



Math-Net.Ru

All Russian mathematical portal

V. G. Mikhailov, Limit theorems for the number of nonzero solutions of a system of random equations over the field  $\text{GF}(2)$ ,

*Diskr. Mat.*, 2000, Volume 12, Issue 1, 70–81

<https://www.mathnet.ru/eng/dm318>

Use of the all-Russian mathematical portal Math-Net.Ru implies that you have read and agreed to these terms of use

<https://www.mathnet.ru/eng/agreement>

Download details:

IP: 18.97.14.91

May 13, 2025, 02:54:21



УДК 519.2

## Предельные теоремы для числа ненулевых решений одной системы случайных уравнений над полем $\text{GF}(2)$

© 2000 г. В. Г. Михайлов

Исследуются свойства числа  $\nu$  ненулевых решений системы случайных уравнений, левые части которых являются произведениями выражений вида  $a_{t1}x_1 + \dots + a_{tn}x_n + a_t$  в поле  $\text{GF}(2)$  с независимыми равновероятными коэффициентами при переменных, а правые части равны нулю. Получены неравенства для факториальных моментов случайной величины  $\nu$ , а также необходимые и достаточные условия выполнения для  $\nu$  предельной теоремы Пуассона.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, проект 99-01-00012, и Совета по грантам Президента РФ и государственной поддержке ведущих научных школ, проект 96-15-96092.

Рассмотрим систему случайных нелинейных уравнений над полем  $\text{GF}(2)$

$$\prod_{i=1}^{m_t} (a_{t1}^i x_1 + \dots + a_{tn}^i x_n + a_t^i) = 0, \quad t = 1, \dots, T, \quad (1)$$

где  $m_t \in \{1, \dots, n\}$ , а коэффициенты  $a_{ij}^i$  являются независимыми случайными величинами, принимающими значения 0 и 1 с вероятностями  $1/2$ . Величины  $a_t^i$  считаются заданными. Если при всех  $t = 1, \dots, T$  выполнено равенство  $a_t^1 \dots a_t^{m_t} = 0$ , то система (1) имеет нулевое решение. В остальных случаях его нет. Чтобы не загромождать изложение разбором этих двух случаев, мы будем изучать число  $\nu$  ненулевых решений системы (1).

Введем обозначение  $V^n$  для  $n$ -мерного линейного пространства над полем  $\text{GF}(2)$  и обозначение  $(m)_r = m(m-1) \dots (m-r+1)$ . Положим

$$\Lambda = (2^n - 1) \prod_{t=1}^T (1 - 2^{-m_t}). \quad (2)$$

Как будет показано ниже (см. равенство (19)),  $\Lambda = \mathbf{E}\nu$ .

**Теорема 1.** При  $n \geq r \geq 1$  выполнены неравенства

$$\mathbf{E}(\nu)_r \geq \Lambda^r \prod_{s=0}^{r-1} \frac{2^n - 2^s}{2^n - 1}, \quad (3)$$

$$\mathbf{E}(\nu)_r < \Lambda^r + (\Lambda + 2^{r-1})^r \prod_{t=1}^T \left( 1 - \frac{2^{m_t} - 2}{(2^{m_t} - 1)^2} \right). \quad (4)$$

Введем обозначение

$$\Delta(m_1, \dots, m_T) = \sum_{t=1}^T \frac{2^{m_t} - 2}{(2^{m_t} - 1)^2}.$$

**Теорема 2.** Пусть параметры  $n$  и  $T$  стремятся к бесконечности, а параметры  $m_1, \dots, m_T$  меняются так, что  $\Lambda \rightarrow \lambda$ ,  $0 < \lambda < \infty$ , и

$$\Delta(m_1, \dots, m_T) \rightarrow \infty. \quad (5)$$

Тогда равномерно по наборам свободных членов  $\{a_i^i\}$

$$\mathbf{E}(\nu)_r \rightarrow \lambda^r, \quad r = 1, 2, \dots, \quad (6)$$

а распределение случайной величины  $\nu$  сходится к распределению Пуассона с параметром  $\lambda$  и эта сходимость равномерна по наборам свободных членов  $\{a_i^i\}$ .

