Math-Net.Ru

Общероссийский математический портал

В. Г. Михайлов, Предельные теоремы для числа решений системы случайных линейных уравнений, попавших в заданное множество, *Дискрет. матем.*, 2007, том 19, выпуск 1, 17–26

DOI: <https://doi.org/10.4213/dm4>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 18.209.158.208

26 апреля 2023 г., 17:11:12

Предельные теоремы для числа решений системы случайных линейных уравнений, попавших в заданное множество

© 2007 г. В. Г. Михайлов

Исследуется асимптотическое поведение распределения числа $\xi(B)$ таких решений системы однородных случайных линейных уравнений $Ax = 0$ (матрица A размера $T \times n$ составлена из независимых случайных величин $a_{i,j}$, распределенных равномерно на множестве элементов конечного поля K), которые принадлежат некоторому заданному множеству B ненулевых n -мерных векторов над полем K . Рассмотрена ситуация, когда при согласованном росте параметров $n, T \rightarrow \infty$ и изменении множеств $B_1, \dots, B_s$, обеспечивающем сходимость средних значений к конечным пределам, в качестве предельного распределения для вектора $(\xi(B_1), \dots, \xi(B_s))$ выступает s -мерное сложное пуассоновское распределение. Найдены достаточные условия этой сходимости и параметры предельного распределения. Подробно рассмотрен частный случай, когда B_k — множество векторов, в записи которых отсутствует элемент $k \in K$.

Работа выполнена при поддержке программой РАН “Современные проблемы теоретической математики”, Российского фонда фундаментальных исследований, проекты 02-01-00266 и 05-01-00035, и программой Президента Российской Федерации поддержки ведущих научных школ, грант НШ 1758.2003.1.

1. Введение

Рассмотрим систему из T случайных линейных уравнений относительно n неизвестных над некоторым конечным полем K . Для краткости запишем ее в матричном виде $Ax = b$. Здесь считается, что матрица A распределена на множестве матриц соответствующего размера равномерно или асимптотически равномерно (при увеличении ее размеров), а b — детерминированный вектор. Пусть B — некоторое множество ненулевых n -мерных векторов, $\xi(B)$ — число решений системы, принадлежащих этому множеству. Оказывается, что довольно часто в качестве предельных (при увеличении числа уравнений, числа неизвестных и подходящем изменении множества B) для величины $\xi(B)$ выступают пуассоновское и сложное пуассоновское распределения. Простейшим примером является число решений $x = (x_1, \dots, x_n)$ системы $Ax = b$ над полем $GF(2)$ с равномерно распределенной матрицей A , имеющих в своей записи лишь одну единицу. Эта случайная величина представима как сумма независимых случайных индикаторов, в которой i -е слагаемое отвечает решению с единицей на i -м месте. Условия предельной теоремы Пуассона для такой суммы хорошо известны, и нетрудно описать правила изменения параметров T и n , при которых она имеет место.

Исследование таких асимптотических свойств числа решений системы $Ax = b$ с относительно малым (по сравнению с n) числом ненулевых элементов было проведено В. А. Копытцевым. Пусть $B(r)$ — множество всех n -мерных векторов с r ненулевыми элементами. В. А. Копытцев, в частности, показал, что для случайной системы $Ax = b$ над полем $GF(2)$ при согласованном увеличении числа уравнений T , числа неизвестных n и таком изменении числа r , что $r/n \rightarrow 0$ и $\mathbf{E}\xi(B(r)) \rightarrow \lambda$, распределение случайной величины $\xi(B(r))$ сходится к закону Пуассона с параметром λ . При этом предполагалось, что матрица A распределена на множестве матриц соответствующего размера асимптотически равномерно (подробности см. в [1]).

В 2004 году В. А. Копытцев распространил этот результат на системы над произвольным конечным полем с оговоркой, что $b \neq 0$ (см. [2]). В качестве множества B в этой работе рассматривались не только множества $B(r)$, но и широкий класс их подмножеств. Оговорка о том, что $b \neq 0$, здесь совсем не случайна. При $K \neq GF(2)$ однородная система $Ax = 0$ обладает коллинеарными решениями, а коллинеарные решения имеют одинаковое число ненулевых элементов. По этой причине вместо пуассоновского распределения в качестве предельного в ряде случаев выступает сложное пуассоновское распределение.

