А. В. Ш а п о в а л о в (Москва, ТВП)**. Характеристики случайных систем линейных уравнений, содержащих одночленные уравнения.**

Пусть $\Lambda = \{f_1, \dots, f_{|\Lambda|}\}$ — множество линейных функций над конечным полем из q элементов $\mathrm{GF}(q)$, зависящих от $1, \dots, m$ переменных, $f_1(y_1) = y_1$; $c, c_1, c_{1,0}, c_{1,1}, \dots, c_{1,q-1}$ — неотрицательные константы, $0 < c_1 \leqslant 1$, $c_{1,0} + \dots + c_{1,q-1} = c_1$, $c_{1,a} \neq c_1$, $a = 0, 1, \dots, q-1$; $\lambda = (cc_1)^2/2$, $\mu_1 = c^2(c_{1,0}^2 + \dots + c_{1,q-1}^2)/2$, $\mu_0 = \lambda - \mu_1$.

Случайная система линейных уравнений S относительно n неизвестных $x_1, \dots, x_n$ состоит из $M = M(n)$ уравнений, которые выбираются последовательно, случайно и независимо друг от друга; вероятность появления уравнения $y_1 = a$ равна $c_{1,a}$ для каждого $a \in \mathrm{GF}(q)$; с вероятностью $1 - c_1$ выбирается уравнение с функцией из Λ, зависящее более, чем от одной переменной. Выбор конкретной функции из Λ и значения правой части из $\mathrm{GF}(q)$ осуществляется по какому-то вероятностному закону. Выбор упорядоченного множества неизвестных $x_{s_1}, \dots, x_{s_i}$ для каждого уравнения с функцией из Λ, зависящей от i переменных, осуществляется случайно, равновероятно и бесповторно из всех $n(n-1)\cdots(n-i+1)$ возможных наборов неизвестных по i штук, $i = 1, \dots, m$. Система S удовлетворяет условию **B**, если правая часть каждого ее уравнения принимает значения $0, 1, \dots, q-1$ с равными вероятностями. *Заведомо совместная случайная система линейных уравнений* $S^{(c)}$ определяется аналогично S, но правые части реализаций $S^{(c)}$ зависят от левых и являются результатом подстановки в левые части некоторого n-мерного вектора с компонентами из $\mathrm{GF}(q)$ (истинного решения). Пусть ζ_n и $\zeta_n^{(c)}$ — числа решений случайных систем уравнений S и $S^{(c)}$, деленные на q^{n-M}.

Теорема. *Если* $n \to \infty$, $M \sim cn$, $c > 0$, *то* $\mathbf{P}\{\zeta_n = 0\} \sim 1 - e^{-\mu_0}$ *и*

$$\mathbf{P}\{\zeta_n = q^k\} \sim 1 - e^{-\mu_0-\mu_1}\frac{\mu_1^k}{k!}, \quad \varliminf_{n\to\infty} \mathbf{E}\,\zeta_n^{k+1} \geqslant e^{-\mu_0+\mu_1(q^{k+1}-1)} = e^{(cc_1)^2(q^k-1)/2},$$

$$\mathbf{P}\{\zeta_n^{(c)} = q^k\} \sim e^{-\lambda}\frac{\lambda^k}{k!}, \quad \mathbf{E}\,(\zeta_n^{(c)})^{k+1} \sim e^{\lambda(q^{k+1}-1)} = e^{(cc_1)^2(q^{k+1}-1)/2}, \quad k = 0, 1, \dots;$$

причем $\mathbf{E}\,\zeta_n^{k+1} \sim e^{-\mu_0+\mu_1(q^{k+1}-1)}$, $k = 0, 1, \dots$, *при условии* **B**.

Результат не зависит от способа выбора уравнений, зависящих от двух и более неизвестных, он справедлив также для выборки переменных по схеме с возвращением. При $c_1 = 1$ вероятность $\mathbf{P}\{\zeta_n > 0\}$ совместности системы S может быть получена из результатов [1], она оценена в [2] для $q = 2$, $c_{1,0} = c_{1,1} = 1/2$, предельные распределения для ζ_n и $\zeta_n^{(c)}$ получены в [3], для $\zeta_n^{(c)}$ — в [2] при $q = 2$, $M = (n/2)\log n + cn + o(n)$.

СПИСОК ЛИТЕРАТУРЫ

1. *Балакин Г. В.* Системы случайных уравнений над конечным полем. — Труды по дискретной математике, 1998, т. 2, с. 21–37.
2. *Колчин В. Ф.* Системы случайных уравнений. М.: МИЭМ, 1988.
3. *Shapovalov A. V.* The Number of Decisions of Random Monomial and Binomial Linear Systems of Equations. – In: Proceedings of the Fourth International Petrozavodsk Conference «Probabilistic Methods in Discrete Mathematics», Petrozavodsk, Russia, June 3–7, 1996. Utrecht: VSP, 1997, p. 333–342.