V. A. Kopyttsev, On the distribution of the number of solutions of random systems of equations which are known to be consistent, *Teor. Veroyatnost. i Primenen.*, 1995, Volume 40, Issue 2, 430–437

СПИСОК ЛИТЕРАТУРЫ

1. *Давыдов Ю. А., Лифшиц М. А.* Метод расслоений в некоторых вероятностных задачах. — Итоги науки и техники. Серия Теория вероятностей, матем. статистика, теор. киберн. М.: ВИНИТИ, 1984, т. 22, с. 61–158.
2. *Давыдов Ю. А.* О распределениях кратных стохастических интегралов Винера–Ито. — Теория вероятн. и ее примен., 1990, т. 35, в. 1, с. 51–62.
3. *Давыдов Ю. А., Розин А. Л.* О временах пребывания для функции и случайных процессов. — Теория вероятн. и ее примен., 1978, т. 23, в. 3, с. 650–654.
4. *Major P.* Multiple Wiener–Itô integrals. — Lect. Notes Math., 1981, v. 849, p. 1–135.

Поступила в редакцию
25.II.1992

КОПЫТЦЕВ В. А.*

О РАСПРЕДЕЛЕНИИ ЧИСЛА РЕШЕНИЙ СЛУЧАЙНЫХ ЗАВЕДОМО СОВМЕСТНЫХ СИСТЕМ УРАВНЕНИЙ

Исследуется распределение числа решений систем, в которых каждое уравнение задается путем подстановки в функцию $\varphi(u_1,\dots,u_d)$, $u_j \in \{0,1\}$, двоичных неизвестных, выбранных случайно и без возвращения из совокупности $\{x_1,\dots,x_n\}$, $n \geqslant d$. Доказывается, что в определенных условиях распределение двоичного логарифма числа решений сходится к распределению Пуассона.

Ключевые слова и фразы: случайные системы уравнений, истинное решение, число решений, распределение Пуассона.

1. Введение. Пусть $\varphi(u_1,\dots,u_d)$ — функция, заданная на множестве d-мерных двоичных векторов и принимающая значения в произвольном алфавите A, элементы которого без ограничения общности обозначим целыми числами от 0 до r, $A = \{0,1,\dots,r\}$, $r \leqslant 2^d$; G — подгруппа группы инерции функции φ в симметрической группе подстановок σ_d.

Рассмотрим систему уравнений:

$$\left\{\varphi(x_{j_{i_1}},\dots,x_{j_{i_d}}) = \alpha_i,\ i = \overline{1,t}\right\}. \tag{1}$$

Неизвестные каждого уравнения системы (1) выбираются независимо и без возвращения из совокупности $\{x_1,\dots,x_n\}$ и затем размещаются в функции φ на места аргументов $u_1,\dots,u_d$. На множестве всех возможных левых частей одного уравнения введено отношение эквивалентности. Две левые части эквивалентны, если они содержат один и тот же набор неизвестных и размещения неизвестных эквивалентны относительно группы подстановок G. На множестве Ω классов эквивалентных левых частей задано равномерное распределение вероятностей:

$$\mathbf{P}(\omega) = \frac{1}{|\Omega|}, \qquad |\Omega| = C_n^d\,\frac{d!}{|G|}, \qquad \omega \in \Omega. \tag{2}$$

*ФАПСИ, Б. Кисельный пер., 4, 103031 Москва, Россия.

Левая часть системы (1) есть результат t независимых испытаний с распределением (2) на исходах. Правая часть задается равенствами $\alpha_i = \varphi(x^0_{j_{i_1}}, \ldots, x^0_{j_{i_d}})$, $i = \overline{1,t}$, при некотором фиксированном векторе $x^0 = (x^0_1, \ldots, x^0_n)$.

По существующей терминологии рассматриваемая система называется случайной заведомо совместной системой уравнений [1]. Вектор x^0 называется истинным решением.

Целью предлагаемой работы является изучение асимптотического поведения числа решений ξ_t системы (1). В работе показано, что утверждение теоремы 2, доказанной в работе [2] для частного случая системы (1), переносится на общий случай.