В настоящей работе рассматривается система случайных однородных линейных уравнений $Ax = 0$ с равномерно распределенной матрицей A . Найдены условия на множество B (точнее, на последовательность множеств, поскольку B меняется при изменении числа неизвестных) и условия на характер изменения остальных параметров схемы, при которых распределение случайной величины $\xi(B)$ сходится к сложному пуассоновскому распределению.

Пусть V^r обозначает r -мерное линейное пространство над полем K , матрица A размера $T \times n$ состоит из независимых случайных величин $a_{i,j}$, распределенных равномерно на множестве элементов конечного поля K , $x \in V^n$, $b \in V^T$, $n > T$. Пусть заданы некоторые подмножества $B_1, \dots, B_s \subseteq V^n$, не содержащие нуля этого пространства, и пусть $\xi(B_k)$ — число решений системы $Ax = 0$, принадлежащих множеству B_k , $k = 1, \dots, s$. Мы изучаем предельное поведение распределения случайного вектора $(\xi(B_1), \dots, \xi(B_s))$ при $T, n \rightarrow \infty$ и таком изменении множеств B_i , когда математические ожидания величин $\xi(B_i)$ стремятся к конечным пределам. Считается, что при этом предельном переходе поле K остается неизменным, а множества $B_1, \dots, B_s$ существенно отличаются от линейных подпространств (подробнее об этом ниже).

Чтобы сформулировать результаты, нам понадобится ряд вспомогательных определений. Рассмотрим отношение эквивалентности на множестве $V^n \setminus \{0^n\}$ ненулевых точек (векторов) n -мерного линейного пространства, задаваемое свойством коллинеарности векторов. Классами эквивалентности этого отношения являются прямые, проходящие через нулевую точку, из которых эта точка исключена. Занумеруем эти классы в некотором порядке от 1 до $N_n = (|K|^n - 1)/(|K| - 1)$, $q = |K|$ (здесь и далее запись $|M|$ обозначает число элементов множества M), и условимся обозначать их через $E_{n,1}, \dots, E_{n,N_n}$.

Пусть $R(s)$ — множество s -мерных векторов $\bar{r} = (r_1, \dots, r_s)$ из неотрицательных целых чисел, удовлетворяющих условиям

$$1 \leq r_1 + \dots + r_s \leq (|K| - 1)s.$$

Для каждого n определим множества

$$F_n(\bar{r}) = \{k: |E_{n,k} \cap B_i| = r_i, i = 1, \dots, s\}$$

и величины

$$\Lambda_{\bar{r}} = |F_n(\bar{r})| |K|^{-T}, \quad \bar{r} \in R(s).$$

Заметим, что множество $F_n(\bar{r})$ состоит из номеров тех классов эквивалентности, которые имеют в B_i ровно по r_i точек, $i = 1, \dots, s$.

Определим величину $N(a_1, a_2, a_3, d, B)$ как число решений уравнения

$$a_1 u^1 \oplus a_2 u^2 \oplus a_3 u^3 = d \quad (1)$$

над полем K относительно тройки векторов (u^1, u^2, u^3) , $u^1, u^2, u^3 \in B$. Здесь коэффициенты $a_1, a_2, a_3 \in K \setminus \{0\}$, $d \in V^n$. Символ $\oplus$ (и символ $\ominus$) используется как для обозначения операции сложения (вычитания) в поле K , так и для обозначения операции сложения (вычитания) векторов в линейных пространствах над полем K . Пусть

$$N(B) = \max_{a_1, a_2, a_3, d} N(a_1, a_2, a_3, d, B). \quad (2)$$

Очевидно, что

$$N(B) \leq |B|^2.$$

Через $\pi_i(\lambda_i)$ (здесь в качестве индекса i может выступать элемент любого конечного множества) условимся обозначать независимые в совокупности случайные величины, распределенные по закону Пуассона с указанными в скобках значениями параметра.

