Math-Net.Ru
Общероссийский математический портал

Г. В. Балакин, Системы случайных булевых уравнений со случайным выбором неизвестных в каждом уравнении, *Тр. по дискр. матем.*, 2000, том 3, 21–28

https://www.mathnet.ru/tdm34

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
https://www.mathnet.ru/rus/agreement

Параметры загрузки:
IP: 18.97.9.169
21 января 2026 г., 19:56:38

Труды по дискретной математике
Том 3, с. 21–28
М.: ФИЗМАТЛИТ, 2000

СИСТЕМЫ СЛУЧАЙНЫХ БУЛЕВЫХ УРАВНЕНИЙ СО СЛУЧАЙНЫМ ВЫБОРОМ НЕИЗВЕСТНЫХ В КАЖДОМ УРАВНЕНИИ

Г. В. БАЛАКИН

Рассматриваются системы случайных булевых уравнений вида $\varphi_i(x_{r_{i1}},\ldots,x_{r_{is}}) = a_i$, $i = 1,\ldots,t$, относительно неизвестных $x_1,\ldots,x_n$, где функции $\varphi_i(y_1,\ldots,y_s)$ выбираются случайно и равновероятно из множества всех булевых функций от s переменных, а наборы индексов $(r_{i1},\ldots,r_{is})$ для разных уравнений независимы и получаются по схеме равновероятного выбора с возвращением из множества $\{1,\ldots,n\}$. Для случая, когда правые части $a_1,\ldots,a_t$ систем независимы и равновероятны, найдены асимптотические формулы для математического ожидания числа решений и оценки для вероятности совместности системы уравнений. Для случая, когда $a_i = \varphi_i\left(x^0_{i_{i1}},\ldots,x^0_{i_{is}}\right)$, $i = 1,\ldots,t$, для некоторого фиксированного вектора $\bar{x}^0 = \left(x^0_1,\ldots,x^0_n\right)$, найдены асимптотики математического ожидания и предельные распределения числа решений.

§1. ПОСТАНОВКА ЗАДАЧИ

Рассмотрим систему булевых уравнений

$$\varphi_i\left(x_{r_{i1}},\ldots,x_{r_{is}}\right) = a_i, \qquad i = \overline{1,t}. \tag{1.1}$$

Предположим, что функция $\varphi_i(y_1,\ldots,y_s)$ случайно и равновероятно выбирается из множества всех булевых функций от s переменных, т.е.

$$\mathbf{P}\left(\varphi_i(\bar{y}) = 1\right) = \mathbf{P}\left(\varphi_i(\bar{y}) = 0\right) = \frac{1}{2}$$

для любого вектора $\bar{y} = (y_1,\ldots,y_s)$, и что значения $\varphi(\bar{y})$, $\bar{y} \in \{0,1\}^n$, независимы в совокупности. Набор индексов $\bar{r}_i = (r_{i1},\ldots,r_{is})$ получается по схеме равновероятного выбора без возвращения из множества $\{1,\ldots,n\}$. Выбор функций и индексов неизвестных для всех уравнений независимы в совокупности.

Систему уравнений (1.1) будем называть случайной, если

© Г. В. Балакин, 2000

$$\mathbf{P}(a_i = 1) = \mathbf{P}(a_i = 0) = \frac{1}{2}, \qquad i = \overline{1,t},$$

и правые части $a_1, \ldots, a_t$ как случайные величины независимы в совокупности и не зависят от левых частей системы (1.1). Систему (1.1) будем называть заведомо совместной, если

$$a_i \equiv \varphi\left(x^0_{r_{i1}}, \ldots, x^0_{r_{is}}\right), \qquad i = \overline{1,t},$$

для некоторого заранее фиксированного вектора $\bar{x}^0 = \left(x^0_1, \ldots, x^0_n\right)$. Пусть ξ_t обозначает число решений случайной системы уравнений, а η_t — число решений заведомо совместной случайной системы уравнений.

В § 2 работы оценивается число уравнений системы, при котором число решений невелико. Для этого находятся математические ожидания числа решений как для случайной системы уравнений, так и для заведомо совместной случайной системы уравнений, приводятся оценки для вероятностей $\mathbf{P}(\xi_t = 0)$, $\mathbf{P}(\eta_t = 1)$ и изучается структура множества решений.

В § 3 находится распределение числа решений заведомо совместной системы уравнений и описываются свойства множества ее решений.

