Math-Net.Ru

Общероссийский математический портал

В. Ф. Колчин, Пороговое свойство для систем уравнений
в конечных полях, *Дискрет. матем.*, 1999, том 11, вы-
пуск 3, 15–23

DOI: <https://doi.org/10.4213/dm382>

Использование Общероссийского математического портала Math-Net.Ru под-
разумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.89.56.158

26 апреля 2023 г., 14:03:34

УДК 519.2

Пороговое свойство для систем уравнений в конечных полях

© 1999 г. В. Ф. Колчин

Рассматривается система уравнений относительно неизвестных $x_1, \dots, x_N$ в $\text{GF}(q)$

$$a_1^{(t)} x_{i_1(t)} + \dots + a_r^{(t)} x_{i_r(t)} = b_t, \quad t = 1, \dots, T,$$

где $i_1(t), \dots, i_r(t)$, $t = 1, \dots, T$, — независимые одинаково распределенные случайные величины, принимающие значения $1, \dots, N$ с равными вероятностями, коэффициенты $a_1^{(t)}, \dots, a_r^{(t)}$, $t = 1, \dots, T$, — независимые одинаково распределенные случайные величины, не зависящие от $i_1(t), \dots, i_r(t)$, $t = 1, \dots, T$, и принимающие ненулевые значения из $\text{GF}(q)$ с равными вероятностями, а b_t , $t = 1, \dots, T$, — независимые случайные величины, не зависящие от левой части системы и принимающие значения из $\text{GF}(q)$ с равными вероятностями.

Обозначим A_r матрицу этой системы. Критический набор строк матрицы A_r определяется так же, как в $\text{GF}(2)$, но в этом случае строки входят в критический набор с весами из $\text{GF}(q)$. Доказано, что общее число $S(A_r)$ критических наборов в матрице A_r обладает пороговым свойством. Пусть $N, T \rightarrow \infty$ и $T/N \rightarrow \alpha$. Тогда при любом фиксированном целом $r \geq 3$ и любом фиксированном поле $\text{GF}(q)$ с $q \geq 3$ существует такая постоянная α_r , что $\mathbf{ES}(A_r) \rightarrow 0$, если $\alpha < \alpha_r$, и $\mathbf{ES}(A_r) \rightarrow \infty$, если $\alpha > \alpha_r$.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, проекты 96-01-00338 и 96-15-96092.

Напомним определение понятия критического набора, введенного в [3] (см. также [1, 2]) для $\text{GF}(2)$ и обобщенного на произвольные конечные поля в [5].

Рассмотрим $T \times N$ матрицу $A = \|a_{tj}\|$ в конечном поле $\text{GF}(q)$ с q элементами, и пусть

$$a_t = (a_{t1}, \dots, a_{tN}), \quad t = 1, \dots, T,$$

— ее строки.

Строки с номерами $t_1, \dots, t_m$ и весами $\varepsilon_1, \dots, \varepsilon_m$, принимающими ненулевые значения из $\text{GF}(q)$, образуют критический набор $B = \{t_1, \dots, t_m; \varepsilon_1, \dots, \varepsilon_m\}$, если сумма

$$\varepsilon_1 a_{t_1} + \dots + \varepsilon_m a_{t_m}$$

есть нулевой вектор.

Для критических наборов определим умножение на ненулевую константу $\alpha \in \text{GF}(q)$, полагая для $B = \{t_1, \dots, t_m; \varepsilon_1, \dots, \varepsilon_m\}$

$$\alpha B = \{t_1, \dots, t_m; \alpha \varepsilon_1, \dots, \alpha \varepsilon_m\},$$

