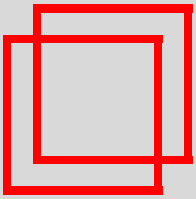
Math-Net.Ru
All Russian mathematical portal

V. A. Kopyttsev, Reliability estimate of the maximum likelihood method used for the solution of systems of equations with distorted right parts, *Mat. Vopr. Kriptogr.*, 2023, Volume 14, Issue 3, 107–117

DOI: 10.4213/mvk449

Use of the all-Russian mathematical portal Math-Net.Ru implies that you have read and agreed to these terms of use
http://www.mathnet.ru/eng/agreement

Download details:
IP: 18.97.9.168
March 25, 2025, 16:02:17

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2023 Т. 14 № 3 С. 107–117

УДК 519.233.2+519.719.2 DOI https://doi.org/10.4213/mvk449

Оценка надежности метода максимального правдоподобия при его использовании для решения систем уравнений с искажениями в правых частях

В. А. Копытцев

Академия криптографии Российской Федерации, *Москва*

Получено 24.IV.2023

Аннотация. Исследуется надежность метода максимального правдоподобия для решения систем булевых уравнений со случайным выбором неизвестных в каждом уравнении и с искажениями в правых частях. Определяются условия, при которых надежность метода близка к единице.

Ключевые слова: системы уравнений с искажениями в правых частях, метод максимального правдоподобия решения систем

Reliability estimate of the maximum likelihood method used for the solution of systems of equations with distorted right parts

V. A. Kopyttsev

Academy of Cryptography of the Russian Federation, *Moscow*

Abstract. Reliability of method of maximum likelihood for the solution of systems of the Boolean equations with the random choice of unknown in each equation and with distortions in the right parts is investigated. Conditions under which reliability of method is close to unit are defined.

Keywords: the systems of the equations with distortions in the right parts, method of maximum likelihood of the solution of systems

Citation: Matematicheskie Voprosy Kriptografii, 2023, v. 14, № 3, pp. 107–117 (Russian)
© Академия криптографии Российской Федерации, 2023 г.

1. Постановка задачи

Будем рассматривать систему уравнений с искаженными правыми частями следующего вида:

$$\{g(x_{s_{i,1}},\dots,x_{s_{i,r}})=a_i,\quad i=\overline{1,t},\tag{1}$$

где g – фиксированная булева функция от r переменных, а $(x_{s_{i,1}},\dots,x_{s_{i,r}})$, $i=\overline{1,t}$, – выборки без возвращения по r элементов из множества $\{x_1,\dots,x_n\}$ двоичных величин, независимые в совокупности и равномерно распределенные на множестве из всех $(n)_r=n(n-1)\dots(n-r+1)$ таких выборок. Правые части

$$a_i=g(x^o_{s_{i,1}},\dots,x^o_{s_{i,r}})\oplus\eta_i,$$

где $(x^o_{s_{i,1}},\dots,x^o_{s_{i,r}})$, $i=\overline{1,t}$, – выборки из элементов неизвестного вектора $x^o=(x^o_1,\dots,x^o_n)$, который требуется найти, а η=$(\eta_1,\dots,\eta_t)$ – вектор ошибок, компоненты которого независимы и одинаково распределены,

$$\mathbf{P}\{\eta_i=1\}=\delta<0,5,\ i=\overline{1,t},\tag{2}$$

и не зависят от левых частей уравнений.

Системы уравнений вида (1) для различных классов функций g исследовались в ряде работ (см. [1–7]). В частности в работе [6] приведены оценки надежности применения метода максимального правдоподобия для решения системы, порожденной дважды биюнктивной функцией g произвольного вида. В данной работе оценка надежности метода максимального правдоподобия приведена в случае, когда g – любая функция, отличная от константы.