§ 2. СРЕДНЕЕ ЧИСЛО РЕШЕНИЙ СИСТЕМЫ УРАВНЕНИЙ

Вероятность того, что фиксированный вектор $\bar{x} = (x_1, \ldots, x_n)$ является решением случайной системы уравнений, равна 2^{-t}, поэтому

$$\mathrm{M}\xi_t = 2^n \left(\frac{1}{2}\right)^t = 2^{n-t}.$$

Значит, при $n,\ t - n \to \infty$ верны оценки

$$\mathrm{M}\xi_t = o(1), \qquad \mathbf{P}(\xi_t \geq 1) \leq \mathrm{M}\xi_t = 2^{n-t} = o(1),$$

и для выполнения соотношения $\mathrm{M}\xi_t = O(1)$ при $n \to \infty$ необходимым и достаточным условием является неравенство $t \geq n + c$, $c = \mathrm{const}$.

Заметим, что если случайная система уравнений (1.1) имеет решения, то их число не меньше 2^{ν_t}, где

$$\nu_t = \left| \{1, \ldots, n\} \setminus \bigcup_{i=1}^{t} \{r_{i1}, \ldots, r_{is}\} \right|$$

— число отсутствующих неизвестных в системе (1.1). Найдем условия на t', при которых $\mathrm{M}\nu_t = O(1)$ при $n \to \infty$, $t \geq t'$. Легко видеть, что

$$\mathrm{M}\nu_t = n \left[\frac{C^s_{n-1}}{C^s_n}\right]^t \sim n \exp\left\{-\frac{st}{n}\right\}$$

при $s = o\left(n/\sqrt{t}\right)$ и, следовательно, при $t' = n(\ln n + z)/s$, $z = O(1)$ получаем оценку $\mathrm{M}\nu_{t'} = \exp\{-z\} = O(1)$.

Дополнительно отметим, что в уравнения системы некоторые неизвестные могут входить несущественным образом. Напомним, что x_i $(i = \overline{1,s})$ несущественно входит в функцию $\varphi(x_1, \ldots, x_s)$, если равенство

$$\varphi\left(x_1,\ldots,\underset{i}{0},\ldots,x_s\right)=\varphi\left(x_1,\ldots,\underset{i}{1},\ldots,x_s\right) \tag{2.1}$$

выполняется для всех 2^{s-1} наборов значений остальных $(s-1)$ неизвестных. Вероятность события (2.1) для равновероятного случая равна $(1/2)^{2^{s-1}}$. Если некоторое неизвестное входит в m уравнений, то вероятность того, что это вхождение несущественно для всех m функций из левых частей этих уравнений, равна $(1/2)^{m2^{s-1}}$.

Для заведомо совместных систем уравнений считают, что неизвестное x_i входит в уравнение $\varphi(x_1,\ldots,x_s)=a$ несущественным образом относительно истинного решения, если условие (2.1) выполнено при

$$x_1=x_1^0,\ \ \ldots,\ \ x_{i-1}=x_{i-1}^0,\quad x_{i+1}=x_{i+1}^0,\ \ \ldots,\ \ x_s=x_s^0.$$

Вероятность события

$$\varphi\left(x_1^0,\ldots,0,\ldots,x_s^0\right)=\varphi\left(x_1^0,\ldots,1,\ldots,x_s^0\right)$$

при равновероятном выборе функции φ равна $1/2$. Поэтому, если неизвестное x_i встречается в s_i уравнениях, $s_1+\ldots+s_n=st$, то вероятность того, что x_i несущественно относительно $\bar{x}^0$ входит в систему уравнений, равна $(1/2)^{s_i}$.

Лемма 2.1. *Если при $n,t\to\infty$ величина $\mathbf{M}\eta_t\to 1$, то $\mathbf{P}\{s_i\geq K\}\to 1$ для любых $K<\infty$ и $i=\overline{1,n}$.*

Доказательство. Действительно, пусть неизвестное x_i встречается в $s_i<K$ уравнениях. Тогда с вероятностью, не меньшей $(1/2)^K$, системе уравнений помимо вектора $\bar{x}^0$ будет удовлетворять вектор $\bar{x}^i$, который отличается от вектора $\bar{x}^0$ только i-й координатой. Следовательно, с вероятностью не менее $(1/2)^K$ система будет иметь не менее двух решений, и $\mathbf{M}\eta_t\geq 1+(1/2)^K$, т.е. $\mathbf{M}\eta_t\to 1$ только если $\mathbf{P}\{s_i\geq K\}\to 1$ при любом $K<\infty$ и любом $i\in\{1,\ldots,n\}$.

