

В. И. Масол, Н. В. Слободян (Киев, КНУ). Оценка скорости сближения распределения числа ложных решений системы нелинейных случайных уравнений над полем $\text{GF}(2)$ с распределением Пуассона.

Рассмотрим систему уравнений

$$\sum_{k=1}^{g_i(n)} \sum_{1 \leq j_1 < \dots < j_k \leq n} a_{j_1 \dots j_k}^{(i)} x_{j_1} \dots x_{j_k} = b_i, \quad i = 1, 2, \dots, N, \quad (1)$$

над полем $\text{GF}(2)$ при условии (A): коэффициенты $a_{j_1 \dots j_k}^{(i)}$ ($1 \leq j_1 < \dots < j_k \leq n$, $k = 1, 2, \dots, g_i(n)$, $i = 1, 2, \dots, N$) — независимые случайные величины, $\mathbf{P}\{a_{j_1 \dots j_k}^{(i)} = 1\} = 1 - \mathbf{P}\{a_{j_1 \dots j_k}^{(i)} = 0\} = p_{ik}$; элементы b_i ($i = 1, 2, \dots, N$) — результат подстановки в левую часть системы (1) фиксированного n -мерного $(0,1)$ -вектора $\bar{x}^0$, имеющего $0 < \rho(n) \leq n$ ненулевых компонент; функция $g_i(n)$ — неслучайная, $g_i(n) \in \{2, 3, \dots, n\}$ ($i = 1, 2, \dots, N$).

Обозначим $M(\bar{x}^0, f(n))$ множество всех n -мерных векторов $\bar{x}$, отличных от $\bar{x}^0$, удовлетворяющих неравенству $|\bar{x}| \geq f(n)$, $f(n) \in \{0, 1, 2, \dots, n\}$.

Число всех ложных решений (число решений системы (1), отличных от $\bar{x}^0$), принадлежащих множеству $M(\bar{x}^0, f(n))$, обозначим ν_n .

Теорема. Пусть выполняются условия: (A); $n - N = m = \text{const}$; существует такая функция $\varphi(n)$, $\varphi(n) \leq n$, что $f(n) = o(\varphi(n))$, $f(n) \geq 2$ при $n \rightarrow \infty$; для произвольного $i = 1, 2, \dots, N$ существует такое множество T_i , $T_i \neq \emptyset$, что при всех достаточно больших n

$$T_i \subseteq \{2, \dots, g_i(n)\}, \quad \delta_{it}(n) \leq p_{it} \leq 1 - \delta_{it}(n), \quad t \in T_i; \quad (2)$$

для фиксированного целого $l \geq 0$ и $\tau > 0$ существует такое натуральное $n_0 = n_0(\varepsilon_0, l)$, что для всех $n \geq n_0$

$$2^\gamma B(n) < \varepsilon_0, \quad (3)$$

где $B(n) = \sum_{i=1}^N \exp\{-2 \sum_{t \in T_i} \delta_{it}(n) C_{f(n)-1}^{t-1}\}$, $\gamma = [(\log_2 \mu(k, n))/\tau]$, $\mu(k, n) = (n - \rho(n))/(\varphi(n) \ln n)$, $\mu(k, n) \geq 2^{\tau k}$, $[\cdot]$ — знак целой части.

Тогда для фиксированного $k = 0, 1, \dots$

$$\left| \mathbf{P}\{\nu_n = k\} - \frac{\lambda^k}{k!} e^{-\lambda} \right| \leq \left(\frac{2e\lambda}{\gamma} \right)^\gamma ((1 + \varepsilon_0)(2 + 4\Theta_3) + (1 + 2\varepsilon_0)(\Theta_1 + \Theta_2)) + \gamma \left(\frac{2e\lambda}{k} \right)^k e^{2\lambda B(n)} + \gamma \left(\frac{e\lambda}{k} \right)^k e^\lambda (1 + 2\varepsilon_0)((\Theta_1 + \Theta_2) + (1 + \varepsilon_0)\Theta_3), \quad (4)$$

где

$$\begin{aligned} \lambda &= 2^m, \quad \Theta_1 = \gamma 2^{-(n-\rho(n)) + (\gamma-1)\varepsilon\varphi(n)} \sqrt{\varepsilon\varphi(n)} \left(\frac{(n-\rho(n))e}{\varepsilon\varphi(n)} \right)^{\varepsilon\varphi(n)}, \\ \Theta_2 &= 2^{-n} \exp \left\{ \varepsilon 2^\gamma \varphi(n) \left(\gamma + \ln \left(\frac{n\varepsilon}{\varepsilon 2^\gamma \varphi(n)} \right) \right) + 2^\gamma + 2 \ln(\varepsilon 2^\gamma \varphi(n)) \right\}, \\ \Theta_3 &= 2^{-m} \exp \left\{ -\frac{n-\rho(n)}{2^\gamma} + 2\gamma 2^\gamma \varepsilon \varphi(n) + 2^\gamma + 2 \ln(2^\gamma \varepsilon \varphi(n)) + 2^{\gamma+1} \varepsilon \varphi(n) \ln \left(\frac{\tilde{\rho}(n)e}{2^\gamma \varepsilon \varphi(n)} \right) \right\}, \end{aligned}$$

$\tilde{\rho}(n) = \max\{\rho(n), n - \rho(n)\}$, $\varepsilon \in (0, 1)$. Здесь $0^0 \equiv 1$.

П р и м е р. Если выполняются условия: $T_i = \{3\}$, $\delta_{it}(n) = 1/2$, $t \in T_i$, $i = 1, \dots, N$, $\rho(n) = n/2$, $\varphi(n) = (\ln n)^{3/2}$, $f(n) = [\ln n]$, $\tau = 2$, $m = -8$, $\varepsilon = 1/2$, то имеют место (2), (3) и в силу (4)

$$|\mathbf{P}\{\nu_{1006} = 1\} - \lambda e^{-\lambda}| \leq 0,042, \quad |\mathbf{P}\{\nu_{15000} = 1\} - \lambda e^{-\lambda}| \leq 0,0002.$$