2. Формулировка и доказательство основного результата

Пусть V_n – множество булевых векторов размерности n. Метод решения систем уравнений, называемый методом максимального правдоподобия, состоит в переборе векторов $z=(z_1,\dots,z_n)\in V_n$, подсчете для каждого вектора статистики невязки вида

$$S(z)=\sum_{i=1}^{t}(g(z_{s_{i,1}},\dots,z_{s_{i,r}})\oplus a_i)$$

и выборе того значения z, для которого данная статистика имеет наименьшее значение. Оценим надежность этого метода для систем вида (1), т. е. оценим вероятность

$$\mathcal{P}_{t,n} = \mathbf{P}\left\{ S(x^o) \leqslant \min_{z \neq x^o} S(z) \right\}.$$

Обозначим I_0 (I_1) множество индексов нулевых (соответственно, единичных) координат истинного решения x^o. Положим

$$|I_0| = n_0 = \theta n, \;\; |I_1| = n_1 = (1-\theta)n, \;\; 0 < \theta < 1. \tag{3}$$

Обозначим $B_r^{(1)}(k)$ множество пар r-мерных булевых векторов, отличающихся друг от друга различными значениями только одной координаты, содержащих среди совпадающих координат k единиц ($0 \leqslant k \leqslant r-1$), и таких, что для каждой пары $(u^1, u^2) \in B_r^{(1)}(k)$ выполняется неравенство $g(u^1) \neq g(u^2)$. Введем числа:

$$\gamma(k) = |B_r^{(1)}(k)|, \tag{4}$$

$$\gamma = \Delta \sum_{k=0}^{r-1} (1-\theta)^k \theta^{r-1-k} \gamma(k), \tag{5}$$

где $\Delta = 1 - \sqrt{4\delta(1-\delta)}$. Пусть $g(u) \neq \mathrm{Const}$, тогда $\sum_{k=0}^{r-1} \gamma(k) \neq 0$ и $\gamma \neq 0$.

Теорема 1. *Пусть* 1) $g(u') \neq g(u' \oplus (1, \ldots, 1))$ *для некоторого вектора* $u' \in V_r$, 2) $t = \gamma^{-1} n(\ln n + \omega)$, $\omega = O(1)$ *при* $n \to \infty$.

Тогда при $n \to \infty$

$$\mathcal{P}_{t,n} > 2 - \exp\left\{ e^{-\omega} + o(1) \right\}.$$

Теорема 2. *Пусть* 1) $g(u) \neq Const$ *и* $g(u) = g(u \oplus (1, \ldots, 1))$ *для любого вектора* $u \in V_r$, 2) $t = \gamma^{-1} n(\ln n + \omega)$, $\omega = O(1)$ *при* $n \to \infty$.

Тогда при $n \to \infty$

$$\mathcal{P}_{t,n} > 3 - 2\exp\left\{ e^{-\omega} + o(1) \right\}.$$

Доказательство теоремы 1. Предположим, что некоторый вектор z имеет q единичных и $n_0 - q$ нулевых координат с индексами из множества I_0, а также p нулевых и $n_1 - p$ единичных координат с индексами

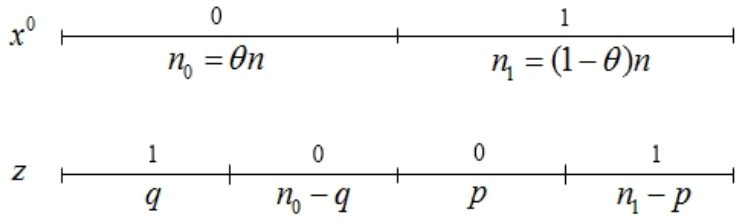

Рис. 1. Схематичное представление векторов x^0 и z

из множества I_1 (см. определения множеств I_0, I_1 перед обозначениями (3)). Пусть

$$\tilde{P}(p,q) = \mathbf{P}\{g(z_{s_{i,1}}, \ldots, z_{s_{i,r}}) \neq g(x^o_{s_{i,1}}, \ldots, x^o_{s_{i,r}})\} \tag{6}$$

– вероятность того, что функция g при случайном (но одинаковом) выборе значений аргументов из векторов x^o, z принимает различные значения.

Отметим, что величина $\tilde{P}(p,q)$ не зависит от конкретных вариантов пересечения множества индексов q единичных координат вектора z с множеством I_0 и от конкретных вариантов пересечения множества индексов p нулевых координат вектора z с множеством I_1. При фиксированных p и q удобно представлять векторы x^o и z в следующем виде:

Воспользуемся следующим неравенством для вероятности $\mathcal{P}_{t,n}$ правильного решения системы уравнений (1) методом максимума правдоподобия:

$$\mathcal{P}_{t,n} = \mathbf{P}\left\{S(x^o) \leqslant \min_{z \neq x^o} S(z)\right\} > 1 - \sum_{1 \leqslant q+p \leqslant n} C^q_{n_0} C^p_{n_1} \{1 - \tilde{P}(p,q)\Delta\}^t, \tag{7}$$

где $\Delta = 1 - \sqrt{4\delta(1-\delta)}$. Это неравенство получено Г. В. Балакиным, его вывод можно найти также в [6] (см. формулу (14) в этой работе и ее доказательство, которое начинается с формулы (8); следует учесть, что в указанной формуле из [6], в отличие от нашей формулы (5), вместо символа p используется обозначение k_0 и вместо q используется разность $k - k_0$).