**Теорема 3.** Пусть параметры  $n$  и  $T$  стремятся к бесконечности, а параметры  $m_1, \dots, m_T$  меняются таким образом, что выполнены условия

$$\Lambda \rightarrow \infty, \quad \Lambda \leq \frac{n}{10}, \quad \Lambda^2 \leq \frac{\Delta(m_1, \dots, m_T)}{49 \ln 2}. \quad (7)$$

Тогда функция распределения случайной величины  $(\nu - \Lambda)\Lambda^{-1/2}$  сходится к стандартной нормальной функции распределения равномерно по наборам  $\{a_i^i\}$ .

**Замечание 1.** Из теорем 1, 2 и 3 вытекают аналогичные утверждения для системы вида (1) со случайными свободными членами  $a_i^i$ . В этом случае распределение свободных членов может быть произвольным, достаточно предполагать лишь независимость набора  $\{a_i^i\}$  от набора случайных коэффициентов  $\{a_{i,j}^i\}$ . Кстати, при равновероятном выборе набора  $\{a_i^i\}$  из  $2^M$ ,  $M = m_1 + \dots + m_T$ , возможных оказывается, что при условии (5) вероятность наличия нулевого решения стремится к нулю. Поэтому в условиях теоремы 2 имеет место предельная теорема Пуассона с параметром  $\lambda$  и для общего числа решений.

**Замечание 2.** Случай  $m_1 = \dots = m_T \geq 2$  изучался в работе [1], где были получены утверждения, аналогичные теоремам 1, 2 и 3, и ряд иных результатов. В отличие от [1] в настоящей работе допускается ситуация, когда в систему (1) входят уравнения различных степеней (здесь под степенью уравнения понимается число сомножителей произведения в левой части (1), которое, разумеется, с некоторой вероятностью может отличаться от истинной степени случайного уравнения), в том числе и линейные уравнения.

**Замечание 3.** Условие (5) теоремы 2 эквивалентно условию

$$\sum_{t: m_t \geq 2} 2^{-m_t} \rightarrow \infty. \quad (8)$$

Если все  $m_t \geq 2$ , то условие (8) (а значит, и условие (5)) следует из условия  $\Lambda \rightarrow \lambda$ ,  $0 < \lambda < \infty$ . Поскольку  $\Lambda = \mathbf{E}\nu$ , это означает, что условие (5) является в данном случае необходимым для сходимости моментов случайной величины  $\nu$  к моментам предельного пуассоновского распределения.

Следующее утверждение показывает, что и в общем случае условие (5) необходимо для сходимости (6).

**Теорема 4.** Пусть при  $n \rightarrow \infty$

$$\mathbf{E}(\nu)_r \rightarrow \lambda^r, \quad r = 1, 3, 4. \quad (9)$$

Тогда выполнено условие (5).

Описание основных задач теории систем случайных уравнений над конечными полями можно найти в книгах [2, 3] и работах [4, 5, 6]. Задача о числе решений системы случайных уравнений тесно связана с задачей о числе непокрытых точек при покрытии конечного множества его случайно выбираемыми подмножествами. Роль таких подмножеств играют дополнения к множествам решений отдельных уравнений системы (см. [7]).

Важным классом систем случайных уравнений являются заведомо совместные системы случайных уравнений. Асимптотические свойства числа решений ряда таких систем нелинейных уравнений изучалось в работах [8] и [9]. В работах [10–12] исследовались некоторые заведомо совместные системы нелинейных уравнений, в которых случайной была лишь правая часть. В этих работах в качестве предельных появлялись логарифмически пуассоновское и логарифмически нормальное распределения. В литературе отмечалось также, что в качестве предельного распределения для числа ложных решений заведомо совместных систем случайных булевых уравнений может выступать и пуассоновское распределение (см., например, [13]).

Перейдем к доказательствам.

Доказательство теоремы 1 во многом повторяет рассуждения работы [1]. Однако мы приводим его достаточно подробно, поскольку ряд промежуточных результатов потребуется при доказательстве теоремы 4.

Система уравнений (1) эквивалентна системе из  $T$   $m_t$ -мерных включений (здесь и далее под включением понимается соотношение типа вектор принадлежит множеству)

$$\begin{pmatrix} a_{t1}^1 x_1 + \dots + a_{tn}^1 x_n \\ \dots \\ a_{t1}^{m_t} x_1 + \dots + a_{tn}^{m_t} x_n \end{pmatrix} \in D \begin{pmatrix} a_t^1 \\ \dots \\ a_t^{m_t} \end{pmatrix}, \quad t = 1, \dots, T, \quad (10)$$

где множество  $D(a)$ ,  $a \in V^{m_t}$ , получается из множества  $V^{m_t}$  выбрасыванием вектора  $a + 1^{m_t}$  (вектор  $1^m$  имеет размерность  $m$  и состоит из одних единиц, аналогичный смысл имеет обозначение  $0^m$ ).

