностной меры на положительных значениях η'_{km}.

Прежде чем перейти к отысканию условного предельного распределения $\widetilde{\eta}_{km}$, введем следующее обозначение для сходящегося ряда:

$$C(\alpha) = \sum_{\nu=0}^{\infty} \frac{C_{\nu}(\alpha)}{q^{\nu(\nu+\alpha+1)}}. \tag{2.28}$$

Теорема 3. *Для условного распределения $\widetilde{\eta}_{km}$ - числа решений случайной системы вида (2.1) - имеют место следующие предельные представления:*

а) если $k = m + \gamma$, $\gamma \geq 0$, то

$$\begin{array}{l} \lim\limits_{m\to\infty} \mathbf{P}(\widetilde{\eta}_{km} = q^{\mu}) = \frac{1}{q^{\mu(\mu+\gamma+1)}} \frac{C_{\mu}(\gamma)}{C(\gamma)}, \quad 0 \leq \gamma < \infty; \\ \lim\limits_{\substack{m\to\infty \\ \gamma\to\infty}} \mathbf{P}(\widetilde{\eta}_{km} = 1) = 1, \end{array} \tag{2.29}$$

б) если $m = k + \delta$, $\delta \geq 0$, то

$$\begin{array}{l} \lim\limits_{k\to\infty} \mathbf{P}(\widetilde{\eta}_{km} = q^{\delta+\mu}) = \frac{1}{q^{\mu(\mu+\delta+1)}} \frac{C_{\mu}(\delta)}{C(\delta)}, \quad 0 \leq \delta < \infty; \\ \lim\limits_{\substack{k\to\infty \\ \delta\to\infty}} \mathbf{P}(\widetilde{\eta}_{km} = q^{\delta}) = 1, \end{array} \tag{2.30}$$

$$\mu = 0, 1, \ldots,$$

где $C_{\mu}(\alpha)$ определяются формулами (2.9) и (2.10).

Если ранг матрицы системы (2.1) равен r, то из указанной выше связи решений неоднородной и соответствующей однородной систем имеем:

$$\mathbf{P}(\widetilde{\eta}_{km} = q^{m-r}) = \mathbf{P}(\eta_{km} = q^{m-r} | \widetilde{\eta}_{km} > 0).$$

Из равенств:

$$\mathbf{P}(\{\eta_{km} = q^{m-r}\} \cap \{\widetilde{\eta}_{km} > 0\}) = \frac{1}{q^{k-r}}\mathbf{P}(\eta_{km} = q^{m-r}),$$

$$\mathbf{P}(\widetilde{\eta}_{km} > 0) = \mathbf{P}(k, m),$$

следует, что

$$\mathbf{P}(\widetilde{\eta}_{km} = q^{m-r}) = \frac{1}{q^{k-r}}\frac{\mathbf{P}(\eta_{km} = q^{m-r})}{\mathbf{P}(k, m)}. \tag{2.31}$$

С учетом равенств (2.7), (2.20) и (2.21) формула (2.31) определяет точное распределение случайной величины.

Предельные распределения (2.29) и (2.30) получаются из формулы (2.31) путем соответствующих замен переменных и предельных переходов соответственно при $m \to \infty$ и $k \to \infty$.

Установим некоторые свойства предельных распределений (2.29) и (2.30).

При $\gamma = k - m \geq 0$ отношение $(\mu + 1)$-й вероятности к μ-й в распределении (2.29) равно

$$(q^{\mu+1} - 1)^{-1}(q^{\mu+\gamma+1} - 1)^{-1}.$$

Для $\gamma \geq 1$ при всех $q \geq 2$ это отношение строго меньше единицы, и, следовательно, мода распределения $\widetilde{\eta}_{km}$ расположена в точке $\mu = 0$, а вероятности монотонно убывают с ростом μ. Эта картина сохраняется и при $\gamma = 0$, если $q > 2$. Таким образом, в этих случаях распределение $\widetilde{\eta}_{km}$ унимодально.

При $\gamma = 0$ и $q = 2$ распределение $\widetilde{\eta}_{km}$ бимодально и моды расположены в точках $\mu = 0$ и $\mu = 1$. Это означает, что при $k = m$ и $q = 2$ одинаковые максимальные вероятности имеют события, состоящие в том, что система имеет число решений 1 или 2. Остальные вероятности с ростом μ монотонно убывают. С ростом γ распределение "сжимается" к точке $\mu = 0$ и в пределе становится вырожденным.

