Math-Net.Ru

Общероссийский математический портал

В. Г. Михайлов, Предельные теоремы для числа ненулевых решений одной системы случайных уравнений над полем $GF(2)$, *Теория вероятн. и ее примен.*, 1998, том 43, выпуск 3, 598–606

DOI: <https://doi.org/10.4213/tvp1564>

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: 54.92.164.108

26 апреля 2023 г., 14:39:17

9. Burkholder D. L. Explorations in martingale theory and its applications. — Lecture Notes in Math., 1991, v. 1464, p. 3–66.
10. Métivier M. Reele und vektorwertige quasimartingale and die theorie der stochastischen integration. — Lecture Notes in Math., 1977, v. 607, p. 1–310.
11. Métivier M., Pellaumail J. Stochastic Integration. New York: Academic Press, 1980, 196 p.
12. Burkholder D. L. Martingale transforms and the geometry of Banach spaces. — Lecture Notes in Math., 1981, v. 860, p. 35–50.
13. Burkholder D. L. A geometrical characterization of Banach spaces in which martingale differences are unconditional. — Ann. Probab., 1981, v. 9, № 6, p. 997–1011.
14. Rubio de Francia J. L. Martingale and integral transforms of Banach space valued functions. — Lecture Notes in Math., 1985, v. 1221, p. 195–222.
15. Tozoni S. A. Weighted inequalities for vector operators on martingales. — J. Math. Anal. Appl., 1995, v. 191, № 2, p. 229–249.
16. Tozoni S. A. Vector-valued extensions of operators on martingales. — J. Math. Anal. Appl., 1996, v. 201, № 1, p. 128–151.
17. Diestel J., Uhl J. J. Vector Measures. Providence, RI: Amer. Math. Soc., 1977, 322 p.
18. Lindenstrauss J., Tzafriri L. Classical Banach Spaces. II. Function Spaces. Berlin: Springer-Verlag, 1979, 244 p.

Поступила в редакцию
10.VII.1997

© 1998 г.

МИХАЙЛОВ В. Г.*

ПРЕДЕЛЬНЫЕ ТЕОРЕМЫ ДЛЯ ЧИСЛА НЕНУЛЕВЫХ РЕШЕНИЙ ОДНОЙ СИСТЕМЫ СЛУЧАЙНЫХ УРАВНЕНИЙ НАД ПОЛЕМ $GF(2)^{1)}$

Изучается предельное поведение числа решений системы случайных уравнений специального вида над полем $GF(2)$. Левые части уравнений этой системы представляют собой произведения независимо распределенных равновероятных линейных функций от n переменных из $GF(2)$, а правые части равны нулю. Показано, что при естественных предположениях на характер изменения параметров схемы (число неизвестных, число уравнений и число сомножителей в левой части отдельного уравнения) распределение числа ненулевых решений сходится к распределению Пуассона. Указаны также достаточные условия асимптотической нормальности числа ненулевых решений. В доказательствах использован метод моментов.

Ключевые слова и фразы: системы случайных уравнений, число решений, распределение Пуассона.

*Математический институт им. В. А. Стеклова РАН, ул. Губкина, 8, 117966, Москва, Россия.

¹⁾Работа выполнена при поддержке Российского фонда фундаментальных исследований, проект 96-01-00531, и Совета по грантам Президента РФ и государственной поддержке ведущих научных школ, проект 96-15-96092.

Рассмотрим систему случайных нелинейных уравнений над полем $GF(2)$

$$\prod_{i=1}^m (a_{i1}^i x_1 + \dots + a_{in}^i x_n + a_i^i) = 0, \quad t = 1, \dots, T, \quad (1)$$

где $m \geq 2$, коэффициенты a_{ij}^i являются независимыми случайными величинами, принимающими значения $0, 1 \in GF(2)$ с вероятностями $\frac{1}{2}$. Величины a_i^i считаются заданными. Если все произведения $a_i^1 \dots a_i^m$, $t = 1, \dots, T$, равны нулю, то система (1) имеет нулевое решение. В остальных случаях его нет. Поэтому имеет смысл изучать число ν ненулевых решений системы (1). Будем использовать обозначение V^n для n -мерного линейного пространства над полем $GF(2)$ и обозначения

$$(m)_r = m(m-1) \dots (m-r+1), \quad \Lambda = (2^n - 1)(1 - 2^{-m})^T. \quad (2)$$

Как будет показано ниже, $\Lambda = E\nu$.