Разобьем сумму в правой части (7) на три слагаемых:

$$\sum_{1 \leqslant q+p \leqslant n} = \sum_{1 \leqslant q+p \leqslant n^{1/3}} + \sum_{n^{1/3} < q+p \leqslant \varepsilon n} + \sum_{\varepsilon n < q+p \leqslant n} = \Sigma_1 + \Sigma_2 + \Sigma_3 \tag{8}$$

и оценим каждое слагаемое отдельно.

Отметим, что величина $\tilde{P}(p,q)$ оценивается снизу суммой вероятностей попарно несовместных событий, каждое из которых состоит в том, что пара векторов $((z_{s_{i,1}},\dots,z_{s_{i,r}}),(x^o_{s_{i,1}},\dots,x^o_{s_{i,r}}))$ принимает некоторое значение из множеств $B_r^{(1)}(k)$, $k=0,\dots,r-1$ (см. (4) и выше) и для которых $g(z_{s_{i,1}},\dots,z_{s_{i,r}})\neq g(x^o_{s_{i,1}},\dots,x^o_{s_{i,r}})$. Отметим также, что при фиксированном k эти события равновероятны. Отсюда находим (см. рис. 1)

$$\tilde{P}(p,q)\geqslant\sum_{k=0}^{r-1}\frac{(p+q)(n_1-p)_k(n_0-q)_{r-1-k}}{(n)_r}\cdot\gamma(k), \tag{9}$$

где величина $\gamma(k)$ определяется формулой (4). Используя это неравенство, получаем при $p+q\leqslant n^{1/3}$

$$\begin{aligned}\tilde{P}(p,q)\Delta&\geqslant\frac{p+q}{n}\Delta\sum_{k=0}^{r-1}(1-\theta)^k\theta^{r-1-k}\gamma(k)(1+O(n^{-2/3}))\\&=\gamma\frac{p+q}{n}(1+O(n^{-2/3})).\end{aligned}$$

Положим $t=\gamma^{-1}n(\ln n+\omega)$, $\omega=O(1)$. При этом условии, используя неравенство $1-x<e^{-x}$ при $0<x<1$, получаем

$$\begin{aligned}\Sigma_1&=\sum_{1\leqslant q+p\leqslant n^{1/3}}C_{n_0}^qC_{n_1}^p\{1-\tilde{P}(p,q)\Delta\}^t\leqslant\sum_{1\leqslant q+p\leqslant n^{1/3}}C_{n_0}^qC_{n_1}^p\exp\{-t\tilde{P}(p,q)\Delta\}\\&=\sum_{1\leqslant q+p\leqslant n^{1/3}}C_{n_0}^qC_{n_1}^p\exp\left\{-(\ln n+\omega)(p+q)+O\left(\frac{\ln n}{n^{1/3}}\right)\right\}\\&=\sum_{1\leqslant q+p\leqslant n^{1/3}}\frac{\theta^q}{q!}\frac{(1-\theta)^p}{p!}\exp\left\{-\omega(p+q)+O\left(\frac{\ln n}{n^{1/3}}\right)\right\}\\&=\exp\left\{e^{-\omega}+o(1)\right\}-1.\end{aligned} \tag{10}$$

Оценим теперь вторую сумму в правой части (8). При $\varepsilon<\min(\theta,1-\theta)$ из неравенства (9) получаем (здесь используем обозначение $[\varepsilon n]'$ для целой части числа εn)

$$\begin{aligned}\tilde{P}(p,q)\Delta&\geqslant\Delta\sum_{k=0}^{r-1}\frac{(p+q)(n_1-[\varepsilon n]'-1)_k(n_0-[\varepsilon n]'-1)_{r-1-k}}{(n)_r}\cdot\gamma(k)\\&=\gamma_\varepsilon\frac{p+q}{n}(1+O(n^{-2/3})),\end{aligned}$$

где

$$\gamma_\varepsilon = \Delta \sum_{k=0}^{r-1} (1-\theta-\varepsilon)^k (\theta-\varepsilon)^{r-1-k} \gamma(k).$$