Запишем систему включений (10) относительно вектора  $x = (x_1, \dots, x_n)$  (рассматриваемого как вектор-столбец) как одно включение

$$Ax \in B \tag{11}$$

в пространстве размерности

$$M = m_1 + \dots + m_T.$$

Для этого обозначим матрицу размера  $m_t \times n$  случайных коэффициентов линейных форм из левой части включения (10) через  $A_t$ , а вектор-столбец в обозначении множества в правой части (10) через  $a_t$ . В качестве матрицы  $A$  возьмем матрицу размера  $M \times n$ , полученную расположением друг под другом в естественном порядке матриц  $A_t$ ,  $t = 1, \dots, T$ . В качестве множества  $B$  возьмем множество

$$B = D(a_1) \times \dots \times D(a_T).$$

Заметим, что

$$|B| = \prod_{t=1}^T (2^{m_t} - 1). \tag{12}$$

При выбранных  $A$  и  $B$  система (10) теперь запишется в виде (11).

Сопоставим каждой паре значений

$$(x, b), \quad x \in V^n \setminus \{0^n\}, \quad b \in B,$$

случайную величину

$$\eta_{x,b} = I\{Ax = b\}.$$

Тогда

$$\nu = \sum_{x \in V^n \setminus \{0^n\}} \sum_{b \in B} \eta_{x,b}. \tag{13}$$

Из этого равенства вытекает следующее выражение для факториальных моментов случайной величины  $\nu$ :

$$\mathbf{E}(\nu)_r = \sum_S \mathbf{E} \eta_{x^1, b^1} \dots \eta_{x^r, b^r}, \tag{14}$$

где

$$S = \{((x^1, b^1), \dots, (x^r, b^r)) \in ((x \in V^n \setminus \{0^n\}) \times B)^r : (x^i, b^i) \neq (x^j, b^j), i \neq j\}. \tag{15}$$

**Лемма 1.** Пусть  $n \geq r \geq k \geq 1$ ,  $x^1, \dots, x^r \in V^n \setminus \{0^n\}$ , и  $\text{rank}(x^1, \dots, x^r) = k$ . Тогда если для любых  $i_1, \dots, i_s$ ,  $s \leq r$ , выполнено неравенство

$$\text{rank}(b^{i_1}, \dots, b^{i_s}) \leq \text{rank}(x^{i_1}, \dots, x^{i_s}),$$

то

$$\mathbf{E} \eta_{x^1, b^1} \dots \eta_{x^r, b^r} = \frac{1}{2^{kM}}; \tag{16}$$

если

$$\text{rank}(b^{i_1}, \dots, b^{i_s}) \geq \text{rank}(x^{i_1}, \dots, x^{i_s})$$

для некоторых  $i_1, \dots, i_s$ ,  $s \leq r$ , то

$$\mathbf{E}\eta_{x^1, b^1} \dots \eta_{x^r, b^r} = 0. \quad (17)$$

Доказательство леммы 1 достаточно прозрачно, и мы его опустим.

Из леммы 1 вытекает следующий результат, которым мы будем неоднократно пользоваться в дальнейшем.

**Лемма 2.** Пусть  $x^1, \dots, x^r \in V^n \setminus \{0^n\}$  и  $\text{rank}(x^1, \dots, x^r) = k$ . Тогда при любых  $b^1, \dots, b^r \in B$  выполнено неравенство

$$\mathbf{P}\{\eta_{x^1, b^1} = \dots = \eta_{x^r, b^r} = 1\} \leq \frac{1}{2^{kM}}, \quad (18)$$

причем при  $k = r$  в (19) имеет место равенство.

Непосредственно из леммы 1 следует равенство

$$\mathbf{E}\nu = \sum \eta_{x^1, b^1} = |B||V^n \setminus \{0^n\}|2^{-M} = (2^n - 1) \prod_{t=1}^T (1 - 2^{-m_t}). \quad (19)$$

Рассмотрим старшие факториальные моменты (при  $2 \leq r \leq n$ ). Введем обозначение

$$S_{r,k} = \{(x^1, \dots, x^r) : x^1, \dots, x^r \in V^n \setminus \{0^n\} \text{ различны, } \text{rank}(x^1, \dots, x^r) = k\}.$$

Очевидно, что  $S_{r,0} = S_{r,1} = \emptyset$ ,  $r \geq 2$ ,  $S_{r,2} = \emptyset$ ,  $r \geq 4$ .