Теорема 1. При $n > r$ выполнены неравенства

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

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

Теорема 2. Пусть параметры n и T стремятся к бесконечности, а параметр $m \geq 2$ меняется таким образом, что

$$\Lambda \rightarrow \lambda. \quad (5)$$

Тогда при всех натуральных r равномерно по наборам $\{a_i^i\}$

$$E(\nu)_r \rightarrow \lambda^r, \quad (6)$$

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

Теорема 3. Пусть параметры n и T стремятся к бесконечности, а параметр $m \geq 2$ меняется таким образом, что выполнены условия

$$\Lambda \rightarrow \infty, \quad (7)$$

$$n - \Lambda \left(7 + \frac{2}{\ln 2}\right) - \frac{\ln \Lambda}{2 \ln 2} \rightarrow \infty, \quad (8)$$

$$T - \frac{(2^m - 1)^2}{2^m - 2} \left(\frac{7}{2} 2^{7\Lambda} + 2\Lambda - \frac{1}{2} \ln \Lambda\right) \rightarrow \infty. \quad (9)$$

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

Рассмотрим теперь случай, когда для каждого n и m имеется бесконечная последовательность независимых уравнений вида (1). Тогда можно определить случайные величины

$$\tau_{n,m} = \max\{T: \text{система, образованная первыми } T \text{ уравнениями, имеет ненулевое решение}\}.$$

Теорема 4. Пусть $n \rightarrow \infty$, а $m \geq 2$ фиксировано. Тогда

$$\begin{aligned} \lim_{n \rightarrow \infty} P \left\{ \tau_{n,m} \leq \frac{n \ln 2 + x}{\ln 2^m - \ln(2^m - 1)} \right\} &= \exp \left\{ - \exp \left\{ -x + \ln(1 - 2^{-m}) \right\} \right\}, \\ \lim_{n \rightarrow \infty} P \left\{ \tau_{n,m} \leq \frac{n \ln 2 + x}{\ln 2^m - \ln(2^m - 1)} \right\} &= \exp \left\{ - \exp \{-x\} \right\}. \end{aligned} \quad (10)$$

Следствие. Пусть $n, m \rightarrow \infty$. Тогда имеет место равномерная по всем наборам $\{a_i^j\}$ сходимость

$$P \left\{ \tau_{n,m} < 2^m (n \ln 2 + x) \right\} \rightarrow e^{-e^{-x}}.$$

З а м е ч а н и е 1. Из теорем 1–4 вытекают аналогичные утверждения для системы вида (1) со случайными свободными членами $\{a_i^j\}$. При этом распределение вектора из свободных членов может быть произвольным, и достаточно предполагать лишь независимость этого вектора от набора случайных коэффициентов a_{ij}^j .

З а м е ч а н и е 2. Изложенные результаты показывают, что свойства системы уравнений (1) отличаются от свойств систем случайных линейных уравнений над полем $GF(2)$ (см., например, [1]). Если система случайных линейных уравнений совместна, то число ее решений является степенью двойки, поскольку множество решений каждого отдельного уравнения является гиперплоскостью в $GF(2)$. В нашем случае, на первый взгляд, геометрические свойства множеств решений отдельных уравнений (они заключаются в том, что дополнение к множеству решений в типичном случае является аффинной гиперплоскостью коразмерности m) тоже должны играть важную роль. Однако с ростом числа уравнений геометрические обстоятельства перестают быть определяющими, уступая эту роль комбинаторным свойствам системы. Это видно уже по тому, сколькими решениями обладают системы. Рассмотрим для примера систему (1) второй степени ($m = 2$) с единичными свободными членами ($a_i^j = 1$) при $n = 2$ и $n = 3$.