Будем считать, что параметры $n = n(m)$ и $T = T(m)$ зависят от некоторого целочисленного параметра m , предельный переход осуществляется при $m \rightarrow \infty$. Разумеется, при этом от m зависят и множества $B_1 = B_1(m), \dots, B_s = B_s(m)$.

Теорема 1. Пусть $m \rightarrow \infty$, причем $n - T \rightarrow \infty$, а множества $B_1, \dots, B_s$ меняются так, что

$$\Lambda(\bar{r}) \rightarrow \lambda(\bar{r}), \quad 0 \leq \lambda(\bar{r}) < \infty, \quad \bar{r} \in R(s), \quad (3)$$

и для множества $B = \bigcup_i B_i$ выполнено условие

$$N(B)|B|^{-2} \rightarrow 0. \quad (4)$$

Тогда распределение случайного вектора $(\xi(B_1), \dots, \xi(B_s))$ сходится к распределению случайного вектора

$$\left(\sum_{\bar{r} \in R(s)} r_1 \pi_{\bar{r}}(\lambda(\bar{r})), \dots, \sum_{\bar{r} \in R(s)} r_s \pi_{\bar{r}}(\lambda(\bar{r})) \right). \quad (5)$$

Замечание 1. Наиболее важным в теореме является условие (4). Ниже будет показано, что для множеств B , которые являются классами смежности какой-либо подгруппы по сложению в V^n , и только для них выполнено равенство $N(B) = |B|^2$. Так будет, например, если множество B является множеством решений некоторой неоднородной системы уравнений. В этом случае исходная система уравнений может быть дополнена уравнениями, определяющими это множество. Тогда величина $\xi(B)$ будет числом всех решений этой расширенной системы. Ее распределение сосредоточено на множестве $\{0, 1, |K|, |K|^2, \dots\}$. Значит, предельное распределение величины $\xi(B)$ в этом случае не может быть пуассоновским. Условие (4) гарантирует, что множества $B_1, \dots, B_s$ в пределе принципиально отличаются от множеств “линейного типа”, для которых $N(B) = |B|^2$.

Замечание 2. Если дополнительно к условиям теоремы выполнены неравенства

$$\sum_{\bar{r} \in R(s)} r_i \lambda(\bar{r}) > 0, \quad i = 1, \dots, s, \quad (6)$$

то предельное распределение каждой компоненты вектора $(\xi(B_1), \dots, \xi(B_s))$ невырождено. При этом распределение всего вектора в пределе может быть сосредоточенным на пространстве меньшей размерности. Например, если при некоторых $i < j$

$$\lambda(\bar{r}) \equiv 0, \quad \text{если} \quad r_i \neq r_j, \quad (7)$$

то из (5) вытекает, что $\mathbf{P}\{\xi(B_i) = \xi(B_j)\} \rightarrow 1$ при $m \rightarrow \infty$.

Пусть множества I и J образуют разбиение множества $\{1, \dots, s\}$:

$$I, J \neq \emptyset, \quad I \cap J = \emptyset, \quad I \cup J = \{1, \dots, s\}.$$

Положим

$$R(I, J) = \left\{ \bar{r} \in R(s) : \sum_{i \in I} r_i > 0, \sum_{j \in J} r_j > 0 \right\}.$$

Следствие 1. Пусть выполнены условия теоремы 1 и, кроме того, для некоторых $i \in I$ и $j \in J$ выполнено условие (6). Тогда соотношение

$$\Lambda(\bar{r}) \rightarrow 0 \quad \text{для всех} \quad \bar{r} \in R(I, J) \quad (8)$$

является необходимым и достаточным для асимптотической независимости случайных векторов $(\xi(B_\alpha), \alpha \in I)$ и $(\xi(B_\alpha), \alpha \in J)$.

Это утверждение вытекает непосредственно из теоремы 1.

Выделим один интересный частный случай. Множество B назовем r -слоиным, если каждая (проходящая через нуль) прямая, пересекающая множество B , имеет с ним ровно r общих точек. При $K = GF(2)$ любое множество B , не содержащее нулевой точки, является однослойным.