Поэтому

$$\Sigma_2 < \sum_{n^{1/3}<q+p\leqslant \varepsilon n} C_n^{p+q} \exp\left\{-t\gamma_\varepsilon \frac{p+q}{n}(1+O(n^{-2/3}))\right\}$$

$$< \sum_{n^{1/3}<q+p\leqslant \varepsilon n} \exp\left\{-n\left[\frac{\gamma_{\varepsilon,n}}{\gamma}\cdot\frac{p+q}{n}\ln n - h\left(\frac{p+q}{n}\right) + O\left(\frac{\ln n}{n}\right)\right]\right\},$$

где

$$\gamma_{\varepsilon,n} = \gamma_\varepsilon(1+O(\ln^{-1} n),$$

$$h(y) = -y\ln y - (1-y)\ln(1-y), \qquad 0<y<1.$$

Положим $\varphi_{\varepsilon,n}(y) = \frac{\gamma_{\varepsilon,n}}{\gamma}\cdot y\ln n - h(y)$. При малых значениях ε и больших значениях n производная $\varphi'_{\varepsilon,n}(y)$ в интервале $n^{-2/3} < y < \varepsilon$ положительна:

$$\varphi'_{\varepsilon,n}(y) = \frac{\gamma_{\varepsilon,n}}{\gamma}\cdot\ln n + \ln y - \ln(1-y) > 0.$$

Значит, функция $\varphi_{\varepsilon,n}(y)$, принимающая положительные значения в указанном интервале, растет. Следовательно,

$$\Sigma_2 < n^2 \exp\left\{-n\left[\frac{\gamma_{\varepsilon,n}}{\gamma}\cdot\frac{p+q}{n}\ln n - h\left(\frac{p+q}{n}\right) + O\left(\frac{\ln n}{n}\right)\right]\right\}\Bigg|_{p+q=[n^{1/3}]}$$

$$= n^2 \exp\left\{-\left(\frac{\gamma_{\varepsilon,n}}{\gamma}-\frac{2}{3}\right)n^{1/3}\ln n + O\left(n^{1/3}\right)\right\} = o(1) \qquad (11)$$

в силу того, что $\gamma_{\varepsilon,n}\to\gamma$ при $\varepsilon\to 0$, $n\to\infty$.

Оценим третью сумму в правой части (8). Исследуем поведение вероятностей $\tilde{P}(p,q)$ при $n\to\infty$, $(p+q)/n > \varepsilon$. Рассмотрим три возможных при данном условии случая относительно значений p, q.

1. Пусть

$$p \geqslant \varepsilon n_1, \;\; q \leqslant \varepsilon n_0. \qquad (12)$$

Положим

$$\alpha_1(k) = |\{u\in V_r : ||u|| = k,\, g(u)\neq g(0^r)\}|, \qquad (13)$$

где $(0^r) = (0,\ldots,0)$ – нулевой r-мерный вектор.

Заметим, что величину $\tilde{P}(p,q)$ можно оценить снизу суммой вероятностей попарно несовместных событий, каждое из которых состоит в том, что пара векторов $((z_{s_{i,1}},\dots,z_{s_{i,r}}),(x^o_{s_{i,1}},\dots,x^o_{s_{i,r}}))$ принимает значение вида $((0^r),(u_1,\dots,u_r))$, где $(u_1,\dots,u_r)\in\{u\in V_r\colon ||u||=k,\ g(u)\neq g(0^r)\}$. С учетом этого замечания получаем (см. рис. 1)

$$\tilde{P}(p,q)\geqslant\sum_{k=0}^{r}\frac{(p)_k(n_0-q)_{r-k}}{(n)_r}\cdot\alpha_1(k)$$

$$=\big(1+O(n^{-1})\big)\sum_{k=0}^{r}\left(\frac{p}{n}\right)^k\left(\frac{n_0-q}{n}\right)^{r-k}\alpha_1(k)\geqslant B_n^{(1)}(\varepsilon,\theta),\qquad(14)$$

где

$$B_n^{(1)}(\varepsilon,\theta)=\big(1+O(n^{-1})\big)\sum_{k=0}^{r}(\varepsilon(1-\theta))^k((1-\varepsilon)\theta)^{r-k}\alpha_1(k),$$