Из приведенных ниже таблиц видно, что при $m = 2$ и $n = 2$ или 3 системы из трех уравнений могут обладать любым числом решений из диапазона $\{0, 1, \dots, 2^n - 2^{n-2}\}$.

Таблица 1. Число систем второй степени с двумя неизвестными, T уравнениями и заданным числом решений

Число решений	$T = 1$	$T = 2$	$T = 3$	$T = 4$
0	1	31	883	21715
1	0	54	1458	26730
2	9	135	1539	15795
3	6	36	216	1296
всего	16	256	4096	65536

З а м е ч а н и е 3. 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. [2]).

З а м е ч а н и е 4. Описание основных задач теории систем случайных уравнений над конечными полями можно найти в книгах [1], [3] и работах [4] и [5]. Важным классом систем случайных уравнений являются заведомо совместные системы случайных уравнений. Асимптотические свойства числа решений ряда таких систем нелинейных уравнений изучались в работах [6] и [7]. В работах [8]–[10] 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.

Таблица 2. Число систем второй степени с тремя неизвестными, T уравнениями и заданным числом решений

Число решений	$T = 1$	$T = 2$	$T = 3$
0	1	127	13231
1	0	0	18144
2	0	378	64638
3	0	1008	68040
4	21	819	69363
5	0	1512	27216
6	42	252	1512
всего	64	4096	262144

Перейдем к доказательствам.

Доказательство теоремы 1. Система уравнений (1) эквивалентна системе из T m -мерных включений

$$\begin{pmatrix} a_{i1}^1 x_1 + \dots + a_{in}^1 x_n \\ \dots \\ a_{i1}^m x_1 + \dots + a_{in}^m x_n \end{pmatrix} \in D \begin{pmatrix} a_i^1 \\ \dots \\ a_i^m \end{pmatrix}, \quad i = 1, \dots, T, \quad (11)$$

где множество $D(a) \subset V^m$ ($a \in V^m$) получается из множества V^m выбрасыванием вектора $a + 1^m$ (вектор $1^m \in V^m$ состоит из одних единиц). Запишем систему включений (11) как одно включение в пространстве размерности mT . Для этого введем обозначения

$$A = \begin{pmatrix} a_{11}^1 \dots a_{1n}^1 \\ \dots \\ a_{11}^m \dots a_{1n}^m \\ \dots \\ a_{T1}^m \dots a_{Tn}^m \end{pmatrix}, \quad B = D \begin{pmatrix} a_1^1 \\ \dots \\ a_1^m \end{pmatrix} \times \dots \times \begin{pmatrix} a_T^1 \\ \dots \\ a_T^m \end{pmatrix}.$$

Заметим, что $|B| = (2^m - 1)^T$. Система (11) теперь запишется в виде $Ax \in B$.

Сопоставим каждой паре значений (x, b) , $x \in V^n \setminus \{0^n\}$, $b \in B$, случайную величину $\eta_{x,b} = I\{Ax = b\}$. Тогда

$$\nu = \sum_{x \in V^n \setminus \{0^n\}} \sum_{b \in B} \eta_{x,b}. \quad (12)$$

Из этого равенства вытекает следующее выражение для факториальных моментов $E(\nu)_r$ случайной величины ν :

$$E(\nu)_r = \sum_S E \prod_{i=1}^r \eta_{x^i, b^i}, \quad (13)$$

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

При анализе выражения (13) воспользуемся следующим свойством:

$$x^{i_1} + \dots + x^{i_s} = 0^n, \quad b^{i_1} + \dots + b^{i_s} \neq 0^{mT} \implies \eta_{x^{i_1}, b^{i_1}} \dots \eta_{x^{i_s}, b^{i_s}} = 0. \quad (14)$$

Получаем, что при $n \geq r$ и $k = 1, \dots, r$ для любых фиксированных $x^1, \dots, x^r$,

$$\text{rang}(x^1, \dots, x^r) = k,$$

выполняются равенства

$$\mathbb{E} \prod_{i=1}^r \eta_{x^i, b^i} = 2^{-kmT}, \quad (15)$$

если для любых $i_1, \dots, i_s$, $s \leq r$,

$$\text{rang}(b^{i_1}, \dots, b^{i_s}) \leq \text{rang}(x^{i_1}, \dots, x^{i_s}), \quad (16)$$