2. Основной результат. Представим функцию $\varphi(u) = \varphi(u_1, \ldots, u_d)$ в виде d-мерного единичного куба, каждая вершина u которого отмечена меткой $\varphi(u)$. Любой подкуб размерности 1 назовем ребром d-мерного куба. Координату образующих ребро вершин u^1, u^2, по которой эти вершины как векторы различаются, назовем свободной.

Обозначим $M_k^{(\upsilon)} = \{\rho\}$ множество ребер таких, что вершины u^1, u^2 из ребра $\rho = (u^1, u^2) \in M_k^{(\upsilon)}$ содержат k совпадающих нулевых координат (и, следовательно, $d-k-1$ совпадающих единичных координат) и, кроме того, $\varphi(u^1) = \varphi(u^2) = \nu$.

Для пары ребер $\rho_1, \rho_i \in M_k^{(\upsilon)}$ введем множество $W(\rho_1, \rho_i)$ всех подстановок, переводящих нулевые, единичные и свободную координаты вершин, образующих ребро ρ_1, соответственно в нулевые, единичные и свободную координаты вершин, образующих ребро ρ_i. Положим

$$W_k^{(\upsilon)} = \bigcup_{i=1}^{|M_k^{(\upsilon)}|} W(\rho_1, \rho_i).$$

Нетрудно заметить, что $|W_k^{(\upsilon)}| = |M_k^{(\upsilon)}|\, k!\,(d-k-1)!$.

Будем считать, что две подстановки a, b из множества $W_k^{(\upsilon)}$ эквивалентны, если найдется подстановка $c \in G$ такая, что $a * c = b$. Обозначим $\lambda_G^{(\upsilon)}(k)$ число классов эквивалентных подстановок в множестве $W_k^{(\upsilon)}$ и положим

$$\lambda_G(k) = \sum_{\upsilon=0}^{r} \lambda_G^{(\upsilon)}(k). \tag{3}$$

Теорема. *Пусть выполняются следующие условия*:

1) *истинное решение* x^0 *содержит* $n_0 = \theta n$ *нулей и* $n_1 = (1-\theta)n$ *единиц*, $\delta \leqslant \theta \leqslant 1-\delta$, $0 < \delta = \text{const}$;

2) *число неизвестных* n *и число уравнений* t *связаны равенством* $t = \gamma^{-1} n \times (\ln n + z)$, *где* $z = O(1)$,

$$\gamma = d - |G| \sum_{k=0}^{d-1} \frac{\theta^k}{k!} \frac{(1-\theta)^{d-1-k}}{(d-1-k)!} \lambda_G(k). \tag{4}$$

Тогда

$$\mathbf{P}(\xi_t = 2^{m+\Delta}) = \frac{e^{-mz}}{m!} \exp\Big\{ -e^{-z} + O(1) \Big\}, \tag{5}$$

при $n \to \infty$, *где* $\Delta = 0$, *если существуют два набора значений аргументов* u^i, u^j *функции* $\varphi(u)$ *такие, что*

$$u^i \oplus u^j = (1, \ldots, 1), \qquad \varphi(u^i) \neq \varphi(u^j); \tag{6}$$

и $\Delta = 1$, *если* $\varphi(u) \neq \text{const}$ *и для любой пары* u^i, u^j *такой, что* $u^i \oplus u^j = (1, \ldots, 1)$, *выполняется равенство* $\varphi(u^i) = \varphi(u^j)$.

Доказательство. Пусть для некоторой пары u^i, u^j выполняется условие (6). Сначала покажем, что

$$\mathbf{E}\xi_t = \sum_k k\,\mathbf{P}(\xi_t = k) = \exp\left\{e^{-z} + o(1)\right\}. \tag{7}$$

Обозначим I_0 (I_1) множество индексов нулевых (соответственно, единичных) координат истинного решения x^0, $|I_0| = n_0 = \theta n$, $|I_1| = n_1 = (1-\theta)n$. Рассмотрим произвольный вектор $x^1 = (x_1^1, \ldots, x_n^1)$. Пусть x^1 имеет q единичных; $n_0 - q$ нулевых координат с индексами из множества I_0, и p нулевых, $n_1 - p$ единичных координат с индексами из множества I_1. Обозначим $P(p,q)$ вероятность того, что вектор x^1 удовлетворяет одному уравнению системы (1). Нетрудно заметить, что величина $P(p,q)$ не зависит от конкретных вариантов пересечения множества индексов q единичных координат вектора x^1 с множеством I_0 и от конкретных вариантов пересечения множества индексов p нулевых координат вектора x^1 с множеством I_1. Поэтому

$$\mathbf{E}\xi_t = \sum_{q=0}^{n_0}\sum_{p=0}^{n_1} C_{n_0}^q C_{n_1}^p \left[P(p,q)\right]^t. \tag{8}$$