При $\delta = m - k \geq 0$ картина аналогична, но со сдвигом значений μ на величину δ вправо. Из теоремы 3 имеем очевидное следствие.

Следствие 3. *Для условной вероятности единственности решения системы из m случайных линейных уравнений с m неизвестными*

вида (2.1) имеет место формула:

$$\lim_{m\to\infty} \mathbf{P}(\widetilde{\eta}_{m,m}=1)=\left[1+\sum_{\nu=1}^{\infty}[(q-1)\cdots(q^{\nu}-1)]^{-2}\right]^{-1} \tag{2.32}$$

Формула (2.32) следует из равенств (2.29) и (2.30) при $\gamma=\delta=0$.

Из точного распределения $\widetilde{\eta}_{km}$ следуют асимптотики для среднего значения

$$\mathbf{M}\widetilde{\eta}_{km}\sim\begin{cases}\frac{G(\gamma)}{C(\gamma)}, & 0\le\gamma<\infty \quad k=m+\gamma,\quad m\to\infty,\\ 1, & \gamma\to\infty\\ q^{\delta}\frac{G(\delta)}{C(\delta)}, & 0\le\delta<\infty \quad m=k+\delta,\quad k\to\infty,\\ q^{\delta}, & \delta\to\infty\end{cases} \tag{2.33}$$

где

$$G(\alpha)=\sum_{\mu=0}^{\infty}\frac{C_{\mu}(\alpha)}{q^{\mu(\mu+\alpha)}}.$$

Из формул (2.19) и (2.29) следует, что асимптотики средних значений η_{km} и $\widetilde{\eta}_{km}$ совпадают при $\gamma,\delta\to\infty$ и различаются, если $0\le\gamma,\delta<\infty$.

3. Системы уравнений со случайными функциями

Пусть элементы $a_1,\ldots,a_k,\ x_1,\ldots,x_m$ принимают значения из некоторого q-множества X, и для случайных независимых и равновероятных отображений $f_i : X^{(m)}\to X$, $1\le i\le k$ определена система случайных уравнений

$$f_i(x_1,\ldots,x_m)=a_i,\quad i=1,2,\ldots,k, \tag{3.1}$$

где $a_i\in X$, $1\le i\le k$ заданы, а неизвестные $(x_1,\ldots,x_m)=X^{(m)}=X\times\cdots\times X$ (m раз) подлежат определению.

Если Y_i - множество решений уравнения

$$f_i(x_1,\ldots,x_m)=a_i,\quad 1\le i\le k,\quad X_i\cup Y_i=X^{(m)},\quad X_i\cap Y_i=\emptyset,$$

то число решений системы (3.1) есть случайная величина η_{km} равная числу элементов $X^{(m)}$, не покрытых случайным множеством $X_1\cup\cdots\cup X_k$.

Положим $n = q^m$ и рассмотрим сначала случай, когда порядок записи уравнений в системе существенен. В этом случае семейство $X_1, \ldots, X_k$ представляет собой случайную равновероятную k-выработку в некоммутативном несимметричном 2^n-базисе. Число k-выработок, не покрывающих ν фиксированных элементов равно $2^{(n-\nu)k}$, поэтому биномиальные моменты η^c_{km} - числа непокрытых элементов $X^{(m)}$ в данном случае имеют вид:

$$B^c_\nu(m,k) = \binom{n}{\nu}\frac{1}{2^{\nu k}}, \quad \nu = 0,1,\ldots,n. \tag{3.2}$$

и, следовательно, точное распределение η^c_{km} является биномиальным с вероятностью успеха $\frac{1}{2^k}$:

$$\mathbf{P}(\eta^c_{km} = r) = \binom{n}{r}\frac{1}{2^{kr}}\left(1-\frac{1}{2^k}\right)^{n-r}, \quad r = 0,1,\ldots,n. \tag{3.3}$$