и

$$\mathbb{E} \prod_{i=1}^r \eta_{x^i, b^i} = 0 \quad (17)$$

в остальных случаях. В частности,

$$\mathbb{E} \nu = \sum \mathbb{E} \eta_{x^1, b^1} = |B| \left| V^n \setminus \{0^n\} \right| 2^{-mT} = (1 - 2^{-m})^T (2^n - 1). \quad (18)$$

Подсчитаем теперь старшие факториальные моменты. При этом воспользуемся следующим очевидным утверждением.

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

$$\mathbb{P}\{\eta_{x^1, b^1} = \dots = \eta_{x^r, b^r} = 1\} \leq 2^{-kmT}, \quad (19)$$

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

Оценим факториальные моменты снизу. В формуле (13) оставим лишь те слагаемые, для которых $\text{rang}(x^1, \dots, x^r) = r$. Заметим сразу, что таких наборов $x^1, \dots, x^r$ в области суммирования имеется $\prod_{s=0}^{r-1} (2^n - 2^s)$ штук. В каждом наборе $x^1, \dots, x^r$ все векторы различны, поэтому векторы $b^1, \dots, b^r$ в области суммирования могут быть выбраны произвольным образом. Поэтому из (13), (15)–(17) получаем:

$$\mathbb{E}(\nu)_r \geq \sum_{\substack{x^1, \dots, x^r \\ \text{rang}(x^1, \dots, x^r) = r}} \frac{|B|^r}{2^{rmT}} = (1 - 2^{-m})^r \prod_{s=0}^{r-1} (2^n - 2^s). \quad (20)$$

Таким образом, неравенство (3) доказано.

Оценим теперь факториальные моменты сверху. Каждому набору векторов $x^1, \dots, x^r \in V^n$ соответствует некоторая система $L(x^1, \dots, x^r)$ однородных линейных уравнений в V^n вида $x^{i_1} + \dots + x^{i_s} = 0^n$, возможно пустая, описывающая все линейные соотношения между $x^1, \dots, x^r$. Системе $L(x^1, \dots, x^r)$ сопоставим идентичную систему $L(b^1, \dots, b^r)$ из линейных уравнений относительно $b^1, \dots, b^r \in B$. Положим

$$B(x^1, \dots, x^r) = \{(b^1, \dots, b^r): \text{выполнена система } L(b^1, \dots, b^r)\}.$$

Введем обозначение

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

В частности,

$$S_{r,0} = S_{r,1} = \emptyset, \quad r \geq 2.$$

Лемма 2. При $n > r$ выполнено неравенство

$$E(\nu)_r \leq \sum_{k=2}^r \sum_{(x^1, \dots, x^r) \in S_{r,k}} \frac{|B(x^1, \dots, x^r)|}{2^{kmT}}. \quad (21)$$

Доказательство. Из (14) следует, что слагаемые, для которых найдутся такие $i, j, i \neq j$, что $x^i = x^j$, не вносят вклада в сумму (13) для $E(\nu)_r$. Остальные группируем в соответствии с введенным выше определением. Осталось воспользоваться леммой 1. Лемма 2 доказана. Далее нам понадобится

Лемма 3. Пусть $k \geq 3$. Для любого $b \in B$ число решений уравнения

$$b^1 + \dots + b^k = b \quad (22)$$

относительно $b^1, \dots, b^k \in B$ не превосходит $((2^m - 1)(2^m - 2) + 1)^T 2^{Tm(k-3)}$.

Доказательство. Сначала рассмотрим случай $T = 1$. В этом случае уравнение (22) решается при $b \in D(a)$ и относительно неизвестных $b^1, \dots, b^k \in D(a)$ при произвольном фиксированном $a \in V^m$.