Найдем среднее число решений заведомо совместной системы. Пусть вектор $\bar{x}$ отличается k координатами от истинного решения $\bar{x}^0$. Тогда

$$p_k=\mathbf{P}\left(\varphi_i(\bar{x})=\varphi_i(\bar{x}^0)\right)=\frac{C_{n-k}^s}{C_n^s}+\frac{1}{2}\left(1-\frac{C_{n-k}^s}{C_n^s}\right).$$

Для числа $\eta_t(k)$ решений, отличающихся k координатами от $\bar{x}^0$, находим

$$\mathbf{M}\eta_t(k)=C_n^k(p_k)^t=C_n^k\left(\frac{1}{2}\right)^t\left(1+\frac{C_{n-k}^s}{C_n^s}\right)^t.$$

Так как $\eta_t=\eta_t(0)+\eta_t(1)+\ldots+\eta_t(n)$, то

$$\mathbf{M}\eta_t=\left(\frac{1}{2}\right)^t\sum_{k=0}^{n}C_n^k\left(1+\frac{C_{n-k}^s}{C_n^s}\right)^t. \tag{2.2}$$

Лемма 2.2. *Пусть*

$$t = \frac{2n(\ln n + z)}{s}, \qquad z = O(1), \qquad \varlimsup_{n\to\infty} \frac{s}{\ln n} < 1.$$

Тогда при $n \to \infty$ равномерно по $k \le \ln n$

$$\mathrm{M}\eta_t(k) = (1 + o(1))\,\frac{(e^{-z})^k}{k!}.$$

Доказательство. Легко видеть, что в условиях леммы

$$\frac{C_{n-k}^s}{C_n^s} = \prod_{i=0}^{s-1}\left(\frac{1-(k+i)/n}{1-i/n}\right), \qquad \ln\prod_{i=0}^{s-1}\left(\frac{1-(k+i)/n}{1-i/n}\right) = -k\,\frac{s}{n} + O\left(\frac{\ln^3 n}{n^2}\right),$$

$$\mathrm{M}\eta_t(k) = C_n^k\left[\frac{1}{2}\left(1 + \frac{C_{n-k}^s}{C_n^s}\right)\right]^t =$$

$$= \frac{n^k}{k!}\exp\left\{t\ln\left[1 - \frac{1}{2}\,k\,\frac{s}{n} + O\left(\frac{\ln^3 n}{n^2}\right)\right]\right\} = \frac{(e^{-z})^k}{k!}\,(1 + o(1)),$$

что и требовалось доказать.

Теорема 2.1. *Если при $n \to \infty$ число уравнений*

$$t = \frac{2n(\ln n + z)}{s}, \qquad z = O(1), \qquad \varlimsup_{n\to\infty} \frac{s}{\ln n} = \theta < 1,$$

то

$$\mathrm{M}\eta_t = \exp\left\{e^{-z} + o(1)\right\}.$$

Доказательство. Выражение (2.2) для $\mathrm{M}\eta_t$ разделим на три части:

$$\mathrm{M}\eta_t = \sum_{0\le k\le \ln n} \mathrm{M}\eta_t(k) + \sum_{\ln n < k < \varepsilon n} \mathrm{M}\eta_t(k) + \sum_{\varepsilon n < k \le n} \mathrm{M}\eta_t(k), \qquad \varepsilon = \frac{\ln\ln n}{\ln n}.$$

Первая сумма фактически уже оценена при доказательстве леммы 2.2:

$$I_1 = \sum_{0\le k\le \ln n} \frac{(e^{-z})^k}{k!}\left[1 + O\left(\frac{\ln^3 n}{n}\right)\right] \sim \exp\left\{e^{-z}\right\}.$$

Оценим сверху вторую сумму. По формуле Стирлинга

$$C_n^k = \frac{1 + o(1)}{\sqrt{2\pi n\beta_k(1-\beta_k)}}\exp\left\{-n[\beta_k\ln\beta_k + (1-\beta_k)\ln(1-\beta_k)]\right\}, \qquad \beta_k = \frac{k}{n},$$

причем первый множитель меньше единицы. Далее, используя оценку $C_{n-k}^s/C_n^s \le (1-\beta_k)^s$, приходим к неравенству

$$I_2 \le \sum_{\ln n < k < \varepsilon n} \exp\left\{-n\left[\beta_k\ln\beta_k + (1-\beta_k)\ln(1-\beta_k) - \frac{t}{n}\ln\frac{1+(1-\beta_k)^s}{2}\right]\right\}.$$

Изучим поведение функции

$$\varphi(\beta) = \beta \ln \beta + (1-\beta)\ln(1-\beta) - \frac{t}{n}\ln\frac{1+(1-\beta)^s}{2}.$$