Оценим вероятность $P(p,q)$. Представим $P(p,q)$ в виде суммы двух слагаемых, соответствующих двум типам левых частей одного уравнения. К первому типу отнесем левые части, содержащие не более одного неизвестного, имеющего различные значения в векторах x^0, x^1. Ко второму типу отнесем все остальные левые части; их число есть $O(n^{d-2}(p+q)^2)$. Получим:

$$P(p,q) = P'(p,q) + O\left(\left(\frac{p+q}{n}\right)^2\right),$$

где

$$P'(p,q) = \left[C_n^d \frac{d!}{|G|}\right]^{-1}\left[C_{n-p-q}^d \frac{d!}{|G|} + (p+q)\sum_{k=0}^{d-1} C_{n_0-q}^k C_{n_1-p}^{d-1-k}\lambda_G(k)\right]. \tag{9}$$

Отсюда вытекает оценка:

$$P(p,q) = 1 - \gamma\frac{p+q}{n} + O\left(\left(\frac{p+q}{n}\right)^2\right), \tag{9'}$$

где величина γ определяется формулой (4).

Разобьем сумму (8) на три слагаемых:

$$\mathbf{E}\xi = \sum_{0 \leqslant p+q \leqslant n^{1/3}} + \sum_{n^{1/3} < p+q \leqslant \varepsilon n} + \sum_{\varepsilon n < p+q \leqslant n} = \Sigma_1 + \Sigma_2 + \Sigma_3, \tag{10}$$

и оценим каждое слагаемое в отдельности. Пусть $t = \gamma^{-1}n(\ln n + z)$. При $p+q \leqslant n^{1/3}$

$$P(p,q) = \exp\left\{-\gamma^{-1}n(\ln n + z)\left(\frac{p+q}{n}\gamma + O(n^{-4/3})\right)\right\}$$

$$= \exp\left\{-(p+q)(\ln n + z) + O\left(\frac{\ln n}{n^{1/3}}\right)\right\}.$$

Следовательно,

$$\Sigma_1 = \sum_{0\leqslant p+q\leqslant n^{1/3}} \frac{\theta^q}{q!}\frac{(1-\theta)^p}{p!}\exp\left\{-z(p+q)+O\left(\frac{\ln n}{n^{1/3}}\right)\right\} = \exp\left\{e^{-z}+o(1)\right\}.$$

Оценим Σ_2. При достаточно малой величине ε в области $(p+q)/n \leqslant \varepsilon$ выполняется неравенство $P(p,q) \leqslant 1-\gamma_\varepsilon(p+q)/n$, где $\gamma_\varepsilon < \gamma$, причем $\gamma_\varepsilon \to \gamma$, если $\varepsilon \to 0$. Поэтому, учитывая, что функция $f(y) = -\ln(1-\gamma_\varepsilon y)$ выпукла вниз, а функция $h(y) = -y\ln y - (1-y)\ln(1-y)$ выпукла вверх в интервале $0 < y < \varepsilon$, получим:

$$\begin{aligned}
\Sigma_2 &\leqslant \sum_{n^{1/3}\leqslant p+q\leqslant n\varepsilon} C_n^{p+q}\exp\left\{-tf\left(\frac{p+q}{n}\right)\right\}\\
&\leqslant \sum_{n^{1/3}<p+q\leqslant n\varepsilon}\exp\left\{-n\left[\frac{t}{n}f\left(\frac{p+q}{n}\right)-h\left(\frac{p+q}{n}\right)+O\left(\frac{\ln n}{n}\right)\right]\right\}\\
&\leqslant n^2\exp\left\{-n\left[\frac{t}{n}f\left(\frac{p+q}{n}\right)-h\left(\frac{p+q}{n}\right)+O\left(\frac{\ln n}{n}\right)\right]\right\}\Bigg|_{(p+q)/n=n^{1/3}/n}\\
&\leqslant n^2\exp\left\{-\left(\frac{\gamma_\varepsilon}{\gamma}-\frac{2}{3}\right)n^{1/3}\ln n+O\left(n^{1/3}\right)\right\} = o(1),
\end{aligned}$$

если ε достаточно мало.