так как $p\geqslant\varepsilon n_1=\varepsilon(1-\theta)n$, $n_0-q\geqslant n_0-\varepsilon n_0=(1-\varepsilon)\theta n$. Согласно условию $g\neq$Const и определению (13) имеем $\sum_{k=0}^{r}\alpha_1(k)\neq 0$. Следовательно, $B_n^{(1)}(\varepsilon,\theta)>0$, начиная с некоторого значения n, и

$$\Sigma_{3,1}=\sum_{\substack{\varepsilon n<p+q\leqslant n\\ p\geqslant\varepsilon n_1,\ q\leqslant\varepsilon n_0}}C_{n_1}^{p}C_{n_0}^{q}[1-\tilde{P}(p,q)\Delta]^t\leqslant\exp\{-tB_n^{(1)}(\varepsilon,\theta)\Delta\}2^n=o(1).\qquad(15)$$

Рассмотрим второй случай для значений p, q при условии $\varepsilon n<p+q\leqslant n$.

2. Пусть

$$p\leqslant\varepsilon n_1,\ \ q\geqslant\varepsilon n_0.\qquad(16)$$

Положим

$$\alpha_2(k)=\left|\{u\in V_r\colon ||u||=k,g(u)\neq g(1^r)\}\right|,\qquad(17)$$

где $(1^r)=(1,\dots,1)$ – r-мерный вектор, состоящий из единиц.

Величину $\tilde{P}(p,q)$ можно оценить снизу суммой вероятностей попарно несовместных событий, каждое из которых состоит в том, что пара векторов $((z_{s_{i,1}},\dots,z_{s_{i,r}}),(x^o_{s_{i,1}},\dots,x^o_{s_{i,r}}))$ принимает значение вида $((1^r),(u_1,\dots,u_r))$, где $(u_1,\dots,u_r)\in\{u\in V_r\colon ||u||=k,\ g(u)\neq g(1^r)\}$. Поэтому (см. рис. 1)

$$\tilde{P}(p,q)\geqslant\sum_{k=0}^{r}\frac{(n_1-p)_k(q)_{r-k}}{(n)_r}\cdot\alpha_2(k)$$

$$= \bigl(1 + O(n^{-1})\bigr) \sum_{k=0}^{r} \left(\frac{n_1 - p}{n}\right)^k \left(\frac{q}{n}\right)^{r-k} \alpha_2(k) \geqslant B_n^{(2)}(\varepsilon, \theta), \qquad (18)$$

где

$$B_n^{(2)}(\varepsilon, \theta) = \bigl(1 + O(n^{-1})\bigr) \sum_{k=0}^{r} ((1-\varepsilon)(1-\theta))^k (\varepsilon\theta)^{r-k} \alpha_2(k).$$

Значит, $B_n^{(2)}(\varepsilon, \theta) > 0$ при достаточно больших значениях n. Следовательно,

$$\Sigma_{3,2} = \sum_{\substack{\varepsilon n < p+q \leqslant n \\ p \leqslant (\varepsilon/2)n,\ q \geqslant (\varepsilon/2)n}} C_{n_0}^q C_{n_1}^p [1 - \bar{P}(p,q)\Delta]^t$$

$$\leqslant \exp\{-tB_n^{(2)}(\varepsilon, \theta)\Delta\} 2^n = o(1). \qquad (19)$$

Осталось рассмотреть последний случай.

3. Пусть $p \geqslant \varepsilon n_1$, $q \geqslant \varepsilon n_0$. Положим

$$\alpha_3(k) = \left|\{u \in V_r \colon ||u|| = k, g(u) \neq g(u \oplus 1^r)\}\right|. \qquad (20)$$

Теперь величину $\tilde{P}(p,q)$ оценим снизу суммой вероятностей попарно несовместных событий, каждое из которых состоит в том, что пара векторов $((z_{s_{i,1}}, \ldots, z_{s_{i,r}}), (x^o_{s_{i,1}}, \ldots, x^o_{s_{i,r}}))$ принимает значение вида $((u_1, \ldots, u_r), (u_1 \oplus 1, \ldots, u_r \oplus 1))$, где $(u_1, \ldots, u_r) \in \{u \in V_r \colon ||u|| = k, g(u) \neq g(u \oplus 1)\}$.