Заметим, что слагаемые в (14), для которых

$$x^{i_1} + \dots + x^{i_s} = 0^n, \quad b^{i_1} + \dots + b^{i_s} \neq 0^M,$$

равны нулю. Остальные группируем в суммы по  $S_{r,k}$ ,  $k = 2, \dots, r$ , и получаем выражение

$$\mathbf{E}(\nu)_r = \sum_{k=2}^r \sum_{(x^1, \dots, x^r) \in S_{r,k}} \sum_{b^1, \dots, b^r \in B} \mathbf{E}\eta_{x^1, b^1} \dots \eta_{x^r, b^r}. \quad (20)$$

Согласно лемме 2

$$\sum_{(x^1, \dots, x^r) \in S_{r,r}} \sum_{b^1, \dots, b^r \in B} \mathbf{E}\eta_{x^1, b^1} \dots \eta_{x^r, b^r} = \frac{|B|^r |S_{r,r}|}{2^{rM}}.$$

Поэтому с учетом равенства

$$|S_{r,r}| = \prod_{s=0}^{r-1} (2^n - 2^s)$$

и формулы (12) получаем, что

$$\sum_{(x^1, \dots, x^r) \in S_{r,r}} \sum_{b^1, \dots, b^r \in B} \mathbf{E} \eta_{x^1, b^1} \dots \eta_{x^r, b^r} = \Lambda^r \prod_{s=1}^{r-1} \frac{2^n - 2^s}{2^n - 1}. \quad (21)$$

Из (20) и (21) следует (3).

Из (20) и (21) вытекает также равенство

$$\mathbf{E}(\nu)_2 = \frac{2^n - 2}{2^n - 1} \Lambda^2. \quad (22)$$

Перейдем к построению верхней оценки. Каждому набору векторов  $x^1, \dots, x^r$  из  $V^n \setminus \{0^n\}$  соответствует система  $L_x(x^1, \dots, x^r)$  однородных линейных уравнений в  $V^n$  вида

$$x^{i1} + \dots + x^{is} = 0^n,$$

возможно пустая, описывающая все линейные соотношения между  $x^1, \dots, x^r$ . Системе  $L_x(x^1, \dots, x^r)$  сопоставим идентичную систему  $L_b(x^1, \dots, x^r)$  из линейных уравнений относительно  $b^1, \dots, b^r \in B$ . Обозначим через  $B(x^1, \dots, x^r)$  множество решений  $(b^1, \dots, b^r) \in B^r$  системы уравнений  $L_b(x^1, \dots, x^r)$ .

Из (20) и леммы 2 следует оценка

$$\mathbf{E}(\nu)_r \leq \sum_{k=2}^r \sum_{(x^1, \dots, x^r) \in S_{r,k}} \frac{1}{2^{kM}} |B(x^1, \dots, x^r)|. \quad (23)$$

Обозначим через  $C(r, d; u_1, \dots, u_T)$  число решений  $(b^1, \dots, b^r)$  уравнения

$$b^1 + \dots + b^r = d, \quad b^1, \dots, b^r, d \in B, \quad (24)$$

где

$$B = B_1 \times \dots \times B_T, \quad B_t = V^{m_t} \setminus \{u_t\}, \quad u_t \in V^{m_t}, \quad t = 1, \dots, T.$$

**Лемма 3.** Для любых  $u_1, \dots, u_T$  и  $d$

$$\begin{aligned} \prod_{t=1}^T (2^{m_t} - 1)(2^{m_t} - 2) &\leq C(3, d; u_1, \dots, u_T) \\ &\leq \prod_{t=1}^T ((2^{m_t} - 1)(2^{m_t} - 2) + 1). \end{aligned} \quad (25)$$

**Следствие 1.** При  $r \geq 3$  и любых  $u_1, \dots, u_T$  и  $d$

$$C(r, d; u_1, \dots, u_T) \leq \prod_{t=1}^T (2^{m_t} - 1)^{r-3} ((2^{m_t} - 1)(2^{m_t} - 2) + 1). \quad (26)$$

*Доказательство леммы 3.* При доказательстве можно считать, что  $d = 0$ , так как общий случай сводится к этому частному случаю заменой  $b^{it} = b^i + d$ ,  $i = 1, 2, 3$ .