Осталось показать, что Σ_3 есть $o(1)$. Исследуем поведение вероятности $P(p,q)$ при $n\to\infty$, $(p+q)/n \geqslant \varepsilon$. Рассмотрим три возможных случая относительно значений p, q при условии, что $p+q \geqslant \varepsilon n$.

1. $p \geqslant (\varepsilon/2)n$, $q \leqslant (\varepsilon/2)n$, и, следовательно, $n_0 - q \geqslant n(\theta-\varepsilon/2)$. Поскольку $\varphi \neq \text{const}$, то $\varphi(u^1) \neq \varphi(u^j)$, где $u^1 = (0,\ldots,0)$, u^j — некоторый вектор. Пусть u^j содержит k единиц. Тогда

$$1-P(p,q) \geqslant \frac{C_p^k C_{n_0-q}^{d-k}}{C_n^d d!/|G|} \geqslant \frac{|G|}{d!}\left(1+O(n^{-1})\right)\min_{0\leqslant k\leqslant d} C_d^k\left(\frac{\varepsilon}{2}\right)^k\left(\theta-\frac{\varepsilon}{2}\right)^{d-k}.$$

Отсюда вытекает, что $P(p,q) \leqslant 1-\delta(\varepsilon)$ при некотором $\delta(\varepsilon) > 0$, если $\varepsilon < 2\theta$, $\theta \geqslant \delta > 0$.

2. $p \leqslant (\varepsilon/2)n$, $q \geqslant (\varepsilon/2)n$, и, следовательно, $n_1 - p \geqslant (1-\theta-\varepsilon/2)n$. Рассуждая так же, как в первом случае, с заменой вектора $(0,\ldots,0)$ на вектор $(1,\ldots,1)$, получим, что $P(p,q) \leqslant 1-\delta(\varepsilon)$ при некотором $\delta(\varepsilon) > 0$, если $\varepsilon < 2(1-\theta)$, $1-\theta \geqslant \delta > 0$.

3. $p \leqslant (\varepsilon/2)n$, $q \geqslant (\varepsilon/2)n$. Для некоторой пары векторов u^i, u^j имеем: $u^i \oplus u^j = (1,\ldots,1)$, $\varphi(u^i) \neq \varphi(u^j)$. Пусть вектор u^i содержит k нулей, а вектор u^j содержит $d-k$ нулей. Тогда

$$\begin{aligned}
1-P(p,q) &\geqslant \frac{C_p^k C_q^{d-k}}{C_n^d d!/|G|} + \frac{C_q^k C_p^{d-k}}{C_n^d d!/|G|} \geqslant \frac{|G|}{d!}\left(1+O(n^{-1})\right)\min_{0\leqslant k\leqslant d} 2C_d^k\left(\frac{\varepsilon}{2}\right)^k\left(\frac{\varepsilon}{2}\right)^{d-k}\\
&= \frac{|G|}{d!}\,2\left(\frac{\varepsilon}{2}\right)^d\left(1+O(n^{-1})\right).
\end{aligned}$$

Следовательно, и в этом случае найдется число $\delta(\varepsilon) > 0$ такое, что $P(p,q) \leqslant 1-\delta(\varepsilon)$.

Таким образом, показано, что вероятность $P(p,q)$ в области $\varepsilon n \leqslant p+q \leqslant n$ отделена от единицы некоторой фиксированной величиной. Поэтому

$$\sum_{\varepsilon n<p+q\leqslant n} C_{n_1}^p C_{n_0}^q [P(p,q)]^t = o(1).$$

Соотношение (7) доказано.