Рассмотрим уравнение

$$b^1 + b^2 + b^3 = d \quad (23)$$

относительно $b^1, b^2, b^3 \in D(a)$ при произвольном фиксированном $d \in V^m$. Непосредственная проверка показывает, что уравнение (23) имеет при любых $a, d \in V^m$ не более

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

решений. Уравнение (22) приведем к виду (23), положив $d = b + b^4 + \dots + b^k$. Тогда при заданных $b^1, b^2, b^3 \in D(a)$ имеется не более $C(m)$ вариантов набора $b^1, b^2, b^3 \in D(a)$. Каждая из величин $b^4, \dots, b^k$ принимает не более 2^m значений. Поэтому уравнение (22) относительно $b^1, \dots, b^k \in D(a)$ имеет не более $C(m) 2^{m(k-3)}$ решений.

В случае произвольного T равенство (22) эквивалентно системе уравнений относительно координат векторов $b^1, \dots, b^k \in B$, составленной из T подсистем только что рассмотренного вида относительно непересекающихся множеств переменных (координат векторов). Поэтому число решений совокупной системы равно произведению числа решений всех составляющих подсистем. Лемма доказана.

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

$$|B(x^1, \dots, x^r)| \leq \left(1 - \frac{2^m - 2}{(2^m - 1)^2}\right)^T (2^m - 1)^{kT}. \quad (24)$$

Доказательство. Перенумеруем векторы $x^1, \dots, x^r$ так, чтобы $x^1, \dots, x^k$ составляли базис. Тогда систему $L(b^1, \dots, b^r)$ можно преобразовать к виду

$$\begin{aligned} b^{k+1} &= l_{k+1}(b^1, \dots, b^k), \\ &\vdots \\ b^r &= l_r(b^1, \dots, b^k). \end{aligned} \quad (25)$$

Так как из этих уравнений значения $b^{k+2}, \dots, b^r$ определяются по $b^1, \dots, b^k$ однозначно, то число решений системы (25) относительно $b^1, \dots, b^r$ не превосходит числа решений уравнения $b^{k+1} = l_{k+1}(b^1, \dots, b^k)$ относительно $b^1, \dots, b^k$. Последнее по

лемме 3 не превосходит $((2^m - 1)(2^m - 2) + 1)^T 2^{Tm(s-3)}$ (s — число существенных аргументов в выражении $b^{k+1} + l_{k+1}(b^1, \dots, b^k)$), если только $s \geq 3$. Последнее имеет место, поскольку в системах $L(x^1, \dots, x^r)$ и $L(b^1, \dots, b^r)$ нет одно- и двучленных уравнений. Осталось воспользоваться неравенством $s \leq k + 1$ и произвести необходимые преобразования. Лемма 4 доказана.

Вернемся к неравенству (21). Подставив оценку (24) в (21) (для слагаемых с $k < r$) и воспользовавшись очевидной оценкой

$$|B(x^1, \dots, x^r)| < |B| = (2^m - 1)^T,$$

получим:

$$E(\nu)_r \leq \sum_{k=1}^{r-1} |S_{r,k}| \left(1 - \frac{2^m - 2}{(2^m - 1)^2}\right)^T (1 - 2^{-m})^{kT} + |S_{r,r}| (1 - 2^{-m})^{rT}. \quad (26)$$

Очевидно, что

$$|S_{r,k}| \leq \binom{r}{k} \prod_{s=0}^{k-1} (2^n - 2^s) (2^k - 1)^{r-k}. \quad (27)$$

Применив эту оценку в (26), после некоторых упрощений нетрудно получить (4). Теорема 1 доказана.

Доказательство теоремы 2. Заметим, что из условия (5) вытекает сходимость

$$\left(1 - \frac{2^m - 2}{(2^m - 1)^2}\right)^T \rightarrow 0.$$

Поэтому соотношение (6) следует из неравенств (3) и (4) теоремы 1. Из него, в свою очередь, следует сходимость распределения. Обе эти сходимости равномерны по наборам $\{a_i^j\}$. Теорема 2 доказана.

