

А. В. Шаповалов (Москва, ТВП). **Предельные характеристики случайной заведомо совместной системы линейных уравнений над конечным полем.**

Для каждого $i = 2, \dots, m$ через Λ_i обозначим некоторым образом упорядоченное множество всех линейных функций над конечным полем из q элементов $\text{GF}(q)$, зависящих ровно от i переменных. Пусть заданы такие неотрицательные константы $c_2, \dots, c_m, c_{2,1}, c_{2,2}$ ($c_{2,2} = 0$ при $q = 2$), что $c_2 + \dots + c_m = 1$, $c_2 = c_{2,1} + c_{2,2}$.

Случайная заведомо совместная система линейных уравнений S над конечным полем $\text{GF}(q)$ относительно n неизвестных $x_1, \dots, x_n$ состоит из M уравнений, которые выбираются последовательно, случайно и независимо друг от друга. Вероятность появления уравнения с функцией из Λ_i равна c_i , $i = 2, \dots, m$. При $q > 2$ ($q = 2$) вероятности появления в уравнении функций $y_1 - y_2$ и $y_1 + y_2$ равны $c_{2,1}$ и $c_{2,2}$ (c_2), соответственно. Выбор i неупорядоченных переменных для каждого уравнения с функцией из Λ_i осуществляется случайно и равновероятно из всех возможных неупорядоченных наборов неизвестных по i штук по схеме без возвращения. В уравнениях с функцией $y_1 - y_2$ выбранные переменные упорядочиваются независимо, случайно и равновероятно. При условии появления в левой части уравнений функций, зависящих от i переменных, $i = 3, \dots, m$, выбор конкретной функции i переменных, значения правой части уравнения из $\text{GF}(q)$, а также упорядочение переменных для несимметрических функций осуществляется некоторым произвольным образом. Правая часть каждого уравнения равна значению функции в ее левой части, получаемому при подстановке вместо $x_1, \dots, x_n$ компонент некоторого вектора $(b_1, \dots, b_n)$, принадлежащих $\text{GF}(q)$.

Обозначим ζ число решений S , деленное на величину q^{n-M} . Пусть $(s)_2 = s(s-1)$, $\lambda = -(1/4)\log((1-2cc_2)(1+2c(c_{2,2}-c_{2,1}))) - cc_2$. Асимптотические формулы приводятся при $n \rightarrow \infty$, $M = M(n)$.

Теорема. Если c — константа, $c_2 > 0$ и выполнено условие

$$M \sim cn, \quad 0 < c < (c_2(2)_2 + c_3(3)_2 + \dots + c_m(m)_2)^{-1}, \quad (1)$$

то $\mathbf{P}\{\zeta = q^k\} \sim e^{-\lambda} \lambda^k / k!$, $k = 0, 1, 2, \dots$, и $\mathbf{E}\zeta^r \sim e^{\lambda(q^r-1)}$, $r = 1, 2, \dots$.

Если $M = o(n)$ или выполнено условие (1) и $c_2 = 0$, то $\mathbf{P}\{\zeta = 1\} \sim 1$ и $\mathbf{E}\zeta^r \sim 1$, $r = 1, 2, \dots$.

При $q = 2$ предельные распределения для ζ получены в работе [3]. Из результатов статьи [2] можно получить распределение числа решений для соотношения n и $M(n)$, когда $q^{n-M}\mathbf{E}\zeta = O(1)$, случай $q = 2$, $m = 2$ для выборки неизвестных по схеме с возвращением рассмотрен в книге [1]. Теорема справедлива и при выборке по схеме с возвращением, при этом величина λ заменяется на $\hat{\lambda} = \lambda + cc_2$.

СПИСОК ЛИТЕРАТУРЫ

1. Колчин В. Ф. Системы случайных уравнений. М.: МИЭМ, 1988.
2. Копытцев В. А. Предельные теоремы для числа решений системы случайных уравнений. — Теория вероятн. и ее примен., 2000, т. 45, в. 3, с. 52–72.
3. Shapovalov A. V. Characteristics of random systems of Boolean equations with non-regular left-hand side. — In: Proceedings of the Fifth International Petrozavodsk Conference. Utrecht, Boston, Koln, Tokyo: VSP, 2002, p. 333–342.