Следствие 2. Пусть при $m \rightarrow \infty$ разность $n - T$ стремится к бесконечности, множество B является r -слоиным, причем оно меняется так, что $|K|^{-T}|B| \rightarrow \lambda$, $0 < \lambda < \infty$, и для B выполнено условие (4). Тогда распределение случайной величины $r^{-1}\xi(B)$ сходится к распределению Пуассона с параметром $r^{-1}\lambda$.

В частности, для однослойного множества B распределение случайной величины $\xi(B)$ сходится к пуассоновскому распределению.

Теорема 1 представляет собой интерпретацию аналогичного утверждения для числа точек случайного линейного пространства, попавших в заданные множества. Последнее было получено в работе [3]. Несложный вывод теоремы 1 из результатов работы [3] приведен в следующем разделе статьи.

Отметим, что сама задача о числе ненулевых векторов в пересечении $L \cap B$ случайного линейного пространства L с заданным множеством B в свою очередь решается путем сведения ее к аналогичной задаче для числа решений соотношения (случайного линейного включения) $Ax \in B$, где $x \in V^n$, $B \subseteq V^T$, а A — случайная $T \times n$ матрица, составленная из

независимых случайных величин, распределенных равномерно на множестве элементов поля K . Подробности см. в [3–5].

Теперь перейдем к примерам. Рассмотрим задачу о числе решений системы однородных случайных уравнений $Ax = 0$, в которых отсутствует заданный элемент поля. Положим

$$B_k = \{x = (x_1, \dots, x_n) \in V^n \setminus \{0^n\} : x_1, \dots, x_n \neq k\}, \quad k \in K,$$

и рассмотрим случайную величину $\xi_k = \xi(B_k)$, равную числу тех решений системы $Ax = 0$, в которых нет знака k , $k \in K$.

Теорема 2. Пусть $K \neq GF(2)$ и при $m \rightarrow \infty$ выполнены соотношения $n - T \rightarrow \infty$ и

$$(|K| - 1)^n |K|^{-T} \rightarrow \lambda < 0. \quad (9)$$

Тогда при $m \rightarrow \infty$

- (а) $\mathbf{P}\{\xi_k = \xi_l\} \rightarrow 1$ для любых $k, l \in K \setminus \{0\}$,
- (б) случайная величина ξ_0 и вектор $(\xi_k, k \in K \setminus \{0\})$ асимптотически независимы,
- (в) распределение случайной величины $(|K| - 1)^{-1} \xi_0$ сходится к распределению Пуассона с параметром $(|K| - 1)^{-1} \lambda$,
- (г) при $k \in K \setminus \{0\}$ распределение случайной величины ξ_k сходится к распределению Пуассона с параметром λ .

Рассмотрим множества H , $0 \in H \subseteq K$, и

$$B = \bigcup_{k \in H} B_k.$$

Непосредственно из теоремы 2 вытекает следующее утверждение.

Следствие 3. Пусть выполнены условия теоремы 2. Тогда распределение случайной величины $\xi(B)$ сходится к сложному пуассоновскому распределению, отвечающему случайной величине

$$(|K| - 1)\pi_0 + (|H| - 1)\pi_1,$$

где π_0 и π_1 — независимые случайные величины, распределенные по закону Пуассона с параметрами $(|K| - 1)^{-1} \lambda$ и λ соответственно.

При $H = K$ из следствия 3 выводится следующее утверждение. Пусть ξ — число решений системы случайных однородных уравнений $Ax = 0$, содержащих не все элементы поля K .

Следствие 4. Пусть выполнены условия теоремы 2. Тогда распределение случайной величины $(|K| - 1)^{-1} \xi$ сходится к пуассоновскому распределению с параметром $(|K| - 1)^{-1} |K| \lambda$.

Утверждение, аналогичное теореме 2 может быть доказано и для случайных величин $\xi_{k,l} = \xi(B_{k,l})$, где

$$B_{k,l} = \{x = (x_1, \dots, x_n) \in V^n \setminus \{0^n\} : x_1, \dots, x_n \neq k, l\}, \quad k, l \in K, \quad k \neq l,$$

Величина $\xi_{k,l} = \xi(B_{k,l})$ равна числу тех решений однородной системы, в которых нет знаков k и l , $k, l \in K$. Чтобы избежать громоздких формулировок, мы приведем утверждение лишь для одномерных распределений.