Доказательство теоремы 3. Нам понадобится

Лемма 5. Пусть X и Y — неотрицательные целочисленные случайные величины и $\lambda = EX$. Если распределения этих случайных величин меняются так, что

$$\sup_{1 \leq r \leq 7\lambda} |E(X)_r (E(Y)_r)^{-1} - 1| \frac{e^{2\lambda}}{\sqrt{\lambda}} \rightarrow 0 \quad (28)$$

и при всех $r \leq 7\lambda$

$$E(Y)_r \leq C\lambda^r \quad (29)$$

для некоторой постоянной C , то

$$\max_{1 \leq r \leq 2\lambda} |P\{X \geq t\} - P\{Y \geq t\}| \rightarrow 0. \quad (30)$$

Это утверждение является непосредственным следствием леммы 3 работы [11] (см. также теорему 3.2 в обзоре [12]).

Применим эту лемму к случайной величине ν , взяв в качестве Y случайную величину $\pi(\Lambda)$, распределенную по закону Пуассона с параметром Λ . Проверим сначала, что условия леммы 5 в этом случае выполнены.

Так как $E(\pi(\Lambda))_r = \Lambda^r$, то условие (29) выполнено при $C = 1$. Из неравенств (3) и (4) следует, что

$$\frac{E(\nu)_r}{E(\pi(\Lambda))_r} - 1 \geq -r \frac{2^{r-1} - 1}{2^r - 1} \quad \text{и} \quad \frac{E(\nu)_r}{E(\pi(\Lambda))_r} - 1 \leq \exp \left\{ -T \frac{2^m - 2}{(2^m - 1)^2} + \frac{r2^{r-1}}{\Lambda} \right\}.$$

Из этих оценок и условий (8) и (9) следует, что условие (28) для ν и $\pi(\Lambda)$ выполнено.

Используя теперь лемму 5, получаем, что

$$\max_{0 \leq t \leq 2\Lambda} |P\{\nu \geq t\} - P\{\pi(\Lambda) \geq t\}| \rightarrow 0.$$

Отсюда следует неограниченное сближение функций распределения случайных величин $(\nu - \Lambda)\Lambda^{-1/2}$ и $(\pi(\Lambda) - \Lambda)\Lambda^{-1/2}$ в расширяющемся диапазоне $[-\Lambda^{1/2}, \Lambda^{1/2}]$ значений аргумента. Осталось заметить, что функция распределения случайной величины $(\pi(\Lambda) - \Lambda)\Lambda^{-1/2}$ сходится при $\Lambda \rightarrow \infty$ (см. условие (7)) к стандартной нормальной функции распределения. Теорема 3 доказана.

Доказательство теоремы 4. Чтобы отразить зависимость распределения случайной величины ν от параметров n и T , добавим в ее обозначение соответствующие символы: $\nu = \nu(n, T)$. Воспользуемся тождеством $P\{\tau_{n,m} < t\} = P\{\nu(n, t) = 0\}$ и теоремой 2. Положим

$$T(n, m, x) = \left\lfloor \frac{n \ln 2 + x}{\ln 2^m - \ln(2^m - 1)} \right\rfloor.$$

Имеем

$$\begin{aligned} P\left\{\tau_{n,m} \leq \frac{n \ln 2 + x}{\ln 2^m - \ln(2^m - 1)}\right\} &= P\left\{\tau_{n,m} \leq T(n, m, x)\right\} \\ &= \exp\left\{- (1 - 2^m)^{T(n, m, x) + 1} (2^n - 1)\right\} + o(1) \\ &= \exp\left(- \exp\left(\left(T(n, m, x) + 1\right) \ln(1 - 2^{-m}) + \ln(2^n - 1)\right)\right) + o(1) \\ &= \exp\left(- \exp\left(-x + \left(1 - \left\{\frac{n \ln 2 + x}{\ln 2^m - \ln(2^m - 1)}\right\}\right) \ln(1 - 2^{-m})\right)\right) + o(1). \quad (31) \end{aligned}$$

Заметим теперь, что отношение $\ln 2 / (\ln 2^m - \ln(2^m - 1))^{-1}$ является иррациональным числом. Поэтому при любом x

$$\lim_{n \rightarrow \infty} \left\{ \frac{n \ln 2 + x}{\ln 2^m - \ln(2^m - 1)} \right\} = 1, \quad \lim_{n \rightarrow \infty} \left\{ \frac{n \ln 2 + x}{\ln 2^m - \ln(2^m - 1)} \right\} = 0,$$

и из (31) следуют равенства (10). Теорема 4 доказана.