Имеем

$$\tilde{P}(p,q) \geqslant \sum_{k=0}^{r} \frac{(p)_k (q)_{r-k}}{(n)_r} \cdot \alpha_3(k) \geqslant B_n^{(3)}(\varepsilon, \theta),$$

где

$$B_n^{(3)}(\varepsilon, \theta) = \bigl(1 + O(n^{-1})\bigr) \sum_{k=0}^{r} (\varepsilon(1-\theta))^k (\varepsilon\theta)^{r-k} \alpha_3(k).$$

Согласно первому условию теоремы и определению (20) выполнено неравенство $\sum_{k=0}^{r} \alpha_3(k) > 0$. Следовательно, $B_n^{(3)}(\varepsilon) > 0$ (при достаточно больших значениях n) и

$$\Sigma_{3,3} = \sum_{\substack{\varepsilon n < p+q \leqslant n \\ p \geqslant \varepsilon n_1,\ q \geqslant \varepsilon n_0}} C_{n_1}^p C_{n_0}^q [1 - \tilde{P}(p,q)\Delta]^t \leqslant \exp\{-tB_n^{(3)}(\varepsilon, \theta)\Delta\} 2^n = o(1). \qquad (21)$$

Теперь из (2), (7), (8), (10), (15), (19), (21) вытекает утверждение теоремы 1. Теорема 1 доказана. □

Доказательство теоремы 2. При условии 1 теоремы 2 имеем

$$g(x^o_{s_{i,1}} \dots, x^o_{s_{i,r}}) = g(x^o_{s_{i,1}} \oplus 1.., x^o_{s_{i,r}} \oplus 1), \quad i = \overline{1,t}.$$

Используя это равенство и повторяя выкладки работы [6], связанные с выводом неравенства (7), получим неравенство

$$\mathcal{P}_{t,n} = \mathbf{P}\left\{S(x^o) \leqslant \min_{z \not\subseteq \{x^o, x^o \oplus 1^n\}} S(z)\right\} > 1 - \sum_{1 \leqslant p+q \leqslant n-1} C^p_{n_1} C^q_{n_0} \{1 - \tilde{P}(p,q)\Delta\}^t, \tag{22}$$

которое отличается от неравенства (7) только верхним пределом суммирования в его правой части.

Пусть вектору z относительно вектора x^o соответствуют параметры p, q, тогда вектору $z \oplus 1^r$ относительно вектора x^o соответствуют параметры $n_1 - p$, $n_0 - q$ (см. рис. 1). Поэтому согласно определению величины $\tilde{P}(p,q)$ (см. (6)) и равенствам $g(z) = g(z \oplus 1^r)$ имеем

$$\tilde{P}(p,q) = \tilde{P}(n_1 - p, n_0 - q). \tag{23}$$

Следовательно,

$$A(p,q) = A(n_1 - p, n_0 - q), \tag{24}$$

где

$$A(p,q) = C^p_{n_1} C^q_{n_0} \{1 - \tilde{P}(p,q)\Delta\}^t.$$

Значит, сумма в правой части (22) представляется в виде

$$\sum_{1 \leqslant p+q \leqslant n-1} A(p,q) = 2 \sum_{1 \leqslant p+q \leqslant n^{1/3}} A(p,q) + 2 \sum_{n^{1/3} < p+q \leqslant \varepsilon n} A(p,q) + \sum_{\varepsilon n < p+q < (1-\varepsilon)n} A(p,q), \tag{25}$$

где значение ε достаточно мало. В доказательстве теоремы 1 показано, что

$$\sum_{1 \leqslant p+q \leqslant n^{1/3}} A(p,q) = \exp\left\{e^{-z} + o(1)\right\} - 1, \tag{26}$$

$$\sum_{n^{1/3} < p+q \leqslant \varepsilon n} A(p,q) = o(1). \tag{27}$$

Отметим, что для доказательства этих соотношений использовались только условие $g(u) \neq Const$ и условие 2 теоремы 1 (теоремы 2).