Сначала рассмотрим случай  $T = 1$ , в котором уравнение (24) рассматривается над  $B = V^m \setminus \{u\}$ , где  $u \in V^m$ .

Пусть  $u = 0^m$ . Тогда решения уравнения (24) имеют вид  $(b^1, b^2, b^1 + b^2)$ , где  $b^1, b^2 \neq 0^m, b^1 \neq b^2$  (иначе  $b^3 = 0^m$ ). Таких комбинаций имеется ровно  $(2^m - 1)(2^m - 2)$  штук.

Пусть  $u \neq 0^m$ . Решениями являются

$$(0^m, 0^m, 0^m), \quad (0^m, b, b), \quad (b, 0^m, b), \quad (b, b, 0^m)$$

(где  $b \neq 0^m, u$ ) и наборы вида  $(b^1, b^2, b^1 + b^2)$ , где  $b^1, b^2 \neq 0^m, u$ , причем  $b^1 \neq b^2, b^2 + u$  (иначе  $b^3 = 0^m$  или  $b^3 = u$ ). Итого, получаем

$$1 + 3(2^m - 2) + (2^m - 2)(2^m - 4) = (2^m - 1)(2^m - 2) + 1$$

решений.

При  $T \geq 2$  число решений над  $B = B_1 \times \dots \times B_T, B_t = V^{m_t} \setminus \{u_t\}$ , равно произведению числа решений над  $B_t, t = 1, \dots, T$ . Отсюда получаем (25). Лемма 3 доказана.

**Замечание 4.** Пусть  $m_1, \dots, m_T$  и  $u_1, \dots, u_T$  таковы, что

$$\{m_t = 1\} \implies \{u_t = 1\}.$$

Тогда, согласно приведенным выше выкладкам,

$$C(3, d; u_1, \dots, u_T) \geq \prod_{t=1}^T ((2^{m_t} - 1)(2^{m_t} - 2) + I\{m_t = 1\}). \quad (27)$$

Если же  $m_t = 1, u_t = 0$  при некотором  $t$ , то

$$C(3, 0; u_1, \dots, u_T) = 0. \quad (28)$$

**Замечание 5.** Пусть среди уравнений системы (1) имеется уравнение

$$a_{t1}^1 x_1 + \dots + a_{tn}^1 x_n = 1.$$

Тогда из равенств (28), (20) и (21) следует формула

$$\mathbf{E}(\nu)_3 = \frac{(2^n - 2)(2^n - 4)}{(2^n - 1)^2} \Lambda^3.$$

*Доказательство следствия 1.* Фиксируем в уравнении (24) неизвестные  $b^4, \dots, b^r$ , что можно сделать не более, чем  $|B|^{r-3}$  способами. При этом получаем уравнение вида (24) с  $r = 3$ , число решений которого оценивается сверху с помощью правого неравенства в (25). Отсюда и из (12) получаем оценку (26). Следствие доказано.

**Лемма 4.** Пусть  $\text{rank}(x^1, \dots, x^r) = k$  и  $2 \leq k \leq r - 1$ . Тогда

$$|B(x^1, \dots, x^r)| \leq \prod_{t=1}^T (2^{m_t} - 1)^{k-2} \left( 1 - \frac{2^{m_t} - 2}{(2^{m_t} - 1)^2} \right). \quad (29)$$



Доказательство этой леммы аналогично доказательству леммы 4 из [1], и мы его опускаем.

Вернемся к неравенству (23). Подставив оценку (29) в (23) (для слагаемых с  $k < r$ ) и воспользовавшись равенством (21), очевидными оценками

$$|B(x^1, \dots, x^r)| < |B|^r,$$

$$|S_{r,k}| \leq C_r^k (2^k - 1)^{r-k} \prod_{s=0}^{k-1} (2^n - 2^s)$$

и равенством (12), после несложных преобразований получим (4). Теорема 1 доказана.

Докажем теорему 2. Заметим, что из условия (5) следует, что

$$\prod_{t=1}^T \left( 1 - \frac{2^{m_t} - 2}{(2^{m_t} - 1)^2} \right) \rightarrow 0.$$

Поэтому соотношение (6) следует из условия  $\Lambda \rightarrow \lambda$  и неравенств (3) и (4) теоремы 1. Из него, в свою очередь, следует сходимое распределение. Обе сходимости равномерны по наборам  $\{a_{ij}^i\}$ . Теорема 2 доказана.