Осталось показать, что

$$\mathbf{P}\Big(\xi_t = 2^m\Big) = \frac{e^{-mz}}{m!}\exp\Big\{-e^{-z} + o(1)\Big\}. \tag{11}$$

Обозначим $\overline{X}_i$ множество решений уравнения с номером i, $1 \leqslant i \leqslant t$, и определим множество $X_i \subseteq \{x_1, \ldots, x_n\}$ следующим образом: $x_j \in X_i \Longleftrightarrow (x_1^0, \ldots, x_{j-1}^0, x_j^0 \oplus 1, x_{j+1}^0, \ldots, x_n^0) \in \overline{X}_i$. Неизвестные из множества X_i назовем несущественными относительно истинного решения в уравнении с номером i.

Положим $\eta_t = |\cap_{i=1}^t X_i|$. Величина η_t равна числу неизвестных, несущественных относительно истинного решения в каждом уравнении системы.

Найдем распределение случайной величины η_t. По формуле включения и исключения получим:

$$\mathbf{P}(\eta_t = m) = \sum_s (-1)^s C_{m+s}^s \sum_k C_{n_0}^k C_{n_1}^{m+s-k} \times \mathbf{P}\Big(A_{j_1}(t), \ldots, A_{j_k}(t), B_{j_{k+1}}(t), \ldots, B_{j_{m+s}}(t)\Big),$$

где $A_{j_n}(t)$ — событие, состоящее в том, что

$$x_{j_h} \in \bigcap_{i=1}^t X_i \bigcap \Big\{x_\tau\colon x_\tau^0 = 0\Big\}, \qquad x_{j_h}^0 = 0;$$

B_{j_h} — событие, состоящее в том, что

$$x_{j_h} \in \bigcap_{i=1}^t X_i \bigcap \Big\{x_\tau\colon x_\tau^0 = 1\Big\}, \qquad x_{j_h}^0 = 1.$$

Справедливы следующие равенства:

$$\begin{aligned}
&\mathbf{P}\Big(A_{j_1}(t), \ldots, A_{j_k}(t), B_{j_{k+1}}(t), \ldots, B_{j_{m+s}}(t)\Big) \\
&\quad = \mathbf{P}^t\Big(A_{j_1}(1), \ldots, A_{j_k}(1), B_{j_{k+1}}(1), \ldots, B_{j_{m+s}}(1)\Big) \\
&\quad = \left[P'(m+s-k, k) + O\Big(\frac{s^2}{n^2}\Big)\right]^t,
\end{aligned}$$

где величина $P'(m+s-k, k)$ определяется в соответствии с формулой (9). Следовательно,

$$\begin{aligned}
&\mathbf{P}\Big(A_{j_1}(t), \ldots, A_{j_k}(t), B_{j_{k+1}}(t), \ldots, B_{j_{m+s}}(t)\Big) \\
&\quad = \left(1 - \gamma\frac{m+s}{n} + O\Big(\frac{\ln^2 n}{n^2}\Big)\right)^t \\
&\quad = n^{-(m+s)}\exp\left\{-(m+s)z + O\Big(\frac{\ln^3 n}{n}\Big)\right\},
\end{aligned}$$

при условии, что $s \leqslant \ln n$, $t = \gamma^{-1} n(\ln n + z)$. Таким образом, с учетом неравенств Бонферрони для формулы включения и исключения [3], получим, что

$$\mathbf{P}(\eta_t = m) \approx \sum_{s \leqslant \ln n} (-1)^s C_{m+s}^s C_n^{m+s} n^{-(m+s)} \exp\left\{-(m+s)z + O\Big(\frac{\ln^3 n}{n}\Big)\right\}$$

$$= \sum_{s \leqslant \ln n} (-1)^s \frac{1}{m!s!} \exp\left\{ -(m+s)z + O\left(\frac{\ln^3 n}{n}\right)\right\}$$

$$= \frac{e^{-mz}}{m!} \exp\left\{ -e^{-z} + o(1)\right\}. \tag{12}$$

Занумеруем все возможные пары неизвестных числами от 1 до C_n^2 и для пары (x_ν, x_μ) с номером j введем индикаторы событий: $I_{j,i}^{(1)} = I(A_{j,i}^{(1)})$, $I_{j,i}^{(2)} = I(A_{j,i}^{(2)})$, $I_j = I(A_j)$, где событие $A_{j,i}^{(1)}$ состоит в том, что $x_\nu, x_\mu \in X_i$ и уравнение с номером i содержит не более одного неизвестного из пары (x_ν, x_μ); событие $A_{j,i}^{(2)}$ состоит в том, что $x_\nu, x_\mu \in X_i$ и уравнение с номером i содержит оба неизвестных из пары (x_ν, x_μ); событие A_j состоит в том, что $x_\nu, x_\mu \in \cap_{i=1}^t X_i$ и оба неизвестных содержатся по крайней мере в одном уравнении системы.