и сложение, полагая

$$B = B_1 + B_2 = \{t_1, \dots, t_m; \varepsilon_1, \dots, \varepsilon_m\},$$

где $B_1 = \{t_1^{(1)}, \dots, t_{m_1}^{(1)}; \varepsilon_1^{(1)}, \dots, \varepsilon_{m_1}^{(1)}\}$ и $B_2 = \{t_1^{(2)}, \dots, t_{m_2}^{(2)}; \varepsilon_1^{(2)}, \dots, \varepsilon_{m_2}^{(2)}\}$ — критические наборы, и t , $1 \leq t \leq T$, входит в B с весом $\varepsilon = \varepsilon_j^{(1)}$, если $t = t_j^{(1)}$ для некоторого j и $t_j^{(1)} \notin \{t_1^{(2)}, \dots, t_{m_2}^{(2)}\}$, с весом $\varepsilon = \varepsilon_k^{(2)}$, если $t = t_k^{(2)}$ для некоторого k и $t_k^{(2)} \notin \{t_1^{(1)}, \dots, t_{m_1}^{(1)}\}$, и с весом $\varepsilon = \varepsilon_j^{(1)} + \varepsilon_k^{(2)}$, если

$$t = t_j^{(1)} = t_k^{(2)} \in \{t_1^{(1)}, \dots, t_{m_1}^{(1)}\} \cap \{t_1^{(2)}, \dots, t_{m_2}^{(2)}\}$$

и $\varepsilon_j^{(1)} + \varepsilon_k^{(2)} \neq 0$; в остальных случаях t не входит в $\{t_1, \dots, t_m\}$. Ясно, что эти операции над критическими наборами могут привести к объекту B , все веса которого равны нулю. В таком случае мы пишем $B = \emptyset$ и называем B пустым критическим набором.

Ясно, что если B , B_1 и B_2 — критические наборы, то αB и $\alpha_1 B_1 + \alpha_2 B_2$ также являются критическими наборами.

Критические наборы $B_1, \dots, B_s$ называются независимыми, если для любых ненулевых $\alpha_{i_1}, \dots, \alpha_{i_s} \in \text{GF}(q)$, $1 \leq i \leq s$,

$$\alpha_{i_1} B_{i_1} + \dots + \alpha_{i_t} B_{i_t} \neq \emptyset.$$

Обозначим $s(A)$ максимальное число независимых критических наборов в матрице A . Нетрудно показать (см., например, [2, 3]), что ранг $r(A)$ матрицы A и $s(A)$ связаны соотношением

$$r(A) + s(A) = T. \quad (1)$$

Обозначим $S(A)$ общее число непустых критических наборов в матрице A . Ясно, что в $\text{GF}(q)$

$$S(A) = q^{s(A)} - 1.$$

Рассмотрим систему из T уравнений в $\text{GF}(q)$ относительно неизвестных $x_1, \dots, x_N$

$$a_1^{(t)} x_{i_1(t)} + \dots + a_r^{(t)} x_{i_r(t)} = b_t, \quad t = 1, \dots, T, \quad (2)$$

где $i_1(t), \dots, i_r(t)$, $t = 1, \dots, T$, — независимые одинаково распределенные случайные величины, принимающие значения $1, \dots, N$ с равными вероятностями, коэффициенты $a_1^{(t)}, \dots, a_r^{(t)}$, $t = 1, \dots, T$, — независимые одинаково распределенные случайные величины, не зависящие от $i_1(t), \dots, i_r(t)$, $t = 1, \dots, T$, и принимающие ненулевые значения из $\text{GF}(q)$ с равными вероятностями, а b_t , $t = 1, \dots, T$, — независимые случайные величины, не зависящие от левой части системы и принимающие значения из $\text{GF}(q)$ с равными вероятностями.

Одной из основных характеристик системы случайных уравнений является вероятность того, что система совместна, то есть имеет хотя бы одно решение. Обозначим A_r матрицу системы (2). Нетрудно видеть, что вероятность $P_{N,T}$ совместности системы (2) можно представить в виде

$$P_{N,T} = \sum_{k=0}^{\infty} \mathbf{P}\{r(A_r) = k\} \frac{1}{q^{T-k}} = \sum_{s=0}^{\infty} \mathbf{P}\{s(A_r) = s\} \frac{1}{q^s}.$$