Доказательство теоремы 3 аналогично доказательству теоремы 3 из [1], и мы его опускаем.

При доказательстве теоремы 4 рассмотрим два частных случая.

**Теорема 5.** Пусть система (1) не содержит линейных уравнений вида

$$a_{i1}^1 x_1 + \dots + a_{in}^1 x_n = 1. \tag{30}$$

Тогда если при  $n \rightarrow \infty$

$$\mathbf{E}(\nu)_r \rightarrow \lambda^r, \quad r = 1, 3, \quad 0 < \lambda < \infty, \tag{31}$$

то выполнено соотношение (5).

**Теорема 6.** Пусть система (1) содержит линейное уравнение вида (30). Тогда если при  $n \rightarrow \infty$

$$\mathbf{E}(\nu)_r \rightarrow \lambda^r, \quad r = 1, 4, \quad 0 < \lambda < \infty, \tag{32}$$

то выполнено соотношение (5).

Очевидно, что теорема 4 является прямым следствием теорем 5 и 6.

Докажем теорему 5. Из (20) и (21) следует равенство

$$\mathbf{E}(\nu)_3 = M_{3,2} + \frac{(2^n - 2)(2^n - 4)}{(2^n - 1)^2} \Lambda^3, \tag{33}$$

где

$$M_{3,2} = \sum_{(x^1, x^2, x^3) \in S_{3,2}} \sum_{b^1, b^2, b^3 \in B} \mathbf{E} \eta_{x^1, b^1} \eta_{x^2, b^2} \eta_{x^3, b^3}. \tag{34}$$

Заметим, что

$$S_{3,2} = \{(x^1, x^2, x^3) \in (V^n \setminus \{0^n\})^3 : x^i \neq x^j \ (i \neq j), \ x^1 + x^2 + x^3 = 0\}.$$

Определим множество

$$B_{3,2} = \{(b^1, b^2, b^3) \in B^3 : b^1 + b^2 + b^3 = 0\}.$$

Согласно второму утверждению леммы 1 суммирование по  $B$  в выражении (34) для  $M_{3,2}$  можно заменить на суммирование по множеству  $B_{3,2}$ . Поэтому в силу первого утверждения леммы 1 из (34) получаем равенство

$$M_{3,2} = \frac{1}{2^{2M}} |S_{3,2}| |B_{3,2}|. \quad (35)$$

Заметим, что множество  $B_{3,2}$  совпадает с множеством решений, изученным в лемме 3, и для него в силу предположений теоремы справедлива оценка (27). Используя в (35) оценку (27), равенства (2) и

$$|S_{3,2}| = (2^n - 1)(2^n - 2),$$

получаем соотношения

$$\begin{aligned} M_{3,2} &\geq \frac{(2^n - 1)(2^n - 2)}{2^{2M}} \prod_{t=1}^T ((2^{m_t} - 1)(2^{m_t} - 2) + I\{m_t = 1\}) \\ &= \frac{2^n - 2}{2^n - 1} \Lambda^2 \prod_{t=1}^T \left( 1 - \frac{2^{m_t} - 1 - I\{m_t = 1\}}{(2^{m_t} - 1)^2} \right) \\ &\geq \frac{2^n - 2}{2^n - 1} \Lambda^2 \prod_{t=1}^T \left( 1 - \frac{3}{2} \frac{2^{m_t} - 2}{(2^{m_t} - 1)^2} \right). \end{aligned} \quad (36)$$

В силу (31), (33) и (36) при  $n \rightarrow \infty$

$$\prod_{t=1}^T \left( 1 - \frac{3}{2} \frac{2^{m_t} - 2}{(2^{m_t} - 1)^2} \right) \rightarrow 0.$$

Последнее эквивалентно соотношению (5). Теорема 5 доказана.