Среднее значение η^c_{km} имеет вид:

$$\mathbf{M}\eta^c_{km} = 2^{m\log_2 q - k}. \tag{3.4}$$

Рассмотрим теперь случай, когда порядок уравнений в системе является несущественным. В этом случае семейство $X_1, \ldots, X_k$ представляет собой случайную равновероятную k-выработку в коммутативном несимметричном 2^n-базисе. Число k-выработок, не покрывающих ν фиксированных элементов $X^{(m)}$ равно

$$\binom{2^{n-\nu}+k-1}{k}, \quad 0 \le \nu \le n.$$

Поэтому биномиальные моменты для $\eta^{\text{н}}_{km}$ - числа непокрытых элементов $X^{(m)}$ - имеют вид:

$$B^{\text{н}}_\nu(m,k) = \binom{n}{\nu}\frac{(2^{n-\nu}+k-1)k}{(2^n+k-1)k}, \quad \nu = 0,1,\ldots,n, \tag{3.5}$$

а точное распределение определяется формулой:

$$\mathbf{P}(\eta^{\text{н}}_{km} = r) = \sum_{\nu=r}^{n}(-1)^{\nu-r}\binom{\nu}{r}B^{\text{н}}_\nu(m,k), \quad r = 0,1,\ldots,n. \tag{3.6}$$

Для среднего значения $\eta_{km}^{\text{н}}$ имеем формулу

$$\mathbf{M}\eta_{km}^{\text{н}} = \frac{n}{2^k} + O\left(\frac{k^2}{2^k}\cdot\frac{n}{2^n}\right), \tag{3.7}$$

из которой следует, что

$$\mathbf{M}\eta_{km}^{\text{н}} = 2^{m\log_2 q - k} + o(1), \tag{3.8}$$

если выполнено хотя бы одно из условий $m \to \infty$ и $k \to \infty$.

Пусть теперь η_{km} - число решений системы случайных уравнений, совпадающее с $\eta_{km}^{\text{н}}$ и η_{km}^{c} при соответствующих вероятностных схемах. Оказывается, что при обеих вероятностных схемах для η_{km} справедлива следующая предельная теорема.

Теорема 4. *Пусть* $k = m\log_2 q + \gamma_m$ *и* $m \to \infty$.

Тогда

а) если $\gamma_m \to \infty$, *то* $\mathbf{P}(\eta_{km} = 0) \to 1$, *т.е. система (3.1) с вероятностью близкой к единице несовместна.*

б) если $\gamma_m \to \gamma$, $-\infty < \gamma < \infty$, *то* η_{km} *– число решений системы (3.1) – в пределе имеет распределение Пуассона с параметром* $\lambda = 2^{-\gamma}$.

в) если $\gamma_m \to -\infty$, *то случайная величина* $\eta'_{km} = (\eta_{km} - 2^{-\gamma_m})/\sqrt{2^{-\gamma_m}(1 - q^{-m}2^{-\gamma_m})}$ *асимптотически нормальна с параметрами (0,1).*

Для случая $\eta_{km} = \eta_{km}^{c}$ теорема не требует особого доказательства, так как в соответствии с формулой (3.3) η_{km}^{c} имеет биномиальное распределение.

Для $\eta_{km} = \eta_{km}^{\text{н}}$ из формулы (3.8) следует, что при выполнении условий пункта а) теоремы

$$\mathbf{M}\eta_{km}^{\text{н}} = \frac{1}{2^{\gamma_m}} + o(1) \tag{3.9}$$

и, следовательно, $\mathbf{M}\gamma_m \to 0$. Далее для доказательства пункта а) достаточно использовать формулу (3.6) и неравенство Бонферрони.

Из формулы (3.5) имеем следующие неравенства для оценки биномиальных моментов

$$\begin{gathered}\left(1 + \tfrac{1}{2^{n-\nu}}\tbinom{k}{2}\right)\mathrm{e}^{-\frac{1}{2^n}\binom{k}{2}} \le \frac{B_\nu^{\text{н}}(m,k)}{\binom{n}{\nu}2^{-k\nu}} \le \left(1 + \tfrac{1}{2^n}\tbinom{k}{2}\right)\mathrm{e}^{\frac{1}{2^{n-\nu}}\binom{k}{2}}, \\ \nu = 0, 1, \ldots.\end{gathered} \tag{3.10}$$