Имеем:

$$\mathbf{P}(I_j = 1) = \left[\mathbf{P}\left(I_{j,i}^{(1)} = 1\right) + \mathbf{P}\left(I_{j,i}^{(2)} = 1\right)\right]^t - \mathbf{P}^t\left(I_{j,i}^{(1)} = 1\right),$$

где $\mathbf{P}(I_{j,i}^{(1)} = 1) = 1 - \gamma 2/n + O(n^{-2})$, $\mathbf{P}(I_{j,i}^{(2)} = 1) = O(n^{-2})$. Следовательно, $\mathbf{P}(I_j = 1) = O(n^{-3}\ln n)$.

Для величины $I = \sum_j I_j$ получим, что математическое ожидание $\mathbf{E}I = \sum_j \mathbf{E}I_j = C_n^2 \mathbf{P}(I_j = 1) = O(n^{-1}\ln n)$. Отсюда вытекает оценка $\mathbf{P}(I > 0) = O(n^{-1}\ln n)$.

Обозначим R_m^0 событие, состоящее в том, что $\eta_t = m$, $I = 0$. Имеем:

$$\mathbf{P}(\xi_t \geqslant 2^m \mid R_m^0) = 1,$$
$$\mathbf{E}\xi_t \geqslant \sum_m \mathbf{P}(R_m^0)\left[2^m + \left(1 - \mathbf{P}(\xi_t = 2^m \mid R_m^0)\right)\right]. \tag{13}$$

Из асимптотической эквивалентности $\mathbf{P}(R_m^0) \approx \mathbf{P}(\eta_t = m)$ и оценок (7), (12), (13) вытекает, что

$$\mathbf{P}(\xi_t = 2^m \mid R_m^0) \longrightarrow 1. \tag{14}$$

Учитывая (14) и соотношение $\mathbf{P}(\xi_t = 2^m \mid \overline{R}_m^0)\,\mathbf{P}(\overline{R}_m^0) \longrightarrow 0$, где $\overline{R}_m^0$ — событие, дополнительное для R_m^0, получим:

$$\mathbf{P}(\xi_t = 2^m) - \mathbf{P}(\eta_t = m) \longrightarrow 0. \tag{15}$$

Таким образом, оценка (5) в случае $\Delta = 0$ доказана.

Доказательство в случае $\Delta = 1$ проводится аналогично. Если $\varphi(u^i) = \varphi(u^j)$ для любой пары векторов u^i, u^j, такой, что $u^i \oplus u^j = (1, \ldots, 1)$, то вектор x является решением системы, если и только если решением является вектор $\overline{x} = x \oplus (1, \ldots, 1)$. Поэтому

$$P(p, q) = P(n_0 - p, n_1 - q), \qquad \mathbf{E}\xi_t = 2\exp\left\{e^{-z} + o(1)\right\},$$
$$\mathbf{P}(\xi_t \geqslant 2^{m+1} \mid R_m^0) = 1,$$

и, повторив выкладки (13)–(15) с заменой 2^m на 2^{m+1}, получим:

$$\mathbf{P}(\xi_t = 2^{m+1}) - \mathbf{P}(\eta_t = m) \longrightarrow 0. \tag{16}$$

З а м е ч а н и е 1. Параметр γ, определенный формулой (4) можно интерпретировать следующим образом: Имеем:

$$\gamma = d - d\sum_{k=1}^{d-1} C_{d-1}^k \theta^k (1-\theta)^{d-1-k} \lambda_G(k) \left(\frac{d!}{|G|}\right)^{-1}.$$

Рассмотрим множество неизвестных, выбранных из $\{x_i, \dots, x_n\}$ для уравнения с номером i:

$$\{x_{i_1}, \dots, x_{i_d}\}, \qquad i_1 \leqslant \dots \leqslant i_d. \tag{17}$$