Рассмотрим теперь третью сумму в правой части равенства (25). Используя выкладки (12)–(15) и равенство (23), получаем, что

$$\sum_{\substack{\varepsilon n<p+q<(1-\varepsilon)n \\ p\geqslant\varepsilon n_1,\ q\leqslant\varepsilon n_0}} A(p,q) = \sum_{\substack{\varepsilon n<p+q<(1-\varepsilon)n \\ p\leqslant(1-\varepsilon)n_1,\ q\geqslant(1-\varepsilon)n_0}} A(p,q) = o(1), \tag{28}$$

затем, используя выкладки (16)–(19) и равенство (23), находим

$$\sum_{\substack{\varepsilon n<p+q<(1-\varepsilon)n \\ p\leqslant\varepsilon n_1,\ q\geqslant\varepsilon n_0}} A(p,q) = \sum_{\substack{\varepsilon n<p+q<(1-\varepsilon)n \\ p\geqslant(1-\varepsilon)n_1,\ q\leqslant(1-\varepsilon)n_0}} A(p,q) = o(1). \tag{29}$$

Осталось показать, что

$$\sum_{\substack{\varepsilon n_1\leqslant p\leqslant(1-\varepsilon)n_1 \\ \varepsilon n_0\leqslant q\leqslant(1-\varepsilon)n_0}} A(p,q) = o(1). \tag{30}$$

Выберем любую пару векторов $u^1 = (u^1_1, \ldots, u^1_r)$, $u^2 = (u^2_1, \ldots, u^2_r)$ из множества V_r, удовлетворяющих условию $g(u^1) \neq g(u^2)$. Определим числа $r(k,l)$, где $k,l \in \{0,1\}$, формулой

$$r(k,l) = |\{i \in \{1,\ldots,r\}\colon u^1_i = k, u^2_i = l\}|.$$

При условии $\varepsilon n_1 \leqslant p \leqslant (1-\varepsilon)n_1$, $\varepsilon n_0 \leqslant q \leqslant (1-\varepsilon)n_0$ оценим снизу величину $\tilde{P}(p,q)$ вероятностью события, состоящего в том, что пара векторов $((z_{s_{i,1}}, \ldots, z_{s_{i,r}}), (x^o_{s_{i,1}}, \ldots, x^o_{s_{i,r}}))$ принимает значение $((u^1_1, \ldots, u^1_r), (u^2_1, \ldots, u^2_r))$. Получим (см. рис. 1)

$$\tilde{P}(p,q) \geqslant \frac{(n_0-q)_{r(0,0)} \cdot (q)_{r(0,1)} \cdot (p)_{r(1,0)} \cdot (n_1-p)_{r(1,1)}}{(n_r)} \geqslant B_n(\varepsilon,\theta),$$

где

$$B_n(\varepsilon,\theta) = \frac{(\varepsilon n_0)_{r(0,0)} \cdot (\varepsilon n_0)_{r(0,1)} \cdot (\varepsilon n_1)_{r(1,0)} \cdot (\varepsilon n_1)_{r(1,1)}}{(n_r)}$$
$$= (\varepsilon\theta)^{r(0,0)+r(0,1)} (\varepsilon(1-\theta))^{r(1,0)+r(1,1)} (1+O(n^{-1}))$$

– величина, строго бóльшая нуля при достаточно больших значениях n. С учетом этого факта можно повторить выкладки вида (21) и получить оценку (30). Из (28)–(30) следует, что третья сумма в правой части (25)

$$\sum_{\varepsilon n<p+q<(1-\varepsilon)n} = o(1). \tag{31}$$

Теперь из (22), (25)–(27), (31) следует утверждение теоремы 2.
Теорема 2 доказана.

□

Список литературы

[1] Балакин Г.В., "Графы двучленных систем уравнений с булевыми неизвестными", *Теория вероятн. и ее примен.*, **40**:2 (1995), 241–259.

[2] Балакин Г.В., "Введение в теорию случайных систем уравнений", *Труды по дискретной математике*, **1** (1997), 1–18.

[3] Балакин Г.В., "'Системы случайных булевых уравнений со случайным выбором неизвестных в каждом уравнений", *Труды по дискретной математике*, **3** (2000), 21–28.

[4] Михайлов В.Г., "Предельные теоремы для случайного покрытия конечного множества и для числа решений системы случайных уравнений", *Теория вероятн. и ее примен.*, **41**:2 (1996), 272–283.

[5] Михайлов В.Г., "Изучение предельного поведения числа решений систем уравнений со случайным вхождением неизвестных", *Математические вопросы криптографии*, **1**:3 (2010), 27–49.

[6] Тарасов А.В., "Параметры метода максимального правдоподобия при его использовании для решения систем дважды биюнктивных уравнений с искаженными правыми частями", *Математические вопросы криптографии*, **11**:3 (2020), 79–100.

[7] Копытцев В.А., "О распределении числа решений случайных заведомо совместных систем уравнений", *Теория вероятн. и ее примен.*, **40**:2 (1995), 430–437.