Докажем теорему 6. Так как

$$S_{4,0} = S_{4,1} = S_{4,2} = \emptyset,$$

из (20) и (21) следует равенство

$$\mathbf{E}(\nu)_4 = M_{4,3} + \frac{(2^n - 2)(2^n - 4)(2^n - 8)}{(2^n - 1)^3} \Lambda^4, \quad (37)$$

где

$$M_{4,3} = \sum_{(x^1, x^2, x^3, x^4) \in S_{4,3}} \sum_{b^1, b^2, b^3, b^4 \in B} \mathbf{E} \eta_{x^1, b^1} \eta_{x^2, b^2} \eta_{x^3, b^3} \eta_{x^4, b^4}. \quad (38)$$

Пусть

$$S_{4,3}^{(0)} = \{(x^1, x^2, x^3, x^4) \in S_{4,3}: x^1 + x^2 + x^3 + x^4 = 0^n\},$$

$$S_{4,3}^{(1)} = \{(x^1, x^2, x^3, x^4) \in S_{4,3}: x^2 + x^3 + x^4 = 0^n\},$$

а  $S_{4,3}^{(2)}$ ,  $S_{4,3}^{(3)}$  и  $S_{4,3}^{(4)}$  определяются аналогично  $S_{4,3}^{(1)}$  с заменой  $x^1$  на  $x^2$ ,  $x^3$  и  $x^4$  соответственно. Тогда, как нетрудно проверить,  $S_{4,3}$  является объединением непересекающихся множеств  $S_{4,3}^{(i)}$ ,  $i = 0, \dots, 4$ .

Определим также множества

$$B_{4,3}^{(0)} = \{(b^1, b^2, b^3, b^4) \in B^4: b^1 + b^2 + b^3 + b^4 = 0^M\},$$

$$B_{4,3}^{(1)} = \{(b^1, b^2, b^3, b^4) \in B^4: b^2 + b^3 + b^4 = 0^M\},$$

а  $B_{4,3}^{(2)}$ ,  $B_{4,3}^{(3)}$  и  $B_{4,3}^{(4)}$  определим аналогично  $B_{4,3}^{(1)}$  с заменой  $b^1$  на  $b^2$ ,  $b^3$  и  $b^4$  соответственно. Заметим, что при наличии в системе (1) уравнения вида (30) множества  $B_{4,3}^{(i)}$ ,  $i = 1, 2, 3, 4$ , пусты. Поэтому используя (38) и лемму 1, получаем равенства

$$\begin{aligned} M_{4,3} &= \sum_{(x^1, x^2, x^3, x^4) \in S_{4,3}^{(0)}} \sum_{(b^1, b^2, b^3, b^4) \in B_{4,3}^{(0)}} \mathbf{E} \prod_{s=1}^4 \eta_{x^s, b^s} \\ &= \frac{1}{2^{3M}} |S_{4,3}^{(0)}| |B_{4,3}^{(0)}|. \end{aligned} \quad (39)$$

**Лемма 5.** При любом наборе  $m_1, \dots, m_T$  выполнено равенство

$$|B_{4,3}^{(0)}| = \prod_{t=1}^T ((2^{m_t} - 1)^3 - (2^{m_t} - 1)(2^{m_t} - 2)). \quad (40)$$

*Доказательство.* Доказательство леммы 5 проводится по той же схеме, что и доказательство леммы 3. Только теперь речь идет о числе решений в  $B^4$  уравнения

$$b^1 + b^2 + b^3 + b^4 = 0^M. \quad (41)$$

Сначала рассмотрим случай, в котором уравнение (41) рассматривается над  $B = V^m \setminus \{u\}$ , где  $u \in V^m$  (под  $m$  и  $u$  подразумеваются  $m_t$  и  $a_t + 1^{m_t}$  соответственно).

Пусть  $u = 0^m$ . Тогда решения уравнения (41) можно разбить на две группы. Решения из первой группы имеют вид  $(b^1, b^2, b^3, b^4)$ , где

$$b^1 = b^2 \neq 0^m; \quad b^3 = b^4 \neq 0^m.$$

Таких комбинаций имеется ровно  $(2^m - 1)^2$  штук.

Решения из второй группы имеют вид  $(b^1, b^2, b^3, b^4)$ , где

$$b^1 \neq 0^m; \quad b^2 \neq 0^m, b^1; \quad b^3 \neq 0^m, b^1 + b^2; \quad b^4 = b^1 + b^2 + b^3.$$

Таких комбинаций имеется ровно  $(2^m - 1)(2^m - 2)^2$  штук.

Всего получаем

$$(2^m - 1)^2 + (2^m - 1)(2^m - 2)^2 = (2^m - 1)^3 - (2^m - 1)(2^m - 2)$$

решений.