Теорема 3. Пусть $K \neq GF(2)$, $K \neq GF(3)$ и при $t \rightarrow \infty$ выполнены соотношения $n - T \rightarrow \infty$ и

$$(|K| - 2)^n |K|^{-T} \rightarrow \lambda < 0. \quad (10)$$

Тогда при $t \rightarrow \infty$

- (а) при $k \in K \setminus \{0\}$ распределение случайной величины $\xi_{k,-k}/2$ сходится к распределению Пуассона с параметром $\lambda/2$,
- (б) при $l \notin \{k, -k\}$, $k \in K \setminus \{0\}$ распределение случайной величины $\xi_{k,l}$ сходится к распределению Пуассона с параметром λ .

Замечание 3. При $r/n \rightarrow 0$ условие (4) выполнено для множества $B(r)$ всех n -мерных векторов, имеющих ровно по r ненулевых элементов. Впрочем, проверка этого свойства весьма громоздка, и мы ее не приводим. Благодаря этому свойству из следствия 2 вытекает, что при выполнении условий

$$n, T \rightarrow \infty, \quad r/n \rightarrow 0, \quad \mathbf{E}\xi(B(r)) \rightarrow \lambda, \quad 0 < \lambda < \infty,$$

распределение случайной величины $(|K| - 1)^{-1}\xi(B(r))$ сходится к распределению Пуассона с параметром $(|K| - 1)^{-1}\lambda$.

2. Доказательство теоремы 1

Обозначим через $S(A)$ множество решений системы $Ax = 0$. Тогда

$$\xi(B_i) = |S(A) \cap B_i|. \quad (11)$$

Из теорем линейной алгебры вытекает, что множество $S(A)$ является линейным подпространством пространства V^n . При этом, если матрица A имеет ранг T , то размерность подпространства $S(A)$ равна $n - T$. Последний случай является основным при $n - T \rightarrow \infty$.

Рассмотрим пространство L , выбранное случайно и равновероятно из множества всех $(n - T)$ -мерных линейных подпространств пространства V^n . Рассмотрим случайные величины $\mu(B_i) = |L \cap B_i|$ (число точек в пересечениях $L \cap B_i$ при одном и том же случайно выбранном подпространстве L). Предельное поведение распределения вектора $(\mu(B_1), \dots, \mu(B_s))$ при согласованном изменении параметров, описанном в теореме 1, исследовалось в [3]. Приведем для удобства ссылок основной результат этой статьи.

Теорема 4. Пусть при $t \rightarrow \infty$ параметры n и T стремятся к бесконечности, а множества $B_1, \dots, B_s \subseteq V^n$ меняются так, что выполнены условия (3), (6) и (4). Тогда распределение случайного вектора $(\mu(B_1), \dots, \mu(B_s))$ сходится к распределению случайного вектора (5).

Воспользуемся теоремой 4 для вывода теоремы 1. Введем независимое от $S(A)$ линейное пространство L' , распределенное равномерно на множестве всех $(n - T)$ -мерных линейных подпространств пространства V^n . Определим $(n - T)$ -мерное линейное пространство $L(A)$ формулами

$$L(A) = \begin{cases} S(A), & \text{если } \text{rank}(A) = T, \\ L', & \text{если } \text{rank}(A) < T. \end{cases} \quad (12)$$

Так как распределение матрицы A инвариантно относительно невырожденных линейных преобразований пространства V^n , порожденных перестановками и сложением столбцов, а также умножением их на элементы поля, то условное распределение пространств $S(A)$ и $L(A)$ при условии $\text{rank}(A) = T$ является равномерным на множестве всех $(n - T)$ -мерных линейных подпространств пространства V^n . Таким же по определению L' является распределение пространства $L(A)$ при условии $\text{rank}(A) < T$. Значит, пространство $L(A)$ распределено на указанном множестве равномерно.