Для $\nu = o(\sqrt{n})$ в условиях пункта б) имеем следующее асимптотическое представление для биномиальных моментов:

$$B_\nu^{\text{н}}(m,k) = \frac{1}{\nu!}\left(\frac{n}{2^k}\right)^\nu \left(1 + O\left(\frac{(\log_2 n)^2}{2^n}\right)\right). \tag{3.11}$$

Отсюда следует, что для любого $\nu = 0, 1, \ldots$ при $m \to \infty$

$$B_\nu^{\text{н}}(m,k) \to \frac{1}{\nu!}\left(\frac{1}{2^\gamma}\right)^\nu.$$

Этим доказан пункт б) теоремы. Из неравенства (3.10) при выполнении условий пункта в) теоремы имеем следующую асимптотическую оценку при $m \to \infty$:

$$B_\nu^{\text{н}}(m,k) = \binom{n}{\nu}\frac{1}{2^{\nu k}}\left(1 + O\left(\frac{1}{\log_2 n}\right)\right) \tag{3.12}$$

равномерно для всех ν, удовлетворяющих ограничению

$$0 \le \nu \le n - 2\log_2\log_2 n - 1.$$

В свою очередь, для $n - 2\log_2\log_2 n \le \nu \le n$ имеем следующую равномерную оценку:

$$B_\nu^{\text{н}}(m,k) = O\left(\frac{1}{n^{\,n-4\log_2\log_2 n}}\right). \tag{3.13}$$

Производящую функцию $\eta_{km} = \eta_{km}^{\text{н}}$ запишем в следующем виде:

$$\mathbf{P}_{km}(x) = \sum_{\nu=0}^{n} B_\nu^{\text{н}}(m,k)(x-1)^\nu \tag{3.14}$$

и представим ее в виде двух сумм S_1 и S_2, имеющих пределы суммирования $0 \le \nu \le n - 2\log_2\log_2 n - 1$ и $n - 2\log_2\log_2 n \le \nu \le n$ соответственно. Тогда для любого x имеем следующее равномерное асимптотическое представление при $m \to \infty$:

$$\mathbf{P}_{km}(x) = \sum_{\nu=0}^{n-2\log_2\log_2 n-1} \binom{n}{\nu}\frac{(x-1)^\nu}{2^{k\nu}}\Big(1 + o(1)\Big) + o(1), \tag{3.15}$$

из которого следует, что при $m \to \infty$

$$\mathbf{P}_{km}(x) = \left(1 + \frac{(x-1)}{2^k}\right)^n (1 + o(1)). \tag{3.16}$$

Положим

$$M_m = \frac{1}{2^{\gamma_m}}, \tag{3.17}$$

$$\sigma_m^2 = \frac{1}{2^{\gamma_m}} \left(1 - \frac{1}{q^m 2^{\gamma_m}}\right). \tag{3.18}$$

Тогда характеристическая функция случайной величины η'_{km} может быть записана в следующем виде:

$$f_{km}(t) = \mathrm{e}^{-iM_m \frac{t}{\sigma_m}} \mathbf{P}_{km}\left(\mathrm{e}^{\frac{it}{\sigma_m}}\right).$$

При $m \to \infty$ для любого t имеем

$$\mathbf{P}_{km}\left(\mathrm{e}^{\frac{it}{\sigma_m}}\right) = \exp\left\{\frac{itM_m}{\sigma_m} - \frac{t^2}{2} + O\left(\frac{1}{\sigma_m}\right)\right\}.$$

В условиях пункта в) имеем $\sigma_m \to \infty$ при $m \to \infty$, поэтому для любого t

$$f_{km}(t) \to \mathrm{e}^{-t^2/2}.$$

Теорема доказана полностью.