Поэтому, если $s(A_r) \rightarrow 0$ по вероятности, то вероятность $P_{N,T}$ совместности системы (2) стремится к единице. Если $s(A_r) \rightarrow \infty$ по вероятности, то вероятность $P_{N,T}$ стремится к нулю. В этой работе продолжаются исследования, начатые в [1, 2, 5], где рассматривались аналогичные системы уравнений в конечных полях. Здесь мы докажем, что в $\text{GF}(q)$ утверждение, аналогичное теоремам 1 из [1], [2] и [5] справедливо и для системы (2), а именно, доказываем, что $\mathbf{ES}(A_r)$ для системы (2) обладает так называемым пороговым свойством. Существование порогового свойства для $s(A_r)$ или для вероятности $P_{N,T}$ не доказано ни для одной системы, аналогичной системе (2).

Теорема 1. Пусть $r \geq 3$ и $q \geq 3$ фиксированы, $N, T \rightarrow \infty$ так, что $T/N \rightarrow \alpha$. Тогда существует такая постоянная α_r , что $\mathbf{ES}(A_r) \rightarrow 0$, если $\alpha < \alpha_r$, и $\mathbf{ES}(A_r) \rightarrow \infty$, если $\alpha > \alpha_r$.

Постоянная α_r есть первая компонента вектора, являющегося единственным решением следующей системы уравнений относительно трех неизвестных a , λ и x :

$$\begin{aligned} \left(\frac{1}{q} + \frac{q-1}{q} e^{-\lambda q/(q-1)} \right) e^{\lambda-x} \left(\frac{ar}{ar-x} \right)^a &= 1, \\ (q-1) \left(\frac{x}{\lambda} \right)^r \frac{ar-x}{x} &= 1, \\ \frac{\lambda(1 - e^{-\lambda q/(q-1)})}{1 + (q-1)e^{-\lambda q/(q-1)}} &= x. \end{aligned}$$

Численное решение этой системы дает следующие значения критических констант:

r^p	3	4	5	7	9	11	13
3	0.869163	0.853113	0.839614	0.817829	0.800427	0.785881	0.773358
4	0.959500	0.952984	0.947242	0.937362	0.928977	0.921642	0.9136
5	0.986443	0.984037	0.981848	0.977926	0.974444	0.971286	0.9647
6	0.995257	0.994383	0.993575	0.992096	0.990749	0.989498	0.988322
7	0.998299	0.997981	0.997685	0.997139	0.996634	0.996160	0.995707
8	0.999382	0.999266	0.999158	0.998956	0.998770	0.998593	0.998424
9	0.999774	0.999732	0.999692	0.999618	0.999549	0.999484	0.999421
10	0.999917	0.999902	0.999887	0.999859	0.999834	0.999810	0.999810

Общее число критических наборов $S(A_r)$ можно представить как сумму индикаторов. Положим $\xi_{t_1, \dots, t_m; \varepsilon_1, \dots, \varepsilon_m} = 1$, если матрица A_r имеет критический набор $\{t_1, \dots, t_m; \varepsilon_1, \dots, \varepsilon_m\}$, и $\xi_{t_1, \dots, t_m; \varepsilon_1, \dots, \varepsilon_m} = 0$ в противном случае. Ясно, что вероятность $\mathbf{P}\{\xi_{t_1, \dots, t_m; \varepsilon_1, \dots, \varepsilon_m} = 1\}$ не зависит от индексов $t_1, \dots, t_m$, и так как умножение на ненулевой элемент поля $\text{GF}(q)$ не изменяет распределения коэффициентов матрицы (2), эта вероятность не зависит от весов критического набора и равна вероятности $\mathbf{P}\{\xi_{1, \dots, m; 1, \dots, 1} = 1\}$.

Поэтому математическое ожидание общего числа критических наборов в матрице A_r равно

$$\mathbf{ES}(A_r) = \sum_{m=1}^T \binom{T}{m} (q-1)^m P_r(m, N), \quad (3)$$

где $(q-1)^m$ есть число способов выбрать веса критического множества и $P_r(m, N)$ есть вероятность того, что m выбранных строк образуют критический набор с фиксированными весами.

При оценке вероятности $P_r(m, N)$ нам потребуется следующее утверждение.