Первая производная

$$\varphi'(\beta) = \ln\frac{\beta}{1-\beta} + \frac{st}{n}\frac{(1-\beta)^{s-1}}{1+(1-\beta)^s} > 0,$$

так как $st/n = 2(\ln n + z)$ и в области изменения β, s для достаточно больших n выполняется неравенство

$$(1-\beta)^s \geq \left(1 - \frac{\ln\ln n}{\ln n}\right)^{\theta' \ln n} \sim \left(\frac{1}{\ln n}\right)^{\theta'}, \qquad \theta < \theta' < 1.$$

Следовательно, полагая $k_0 = [\ln n + 1]$, находим

$$I_2 < \varepsilon n \cdot \exp\left\{-n\varphi\left(\frac{k_0}{n}\right)\right\} = o(1).$$

Для третьей суммы верна оценка

$$I_3 = \sum_{\varepsilon n < k \leq n} C_n^k \left[\frac{1}{2}\left(1 + \frac{C_{n-k}^s}{C_n^s}\right)\right]^t < 2^n \left[\frac{1}{2}\left(1 + (1-\varepsilon)^s\right)\right]^t =$$

$$= \exp\left\{-n\left[\frac{2(\ln n + z)}{s}\ln\frac{2}{1+(1-\varepsilon)^s} - \ln 2\right]\right\}.$$

Нетрудно убедиться, что при $\varepsilon = \ln\ln n/\ln n$ и любом $s < \ln n$ для достаточно больших n выполняется неравенство

$$\frac{2\ln n}{s}\ln\frac{2}{1+(1-\varepsilon)^s} > \ln 2.$$

Это означает, что $I_3 \to 0$. Теорема доказана.

§ 3. РАСПРЕДЕЛЕНИЕ ЧИСЛА РЕШЕНИЙ ЗАВЕДОМО СОВМЕСТНОЙ СИСТЕМЫ УРАВНЕНИЙ

Согласно утверждениям, доказанным в предыдущем параграфе, при $s \leq \theta \ln n$, $0 < \theta < 1$, среднее число решений заведомо совместной системы уравнений сравнительно невелико, если $t \sim 2n\ln n/s$. В этом параграфе мы найдем распределение числа решений и опишем структуру множества решений заведомо совместной системы уравнений.

Напомним, что неизвестное x_i несущественно относительно решения $\bar{x}^0$ системы уравнений (1.1), если указанной системе уравнений удовлетворяет вектор $\bar{x}^0 \oplus e_i$, отличающийся от вектора $\bar{x}^0$ только i-й координатой.

Заметим, что отсутствующие в системе уравнений неизвестные являются несущественными для любого вектора из множества решений. Определение несущественности неизвестного несколько в ином виде присутствует в работе [1], неявно оно используется и в других работах по системам нелинейных уравнений (см., например, [2]).

Пусть ν_j есть индикатор события

$$\left\{\varphi_i\left(\bar{x}^0 \oplus e_j\right) = \varphi_i\left(\bar{x}^0\right),\ i = \overline{1,t}\right\},$$

а случайная величина

$$\nu = \nu_1 + \nu_2 + \ldots + \nu_n$$

есть число неизвестных, несущественных для системы уравнений (1.1) относительно решения $\bar{x}^0$.

Лемма 3.1. *Если выполнены условия леммы* 2.2, *то*

$$\mathrm{M}\nu = n\left[1 - \frac{s}{2n}\right]^t = e^{-z} + o(1).$$

Доказательство. При независимом и равновероятном выборе функций $\varphi_1, \ldots, \varphi_t$ в системе уравнений (1.1)

$$\mathbf{P}(\nu_j = 1) = \mathbf{P}\left\{\varphi_i\left(\bar{x}^0 \oplus e_j\right) = \varphi_i\left(\bar{x}^0\right),\ i = \overline{1,t}\right\} = \left[\frac{C_{n-1}^s + C_{n-1}^{s-1}/2}{C_n^s}\right]^t =$$

$$= \left(1 - \frac{s}{2n}\right)^t = \exp\left\{-t\left[\frac{s}{2n} + O\left(\frac{s^2}{n^2}\right)\right]\right\} = \frac{e^{-z} + o(1)}{n}.$$

Следовательно,

$$\mathrm{M}\nu = n\mathrm{M}\nu_i = e^{-z} + o(1).$$

Теорема 3.1. *Пусть*

$$t = \frac{2n(\ln n + z)}{s}, \qquad \lim_{n\to\infty} z = c, \qquad \overline{\lim_{n\to\infty}} \frac{s}{\ln n} < 1.$$