Выделим в этом множестве произвольное неизвестное. Обозначим A событие, состоящее в том, что среди остальных $d-1$ неизвестных k неизвестных в истинном решении принимают нулевые значения и $d-1-k$ неизвестных принимают единичные значения. При $n \to \infty$ имеем: $\mathbf{P}(A) = C_{d-1}^{k}\theta^k(1-\theta)^{d-1-k} + o(1)$. Пусть осуществилось событие A. Вероятность того, что неизвестные (17) размещены в функции φ так, что изменение истинного значения выделенного неизвестного на ложное при истинных значениях остальных неизвестных не приводит к изменению значения φ, равна $\lambda_G(k)\,(d!/|G|)^{-1}$. Следовательно, с точностью до величины $o(1)$ при $n \to \infty$ параметр γ равен среднему числу неизвестных одного уравнения, существенных относительно истинного решения.

Параметр $\gamma = 0$, если $\varphi = \mathrm{const}$, так как в этом случае $\lambda_G(k) = d!/|G|$.

Если $\varphi \neq \mathrm{const}$, то $\gamma > 0$. Действительно, в этом случае $\varphi(u^i) \neq \varphi(u^j)$ для некоторой пары векторов u^i, u^j, различающихся по одной координате. Пусть вектора u^i, u^j имеют k общих нулей и $d-1-k$ общих единиц. Тогда

$$1 - P(p,q) \geqslant \left[(p+q)\,C_{n_0-q}^{k}C_{n_1-p}^{d-1-k}\right]\left[C_n^d\frac{d!}{|G|}\right]^{-1} \geqslant \frac{p+q}{n}\,\delta_1 + O\left(\left(\frac{p+q}{n}\right)^2\right),$$

где $\delta_1 > 0$. При $\gamma = 0$ данная оценка противоречит оценке (9′).

З а м е ч а н и е 2. Соотношения (15), (16) означают, что число решений ξ_t сближается по вероятности со случайной величиной $2^{\eta_t+\Delta}$, $\Delta \in \{0,1\}$, где величина η_t равна числу неизвестных, несущественных относительно истинного решения в каждом уравнении системы.

Обозначим $\eta_t^{(0)}$ число неизвестных, отсутствующих в системе, и $\eta_t^{(1)}$ — число неизвестных, каждое из которых входит по крайней мере в одно уравнение системы и является несущественным относительно истинного решения в любом уравнении. Очевидно, $\eta_t = \eta_t^{(0)} + \eta_t^{(1)}$.

Возможны два случая.

1. Функция φ такова, что $\gamma = d$. В [2] показано (см. [2, лемма 1]), что, если $t = d^{-1}n(\ln n + z)$, $n \to \infty$, то

$$\mathbf{P}\left(\eta_t^{(0)} = m\right) = \frac{e^{-mz}}{m!}\exp\left\{-e^{-z} + o(1)\right\}. \tag{18}$$

С учетом оценки (18),

$$\mathbf{P}\left(\xi_t \neq 2^{\eta_t^{(0)}+\Delta}\right) \leqslant \mathbf{E}\left(\xi_t - 2^{\eta_t^{(0)}+\Delta}\right) = o(1).$$

Таким образом, в условиях теоремы $\xi_t \xrightarrow{\mathbf{P}} 2^{\eta_t^{(0)}+\Delta}$, $\eta_t^{(1)} \xrightarrow{\mathbf{P}} 0$.

2. Функция φ такова что $\gamma < d$. В этом случае из оценки (18) вытекает, что в условиях теоремы $\eta_t^{(0)} \xrightarrow{\mathbf{P}} 0$, и, следовательно, $\xi_t \xrightarrow{\mathbf{P}} 2^{\eta_t^{(1)}+\Delta}$.

3. Примеры. Пусть $d = rs$,

$$\varphi(u_1, \dots, u_{rs}) = \psi(u_1, \dots, u_s) + \dots + \psi\left(u_{s(r-1)+1}, \dots, u_{rs}\right), \tag{19}$$

где $\psi\left(u_{1+is}, \dots, u_{(i+1)s}\right)$, $0 \leqslant i \leqslant r-1$, — булева функция, существенно зависящая от всех аргументов, с группой инерции G_ψ в симметрической группе подстановок σ_s;

знак + может означать как сложение в поле вещественных чисел, так и сложение в поле GF(2).