Пусть $\alpha_1, \dots, \alpha_n$ — независимые одинаково распределенные случайные величины с распределением, совпадающим с распределением ненулевых коэффициентов $a_1^{(t)}, \dots, a_r^{(t)}$, $t = 1, \dots, T$, системы (2), то есть

$$\mathbf{P}\{\alpha_1 = \gamma\} = \frac{1}{q-1}, \quad \gamma \in \text{GF}(q), \quad \gamma \neq 0.$$

Рассмотрим сумму в $\text{GF}(q)$

$$S_n = \alpha_1 + \dots + \alpha_n$$

и положим

$$P_n = \mathbf{P}\{S_n = 0\}.$$

Лемма 1. Для $n \geq 1$

$$P_n = \frac{1}{q} \left(1 + (-1)^n \frac{1}{(q-1)^{n-1}} \right).$$

Доказательство. По формуле полной вероятности

$$P_n = \sum_{\gamma \neq 0} \mathbf{P}\{S_{n-1} = \gamma, \alpha_n = -\gamma\} = \frac{1}{q-1} \sum_{\gamma \neq 0} \mathbf{P}\{S_{n-1} = \gamma\} = \frac{1}{q-1} (1 - P_{n-1}).$$

Полагая $P_1 = 0$ и

$$f(x) = \sum_{n=1}^{\infty} P_n x^n,$$

находим из выписанного выше рекуррентного соотношения, что

$$f(x) = \frac{x^2}{(q-1)(1-x)} - \frac{xf(x)}{q-1},$$

откуда следует, что

$$f(x) = \frac{x^2}{(q-1)(1-x)(1+x/(q-1))} = \frac{x^2}{q(q-1)} \left(\frac{q-1}{1-x} - \frac{1}{1+x/(q-1)} \right).$$

Разлагая в ряд простые дроби, получаем приведенную в лемме формулу.

Найдем верхнюю и нижнюю оценки для вероятности $P_r(m, N)$. Основным при получении этих оценок является следующее сведение к задаче о размещении частиц.

Поскольку $i_1(t), \dots, i_r(t)$, $t = 1, \dots, T$, независимы, суммы по столбцам любой $m \times N$ подматрицы матрицы A_r , рассматриваемым как ячейки в равновероятной схеме размещения частиц, есть суммы

$$\eta_1(rm, N), \dots, \eta_N(rm, N)$$

ненулевых коэффициентов, соответственно, где $\eta_1(rm, N), \dots, \eta_N(rm, N)$ — заполнения N ячеек после равновероятного размещения rm частиц. Как обычно, обозначим $\mu_k = \mu_k(rm, N)$ число ячеек, содержащих ровно k частиц.

Лемма 2. Для любого натурального s

$$P_r^{(2s-1)}(m, N) \leq P_r(m, N) \leq P_r^{(2s)}(m, N),$$

где

$$P_r^{(s)}(m, N) = \sum_{k=0}^N \sum_{k_0+k_2+\dots+k_{s-1}=k} \mathbf{P}\{\mu_0=k_0, \mu_1=0, \mu_2=k_2, \dots, \mu_{s-1}=k_{s-1}\} P_2^{k_2} \dots P_{s-1}^{k_{s-1}} P_s^{N-k}.$$

Доказательство. Так как умножение случайных величин $\alpha_1, \dots, \alpha_n$ в $\text{GF}(q)$ на ненулевой элемент поля не меняет их распределения и согласно лемме 1 вероятность $P_1 = 0$, ясно, что если $\mu_1(m, N) \neq 0$, то m выбранных строк не образуют критический набор ни при каких весах.