Автор признателен А. М. Зубкову за ряд полезных замечаний.

СПИСОК ЛИТЕРАТУРЫ

1. Коваленко И. Н., Левитская А. А., Савчук М. Н. Избранные задачи вероятностной комбинаторики. Киев: Наукова думка, 1986.
2. Сачков В. Н. Асимптотическое поведение числа t -минимальных покрытий. — Дискретн. матем., 1993, т. 5, в. 1, с. 36–44.
3. Колчин В. Ф. Системы случайных уравнений. М.: МИЭМ, 1988.
4. Балакин Г. В. Введение в теорию случайных систем уравнений. — Труды по дискретной математике (прилож. к журн. «Дискретная математика»), 1997, т. 1, с. 1–18.
5. Севастьянов Б. А., Чистяков В. П. О числе входных последовательностей, соответствующих выходной последовательности конечного автомата. — Обзор. прикл. промышл. матем., сер. дискретн. матем., 1994, т. 1, в. 1, с. 96–107.

6. 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.
7. Мизайлов В. Г. Предельные теоремы для случайного покрытия конечного множества и для числа решений системы случайных уравнений. — Теория вероятн. и ее примен., 1996, т. 41, в. 2, с. 272–283.
8. Копытцев В. А. О некоторых случайных заведомо совместных системах уравнений. — Обзорение прикл. промышл. матем., сер. дискретн. матем., 1994, т. 1, в. 1, с. 56–84.
9. Полин С. В. О случайных блужданиях на графе с отмеченным ребром. — Обзорение прикл. промышл. матем., сер. дискретн. матем., 1994, т. 1, в. 1, с. 85–92.
10. Мизайлов В. Г. Асимптотическая нормальность логарифма числа прообразов выходной последовательности конечного автомата. — Обзорение прикл. промышл. матем., сер. дискретн. матем., 1994, т. 1, в. 1, с. 126–135.
11. Зубков А. М. Неравенства для вероятностей переходов с запрещениями. — Матем. сб., 1979, т. 109 (151), № 4 (11), с. 491–532.
12. Мизайлов В. Г. Явные оценки в предельных теоремах для сумм случайных индикаторов. — Обзорение прикл. промышл. матем., сер. вероятн. и статист., 1994, т. 1, в. 4, с. 580–617.

Поступила в редакцию
3.XII.1997

© 1998 г.

ФЕЛЬДМАН Г. М.*

К ХАРАКТЕРИЗАЦИИ ГАУССОВСКИХ РАСПРЕДЕЛЕНИЙ НА АБЕЛЕВЫХ ГРУППАХ ПОСТОЯНСТВОМ РЕГРЕССИИ¹⁾

В заметке полностью описаны локально компактные абелевы группы X , на которых возможна характеристика гауссовского распределения постоянством регрессии.

Ключевые слова и фразы: локально компактная абелева группа, гауссовское распределение, регрессия.

В одной из первых работ, посвященных характеристическим задачам математической статистики на группах, А. Л. Рухин, изучая групповой аналог известной теоремы С. Н. Бернштейна о характеристике гауссовского распределения независимостью суммы и разности независимых случайных величин, установил, что для некоторого класса групп возможна характеристика гауссовского распределения в терминах постоянства регрессии (см. [1]).

В настоящей заметке мы дадим полное описание класса локально компактных абелевых групп, для которых эта характеристика имеет место.

Пусть X — локально компактная сепарабельная абелева метрическая группа, $Y = X^*$ — ее группа характеров, (x, y) — значение характера $y \in Y$ на элементе $x \in X$, $M^1(X)$ — множество вероятностных распределений на группе X , $\hat{\mu}(y)$ — характеристическая функция распределения $\mu \in M^1(X)$.

*Физико-технический институт низких температур АН Украины, просп. Ленина, 47, 310164 Харьков, Украина.

¹⁾Работа выполнена при поддержке INTAS-96-0858.