Доказанное свойство позволяет задать случайные величины $\mu(B_i)$ формулами

$$\mu(B_i) = |L(A) \cap B_i|. \quad (13)$$

Формулы (11)–(13) задают величины $\xi(B_i)$ и $\mu(B_i)$ на одном вероятностном пространстве. Из них следует, что

$$\mathbf{P}\{(\xi(B_1), \dots, \xi(B_s)) \neq (\mu(B_1), \dots, \mu(B_s))\} \leq \mathbf{P}\{S(A) \neq L(A)\} \leq \mathbf{P}\{\text{rank}(A) < T\}.$$

По условиям теоремы 1 имеет место соотношение $n - T \rightarrow \infty$. Поэтому, как нетрудно проверить, $\mathbf{P}\{\text{rank}(A) < T\} \rightarrow 0$. Значит, предельные распределения случайных векторов $(\xi(B_1), \dots, \xi(B_s))$ и $(\mu(B_1), \dots, \mu(B_s))$ совпадают.

Осталось заметить, что из условий теоремы 1 вытекают все условия теоремы 4 (в том числе и соотношения $n, T \rightarrow \infty$), и воспользоваться теоремой 4. Теорема 1 доказана.

3. Доказательство теорем 2 и 3

В доказательствах мы воспользуемся теоремой 1. Поэтому все сводится к проверке условий этой теоремы в рассматриваемых случаях. Для проверки условия (4) понадобится следующее утверждение.

Лемма 1. Пусть для некоторого множества $B \subset V^n$ выполнено равенство $N(B) = |B|^2$. Тогда множество B является подгруппой или классом смежности какой-либо подгруппы по сложению векторов пространства V^n .

Замечание 4. Доказательство леммы мы заимствуем из работы [6]. Там оно является частью доказательства леммы 1 о значениях некоторых вспомогательных характеристик. Это неудобно для цитирования. Поэтому мы приводим здесь как формулировку, так и доказательство необходимого для нас утверждения.

Доказательство леммы 1. Пусть $0 \in B$. При определении величины $N(B)$ можно считать, что коэффициент a_1 в уравнении (1) равен единице. Рассмотрим уравнение

$$u^1 \oplus a_2 u^2 \oplus a_3 u^3 = d$$

относительно тройки векторов $u^1, u^2, u^3 \in B$ и предположим, что число его решений равно $|B|^2$. В этом случае для любых $u^1, u^2 \in B$ найдется такой элемент $u^3 \in B$, при котором $u^1 \oplus a_2 u^2 = d \ominus a_3 u^3$ (используем запись $z = x \ominus y$, если $x = z \oplus y$). Это означает, что

$$\{B \oplus a_2 B\} = \{y \oplus a_2 z : y, z \in B\} \subseteq \{d \ominus a_3 B\}.$$

Поэтому

$$|\{B \oplus a_2 B\}| \leq |\{d \ominus a_3 B\}| = |B|.$$

Так как $0 \in B$, то $B \in \{B \oplus a_2 B\}$. Следовательно,

$$|\{B \oplus a_2 B\}| = |B|, \quad \{B \oplus a_2 B\} = B.$$

Аналогичными рассуждениями доказывается, что $\{B \oplus a_2 B\} = a_2 B$. Значит, $a_2 B = B$ и $\{B \oplus B\} = \{B \oplus a_2 B\} = B$. Таким образом, множество B замкнуто относительно сложения.

Из равенства $\{B \oplus B\} = B$ и условия $0 \in B$ следует, что вместе с любым элементом в множестве B содержится и обратный по сложению элемент. Все сказанное выше означает, что множество B является группой по сложению $\oplus$.

Пусть теперь $0 \notin B$. Выберем некоторый элемент $b \in B$ и рассмотрим множество $B' = \{B \ominus b\}$. Уравнение 1 эквивалентно уравнению

$$a_1 u^1 \oplus a_2 u^2 \oplus a_3 u^3 = d \oplus b(a_1 \oplus a_2 \oplus a_3)$$

относительно неизвестных $u^1, u^2, u^3 \in B'$. Так как $0 \in B'$, предыдущие рассуждения показывают, что множество B' является группой относительно операции $\oplus$, а множество B является классом смежности этой группы. Лемма доказана.