Положим $G = G_\varphi$, где G_φ — группа инерции функции φ в σ_{rs}. Группа G_φ порождается всеми перестановками слагаемых в функции (19) и перестановками неизвестных внутри слагаемых по подстановкам из G_φ, $|G_\varphi| = |G_\psi|^r r!$.

Для величины (3) в рассматриваемом случае выполняется равенство:

$$\lambda_G(k) = \lambda_{G_\varphi}(k) = \sum_{j=0}^{\min(k,s-1)} C_k^j C_{rs-k-1}^{s-j-1} \lambda_{G_\psi}(j) \frac{(s(r-1))!}{|G_\psi|^{r-1}(r-1)!}.$$

Подставляя $\lambda_G(k)$ в формулу (4), получим:

$$\gamma = \gamma_\varphi = rs - r|G_\psi| \sum_{j=0}^{s-1} \frac{\theta^j (1-\theta)^{s-j-1}}{j!(s-j-1)!} \lambda_{G_\psi}(j) = r\gamma_\psi.$$

Нетрудно убедиться, что для функции φ, задаваемой равенством (19), справедливо утверждение: в формуле (5) $\Delta = 0$, $\Delta = 1$ тогда и только тогда, когда $\Delta = 0$, $\Delta = 1$ для функции ψ.

1. Пусть $\psi = u_{1+si} \oplus \cdots \oplus u_{s+si}$ — линейная булева функция. Тогда $\lambda_{G_\psi}(j) = 0$, $j = 0, \ldots, s-1$, и, следовательно, $\gamma_\psi = s$, $\gamma_\varphi = rs$. Очевидно, что $\Delta = 0$, если s нечетное число, и $\Delta = 1$, если s четное число.

2. Пусть $s = 2$, $\psi(u_{1+2i}, u_{2+2i})$, $0 \leqslant i \leqslant r-1$, — нелинейная булева функция от двух переменных. Рассмотрим два случая.

Для функции

$$\psi(u_{1+2i}, u_{2+2i}) = u_{1+2i} \vee u_{2+2i} \tag{20}$$

имеем: $|G_\psi| = 2$, $\lambda_{G_\psi}(0) = 1$, $\lambda_{G_\psi}(1) = 0$. Следовательно, $\gamma_\psi = 2 - 2(1-\theta) = 2\theta$, $\gamma_\varphi = 2r\theta$.

Для функции

$$\psi(u_{1+2i}, u_{2+2i}) = \overline{u}_{1+2i} \vee u_{2+2i} \tag{21}$$

имеем: $|G_\psi| = 1$, $\lambda_{G_\psi}(0) = \lambda_{G_\psi}(1) = 1$. Поэтому $\gamma_\psi = 2 - (\theta + 1 - \theta) = 1$, $\gamma_\varphi = r$.

Любую нелинейную булеву функцию от двух переменных, отличную от функций (20), (21), можно получить либо из функции (20), либо из функции (21) путем применения двух операций: инвертирования функции, инвертирования всех переменных. Инвертирование функции: $\psi(u_1, u_2) \longrightarrow \overline{\psi}(u_1, u_2)$, не изменяет параметр γ_ψ; инвертирование переменных: $\psi(u_1, u_2) \longrightarrow \psi(\overline{u}_1, \overline{u}_2)$, приводит к замене в выражении для γ_ψ величины θ на величину $1-\theta$. Очевидно, что $\Delta = 0$ для любой нелинейной булевой функции $\psi(u_1, u_2)$.

СПИСОК ЛИТЕРАТУРЫ

1. *Балакин Г. В.* Заведомо совместные системы случайных уравнений над конечным полем. — Тезисы докладов Всесоюзной конференции «Вероятностные методы в дискретной математике». Петрозаводск: Карельский филиал АН СССР, 1983, с. 8–10.
2. *Балакин Г. В.* О распределении числа решений систем случайных булевых уравнений. — Теория вероятн. и ее примен., 1973, т. 18, в. 3, с. 627–632.
3. *Сачков В. Н.* Комбинаторные методы дискретной математики. М.: Наука, 1977.

Поступила в редакцию
15.VII.1992