Пусть  $u \neq 0^m$ . Тогда решения уравнения (41) можно разбить на три группы. Решения из первой группы имеют вид  $(b^1, b^2, b^3, b^4)$ , где

$$b^1 = b^2 \neq u; \quad b^3 = b^4 \neq u.$$

Таких комбинаций имеется ровно  $(2^m - 1)^2$  штук.

Решения из второй группы имеют вид  $(b^1, b^2, b^3, b^4)$ , где

$$b^1 = 0^m; \quad b^2 \neq u, 0^m; \quad b^3 \neq u, b^2 + u; \quad b^4 = b^2 + b^3.$$

Таких комбинаций имеется ровно  $(2^m - 2)^2$  штук.

Решения из третьей группы имеют вид  $(b^1, b^2, b^3, b^4)$ , где

$$b^1 \neq u, 0^m; \quad b^2 \neq u, b^1; \quad b^3 \neq u, b^1 + b^2 + u; \quad b^4 = b^1 + b^2 + b^3.$$

Таких комбинаций имеется ровно  $(2^m - 2)^3$  штук.

Получаем такое же, как и при  $u = 0^m$ , суммарное число решений:

$$(2^m - 1)^2 + (2^m - 2)^2 + (2^m - 2)^3 = (2^m - 1)^3 - (2^m - 1)(2^m - 2).$$

При  $T \geq 2$  число решений над

$$B = B_1 \times \dots \times B_T, \quad B_t = V^{m_t} \setminus \{u_t\}, \quad u_t = a_t + 1^{m_t},$$

равно произведению числа решений над  $B_t$ ,  $t = 1, \dots, T$ . Отсюда получаем (40) в общем случае. Лемма 5 доказана.

Используя (39), (40), (2) и легко проверяемое равенство

$$|S_{4,3}^{(0)}| = (2^n - 1)(2^n - 2)(2^n - 4),$$

получаем, что

$$M_{4,3} = \frac{(2^n - 2)(2^n - 4)}{(2^n - 1)^2} \Lambda^3 \prod_{t=1}^T \left( 1 - \frac{2^{m_t} - 2}{(2^{m_t} - 1)^2} \right). \quad (42)$$

Из (32), (37) и (42) вытекает соотношение (5). Теорема 6 доказана.

## Список литературы

1. Михайлов В.Г., Предельные теоремы для числа ненулевых решений одной системы случайных уравнений над полем  $GF(2)$ . *Теория вероятностей и ее применения* (1998) **43**, №3, 598–606.
2. Коваленко И.Н., Левитская А.А., Савчук М.Н., *Избранные задачи вероятностной комбинаторики*. Наукова Думка, Киев, 1986.
3. Колчин В.Ф., *Системы случайных уравнений*. МИЭМ, Москва, 1988.
4. Балакин Г.В., Введение в теорию случайных систем уравнений. *Труды по дискретной математике* (1997) **1**, 1–18.

5. Балакин Г.В., Системы случайных систем уравнений над конечным полем. *Труды по дискретной математике* (1998) **2**, 21–37.
6. Севастьянов Б.А., Чистяков В.П., О числе входных последовательностей, соответствующих выходной последовательности конечного автомата. *Обзор прикладной и промышленной математики* (1994) **1**, №1, 96–107.
7. Сачков В.Н., Асимптотическое поведение числа  $t$ -минимальных покрытий. *Дискретная математика* (1993) **5**, №1, 36–44.
8. Копытцев В.А., О распределении числа решений случайных заведомо совместных систем уравнений. *Теория вероятностей и ее применения* (1995) **40**, №2, 430–437.
9. Михайлов В.Г., Предельные теоремы для случайного покрытия конечного множества и для числа решений системы случайных уравнений. *Теория вероятностей и ее применения* (1996) **41**, №2, 272–283.
10. Копытцев В.А., О некоторых случайных заведомо совместных системах уравнений. *Обзор прикладной и промышленной математики* (1994) **1**, №1, 56–84.
11. Полин С.В., О случайных блужданиях на графе с отмеченным ребром. *Обзор прикладной и промышленной математики* (1994) **1**, №1, 85–92.
12. Михайлов В.Г., Асимптотическая нормальность логарифма числа пробразов выходной последовательности конечного автомата. *Обзор прикладной и промышленной математики* (1994) **1**, №1, 126–135.
13. Масол В.И., Теорема о предельном распределении числа ложных решений системы нелинейных случайных булевых уравнений. *Теория вероятностей и ее применения* (1998) **43**, №1, 41–56.

Статья поступила 24.12.1999.