Доказательство теоремы 2. Начнем с проверки условия (4) для множества $B = \bigcup_k B_k$. Покажем сначала, что при $m \rightarrow \infty$

$$N(B_k) = o(|B_k|^2), \quad (14)$$

Из определения множеств B_k вытекает, что

$$N(B_k) \leq (N(K \setminus \{k\}))^n,$$

где

$$N(K \setminus \{k\}) = \max_{a_1, a_2, a_3, d} N(a_1, a_2, a_3, d, K \setminus \{k\}).$$

Здесь $N(a_1, a_2, a_3, d, K \setminus \{k\})$ — число решений уравнения 1 относительно тройки величин $u^1, u^2, u^3 \in K \setminus \{k\}$. В рассматриваемом случае $d \in K$. Множество $K \setminus \{k\}$ не является ни подгруппой, ни классом смежности какой-либо подгруппы в K . Поэтому, согласно лемме 1,

$$N(K \setminus \{k\}) \leq |K \setminus \{k\}|^2 - 1 = (|K| - 1)^2 - 1.$$

Значит, при $m \rightarrow \infty$

$$\frac{N(B_k)}{(|B_k| + 1)^2} \leq \left(\frac{N(K \setminus \{k\})}{(|K| - 1)^2} \right)^n \leq \left(\frac{(|K| - 1)^2 - 1}{(|K| - 1)^2} \right)^n \rightarrow 0.$$

Отсюда следует соотношение (14).

Обозначим через $N(a_1, a_2, a_3, d, B_i, B_j, B_k)$ число решений уравнения (1) относительно тройки u^1, u^2, u^3 , $u^1 \in B_i$, $u^2 \in B_j$, $u^3 \in B_k$. Воспользуемся тем, что любое такое решение переводится заменой

$$u^1 = v^1 + i, \quad u^2 = v^2 + j, \quad u^3 = v^3 + k$$

в решение уравнения

$$a_1 v^1 \oplus a_2 v^2 \oplus a_3 v^3 = d'$$

где $d' = d \ominus a_1 i \ominus a_2 j \ominus a_3 k$, относительно тройки $v^1, v^2, v^3 \in B_0$. Справедливо и обратное. Поэтому

$$N(a_1, a_2, a_3, d, B_i, B_j, B_k) \leq N(a_1, a_2, a_3, d', B_0, B_0, B_0) \leq N(B_0).$$

Воспользуемся этой оценкой следующим образом:

$$N(B) \leq \sum_{i \in K} \sum_{j \in K} \sum_{k \in K} \sup_{a_1, a_2, a_3, d} N(a_1, a_2, a_3, d, B_i, B_j, B_k) \leq |K|^3 N(B_0).$$

Кроме того, $|B| > |B_0|$. Значит, соотношение (4) вытекает из (14).

Докажем утверждение (а). Введем множества

$$B'_k = \{x = (x_1, \dots, x_n) \in B_k : |\{x_1\} \cup \dots \cup \{x_n\}| = |K| - 1\}$$

и случайные величины $\xi'_k = \xi(B'_k)$. Из определений следует, что

$$\begin{aligned} |B_0| &= (|K| - 1)^n, \\ |B_k| &= (|K| - 1)^n - 1, & k \neq 0, \\ 0 &\leq \xi'_k \leq \xi_k, & k \in K, \\ |B'_k| &= |B_k|(1 + o(1)) \quad \text{при } m \rightarrow \infty. \end{aligned} \tag{15}$$

Вместе с условием (9) теоремы 2 все это влечет соотношение

$$\mathbf{P}\{\xi'_k \neq \xi_k\} \leq \mathbf{E}(\xi_k - \xi'_k) \rightarrow 0.$$

Значит,

$$\mathbf{P}\{(\xi'_k, k \in K) = (\xi_k, k \in K)\} \rightarrow 1. \tag{16}$$

Заметим теперь, что число решений системы, принадлежащих множеству B'_k , при $k, a \neq 0$ совпадает с числом решений, принадлежащих множеству B'_{ak} . Поэтому числа $\xi'_k, k \neq 0$, все одинаковы. Благодаря соотношению (16), аналогичным, но уже асимптотическим свойством обладают величины ξ_k . Утверждение (а) доказано.