Тогда при $n \to \infty$ *для любого фиксированного* $k = 0, 1, 2, \ldots$

$$\mathbf{P}(\nu = k) = \frac{\left(e^{-c}\right)^k}{k!} \exp\left\{-e^{-c}\right\} + o(1).$$

Доказательство. Для любого набора $1 \le i_1 < i_2 < \ldots < i_m \le n$

$$\mathbf{P}\{\nu_{i_1} = 1, \ldots, \nu_{i_m} = 1\} = \left[\frac{1}{C_n^s}\sum_{i=0}^{s}\frac{C_m^i C_{n-m}^{s-i}}{2^i}\right]^t =$$

$$= \exp\left\{t\ln\left[\left(1 - \frac{ms}{n}\right) + \frac{ms}{2n}\left(1 + O\left(\frac{ms}{n}\right)\right)\right]\right\} =$$

$$= \frac{\left(e^{-z}\right)^m}{n^m}\left[1 + O\left(\frac{m^2\ln^2 n}{n}\right)\right].$$

Отсюда находим

$$\lim_{n\to\infty} \sum_{1\le i_1<\ldots<i_m\le n} \mathbf{P}\left\{\nu_{i_1} = 1, \ldots, \nu_{i_m} = 1\right\} = \frac{\left(e^{-c}\right)^m}{m!}.$$

Но выражение под знаком предела есть не что иное, как m-й биномиальный момент случайной величины ν, поэтому согласно известной теореме Пуассона (см., например, [3], стр. 260) при любом фиксированном $k = 0, 1, \ldots$

$$\mathbf{P}(\nu = k) = \frac{\left(e^{-c}\right)^k}{k!} \exp\left\{-e^{-c}\right\} + o(1).$$

Теорема доказана.

Теорема 3.2. *В условиях теоремы* 3.1 *число решений* η_t *заведомо совместной системы уравнений* (1.1) *стремится по вероятности при* $n \to \infty$ *к случайной величине* 2^ν, *где* ν — *число несущественных неизвестных относительно решения* $\bar{x}^0$, *и, следовательно, при любом фиксированном* $m = 0, 1, 2, \ldots$

$$\mathbf{P}\left(\eta_t = 2^m\right) = \frac{\left(e^{-z}\right)^m}{m!} \exp\left\{-e^{-z}\right\} + o(1).$$

Доказательство. Предположим, что выполняется событие $A_0(m)$, которое заключается в том, что $\nu = m$ и в любом из t уравнений исходной системы присутствует не более одного из этих m несущественных неизвестных. Очевидно, что

$$\mathbf{P}\left\{\eta_t \geq 2^m | A_0(m)\right\} = 1,$$

а для любого фиксированного m

$$\mathbf{P}\left\{A_0(m)\right\} = \mathbf{P}\left\{\nu = m\right\}(1 - \beta), \qquad 0 \leq \beta = O\left(\frac{s^2 t}{n^2}\right) = o(1),$$

$$\mathbf{P}\left\{A_0(m)\right\} \sim \mathbf{P}\left\{\nu = m\right\} = \frac{\left(e^{-z}\right)^m}{m!} \exp\left\{-e^{-z}\right\} + o(1).$$

С другой стороны, используя теоремы 2.1 и 3.1, находим

$$\mathbf{M}\eta_t = \sum_{i \geq 1} i\mathbf{P}\left(\eta_t = i\right) = \exp\left\{e^{-z} + o(1)\right\} =$$

$$= \mathbf{M}2^\nu + o(1) = \sum_{m \geq 0} 2^m \mathbf{P}\left(\nu = m\right) + o(1).$$

Так как

$$\lim_{n \to \infty} \sum_{m \geq 0} \mathbf{P}\left\{A_0(m)\right\} = 1,$$

то отсюда следует

$$\lim_{n \to \infty} \sum_{i \neq 2^m,\ m \geq 0} \mathbf{P}\left(\eta_t = i\right) = o(1),$$

или

$$\mathbf{P}\left\{\eta_t \neq 2^\nu\right\} = o(1).$$

Теорема доказана.

СПИСОК ЛИТЕРАТУРЫ

1. *Копытцев В. А.* О распределении числа решений случайных заведомо совместных систем уравнений. — Теория вероятн. и ее примен., 1995, т. 40, в. 2, с. 430–437.

2. *Балакин Г. В.* Графы систем двучленных уравнений с булевыми неизвестными. — Теория вероятн. и ее примен., 1995, т. 40, в. 2, с. 241–259.

3. *Сачков В. Н.* Введение в комбинаторные методы дискретной математики. — М.: Наука, 1982.