Из равенств (3.3) и (3.16) следует, что случайная величина η_{km} при $\eta_{km} = \eta^{\mathrm{c}}_{km}$ и при $\eta_{km} = \eta^{\mathrm{н}}_{km}$ при $m \to \infty$ имеет распределение близкое к биномиальному с параметром $\mathbf{P}_k = \frac{1}{2^k}$. В соответствии с этим можно рассматривать еще одну вероятностную модель решений системы уравнений (3.1). Предполагаем, что при любых фиксированных $a_1, \ldots, a_k$, $(x_1, \ldots, x_m) \in X^{(m)}$, равновероятном выборе функций $f_1, \ldots, f_k$ имеем:

$$\mathbf{P}(f_1(x_1, \ldots, x_m) = a_1, \ldots, f_k(x_1, \ldots, x_m) = a_k) = \mathbf{P}_k. \tag{3.19}$$

Далее, при случайном независимом выборе элементов $(x_1, \ldots, x_m) \in X^{(m)}$ число решений системы (3.1) η^0_{km} представляет собой число успехов при n испытаниях в схеме Бернулли с вероятностью успеха $\mathbf{P}_k$, т.е.

$$\mathbf{P}(\eta^0_{km} = r) = \binom{n}{r} \mathbf{P}_r^k (1 - \mathbf{P}_k)^{n-r}, \quad r = 0, 1, \ldots, n. \tag{3.20}$$

Очевидна следующая теорема, являющаяся аналогом теоремы 1.

Теорема 5. *При $m \to \infty$*

а) если $q^m \mathbf{P}_k \to 0$, то распределение η^0_{km} асимптотически вырождено;

б) если $q^m \mathbf{P}_k \to \lambda$, то распределение η^0_{km} сходится к закону Пуассона с параметром λ;

в) если $q^m \mathbf{P}_k \to \infty$, то случайная величина $(\eta^0_{km} - q^m \mathbf{P}_k)/\sqrt{q^m \mathbf{P}_k (1 - \mathbf{P}_k)}$ асимптотически нормальна с параметрами (0.1).

Для любых случайных функций $f_1, \ldots, f_k$, удовлетворяющих условию (3.19), среднее число решений, в том числе без предположения независимости их появлений, равно

$$\mathbf{M}\eta_{km} = q^m \mathbf{P}_k. \tag{3.21}$$

Поэтому при $\delta_m = m + \log_q \mathbf{P}_k$ и $m \to \infty$ имеем

$$\begin{array}{lll} \text{а)} & \mathbf{M}\eta_{km} \to 0 & \text{при} \quad \delta_m \to -\infty, \\ \text{б)} & \mathbf{M}\eta_{km} \to q^\delta & \text{при} \quad \delta_m \to \delta;\ -\infty < \delta < \infty, \\ \text{в)} & \mathbf{M}\eta_{km} \to \infty & \text{при} \quad \delta_m \to \infty. \end{array} \tag{3.22}$$

Условие (3.21) выполняется также для некоторых классов случайных функций $f_1, \ldots, f_k$. В соответствии с этим для этих классов выполнены свойства (3.22). В равновероятном случае эти свойства, грубо говоря, означают, что при $m \to \infty$ если k велико по сравнению с m, то система несовместна, если k близко к m, то система в среднем имеет немного решений и, наконец, если k мало по сравнению с m, то число решений стремится к бесконечности.

Список литературы

[1] Landsberg G. Uber eine Anzahlbestimmung und eine damit zusammenhangende Reihe, J. Reine Angew. Math., 111, 1895, 87-88.

[2] Коваленко И.Н. О предельном распределении числа решений случайной системы линейных уравнений в классе булевых функций. "Теория вероятностей и ее применение", XII, 1967г., 51-61.

[3] Коваленко И.Н., Левитская А.А., Савчук М.Н. Избранные задачи вероятностной комбинаторики. "Наукова думка", Киев, 1988г.

[4] Колчин В.Ф. Системы случайных уравнений. МИЭМ, Москва, 1988г.

[5] Эндрюс Г. Теория разбиений. "Наука", Москва, 1982г.

[6] Сачков В.Н. Вероятностные методы в комбинаторном анализе. "Наука", Москва, 1978г.

[7] Сачков В.Н. Асимптотическое поведение t-минимальных покрытий множеств. "Дискретная математика", 5, 1993г., N1.

[8] Сачков В.Н. Случайные покрытия и системы функциональных уравнений. Москва, Интеллектуальные системы, т.2, вып. 1-4, 297-315.

[9] Балакин Г.В. Введение в теорию случайных систем уравнений. Труды по дискретной математике, т.1, 1-18, (под ред. В.Н.Сачкова и др.), ТВП, 1997г.