Докажем утверждение (б). Пусть величины $\Lambda'(\vec{r})$ определяются для вектора $(B'_k, k \in K)$ аналогично величинам $\Lambda(\vec{r})$, определенным нами для $(B_k, k \in K)$.

Заметим, что $B'_0 \cap B'_k = \emptyset, k \neq 0$. Кроме того, множество B'_0 инвариантно относительно умножения своих элементов на ненулевые элементы поля. Поэтому оно содержит попавшие в него классы эквивалентности целиком. Значит,

$$\Lambda'(\vec{r}) = 0, \quad r_0 > 0, \quad \sum_{k \neq 0} r_k > 0.$$

Поэтому, согласно следствию 1, случайная величина ξ'_0 и случайный вектор $(\xi'_k, k \in K \setminus \{0\})$ асимптотически независимы. В силу (16) таким же свойством обладают величина ξ_0 и вектор $(\xi_k, k \in K \setminus \{0\})$.

Утверждение (б) доказано.

Для доказательства утверждения (в) надо заметить, что множество B_0 является $(|K| - 1)$ -слойным, и воспользоваться следствием 2. При этом условие (4) для этого множества уже проверено (см. (14)).

Для доказательства утверждения (г) заметим, что множество $B'_k, k \in K \setminus \{0\}$, является однослойным, а условие (4) для него вытекает из (14) и (15). Поэтому можно воспользоваться следствием 2 и установить сходимость распределения случайной величины ξ'_k к распределению Пуассона с параметром λ . Остается воспользоваться соотношением (13).

Утверждение (г) и теорема 2 доказаны.

Доказательство следствия 4 использует те же приемы, что и доказательство пункта (в) теоремы 2. Введем вспомогательную случайную величину ξ' , равную числу решений системы случайных однородных уравнений $Ax = 0$, содержащих точно по $|K| - 1$ разных элементов поля K . Тогда

$$\xi' = \sum_{k \in K} \xi'_k.$$

Кроме того, как следует из доказательства теоремы 2,

$$\mathbf{P} \left\{ \sum_{k \in K} \xi'_k = \sum_{k \in K} \xi_k \right\} \rightarrow 1.$$

Поэтому предельное поведение случайной величины ξ' совпадает с распределением случайной величины $(|K| - 1)(\pi_0 + \pi_1)$, то есть для $(|K| - 1)^{-1}\xi'$ предельным является распределением Пуассона с параметром $(|K| - 1)^{-1}|K|\lambda$.

Теперь воспользуемся тем, что $\mathbf{P}\{\xi' = \xi\} \rightarrow 1$. Последнее доказывается аналогично соотношению (16). Утверждение следствия доказано.

Доказательство теоремы 3 проводится вполне аналогично доказательству теоремы 2, и мы его опускаем.

Автор признателен Н. М. Меженной за ряд полезных замечаний.

Список литературы

1. Копытцев В. А., О числе решений систем линейных булевых уравнений в множестве векторов, обладающих заданным числом единиц. *Дискретная математика* (2002) **14**, №4, 87–109.
2. Копытцев В. А., Системы линейных уравнений с ограничениями для значений неизвестных. *Обозрение прикладной и промышленной математики* (2004) **11**, 241–242.
3. Михайлов В. Г., Предельные теоремы для числа точек случайного линейного подпространства, попавших в заданное множество. *Дискретная математика* (2003) **15**, №2, 128–137.
4. 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.
5. Михайлов В. Г., Предельные теоремы для числа ненулевых решений одной системы случайных уравнений над полем $GF(2)$. *Дискретная математика* (2000) **12**, №1, 70–81.
6. Михайлов В. Г., Предельная теорема Пуассона для числа неколлинеарных решений системы случайных уравнений специального вида. *Дискретная математика* (2001) **13**, №3, 81–90.

Статья поступила 27.12.2005.