По формуле полной вероятности

$$P_r(m, N) = \sum_{k=0}^N \sum_{k_0+k_2+\dots+k_{s-1}=k} \mathbf{P}\{\mu_0=k, \mu_1=0, \mu_2=k_2, \dots, \mu_{s-1}=k_{s-1}\} \times P_r(m, N \mid k_0, 0, k_2, \dots, k_{s-1}), \quad (4)$$

где $P_r(m, N \mid k_0, 0, k_2, \dots, k_{s-1})$ — условная вероятность того, что m выбранных строк образуют критический набор с фиксированными весами при условии, что

$$\{\mu_0=k_0, \mu_1=0, \mu_2=k_2, \dots, \mu_{s-1}=k_{s-1}\}.$$

Утверждение леммы следует из этой формулы, так как согласно лемме 1 $P_n \leq P_{2s}$ при $n \geq 2s$ и $P_n \geq P_{2s-1}$ при $n \geq 2s-1$.

Пусть $\xi_1, \dots, \xi_N$ — независимые одинаково распределенные случайные величины, имеющие распределение Пуассона с параметром λ , то есть

$$p_k = \mathbf{P}\{\xi_1 = k\} = \frac{\lambda^k e^{-\lambda}}{k!}, \quad k = 0, 1, \dots$$

Пусть $\xi_1^{(s)}, \dots, \xi_N^{(s)}$ — независимые одинаково распределенные случайные величины с усеченным распределением

$$\mathbf{P}\{\xi_1^{(s)} = k\} = \mathbf{P}\{\xi_1 = k \mid \xi_1 \neq 0, 1, \dots, s-1\}, \quad k = s, s+1, \dots$$

Легко видеть, что

$$\begin{aligned} \mathbf{P}\{\xi_1^{(s)} = k\} &= \frac{\lambda^k e^{-\lambda}}{k! R_s}, \quad k = s, s+1, \dots, \\ \mathbf{E}\xi_1^{(s)} &= \lambda R_{s-1} / R_s, \end{aligned}$$

где

$$R_s = 1 - p_0 - p_1 - \dots - p_{s-1}.$$

Положим

$$\begin{aligned} \sigma^2 &= \mathbf{D}\xi_1^{(s)}, \\ Q_s &= p_0 + p_2 P_2 + \dots + p_{s-1} P_{s-1} + P_s(1 - p_0 - p_1 - \dots - p_{s-1}). \end{aligned}$$

Лемма 3. Если $m, N \rightarrow \infty$ так, что $rm/N = x$, где x — положительная постоянная, то

$$\begin{aligned} & \mathbf{P}\{\mu_0 = k_0, \mu_1 = 0, \mu_2 = k_2, \dots, \mu_{s-1} = k_{s-1}\} P_2^{k_2} \dots P_s^{k_s} \\ &= Q_s^N \left(\frac{x^x e^{-x}}{\lambda^x e^{-\lambda}} \right) \frac{\sqrt{x}}{\sigma \sqrt{q_0 q_2 \dots q_s} (2\pi N)^{(s-1)/2}} \\ &\times \exp\{-(u_0^2 + u_2^2 + \dots + u_s^2)/2 - (2\sqrt{q_2} u_2 + \dots + (s-1)\sqrt{q_{s-1}} u_{s-1})^2 / (2\sigma^2 q_s)\} (1 + o(1)) \end{aligned} \quad (5)$$

равномерно относительно целых

$$k_0, k_2, \dots, k_{s-1}, k_s = N - k = N - k_0 - k_2 - \dots - k_{s-1}$$

таких, что

$$u_i = \frac{k_i - Nq_i}{\sqrt{Nq_i}}, \quad i = 0, 2, 3, \dots, s,$$

лежат в конечных интервалах.

Доказательство. Хорошо известно (см., например, [4]), что совместное распределение заполнений ячеек $\eta_1(rm, N), \dots, \eta_N(rm, N)$, когда rm частиц равномерно размещаются по N ячейкам, совпадает с совместным условным распределением независимых одинаково распределенных величин $\xi_1, \dots, \xi_N$, имеющих распределение Пуассона с произвольным параметром λ , при условии, что $\xi_1 + \dots + \xi_N = rm$. Поэтому

$$\mathbf{P}\{\mu_0 = k_0, \mu_1 = 0, \mu_2 = k_2, \dots, \mu_{s-1} = k_{s-1}\} = C_1 C_2,$$

где

$$\begin{aligned} C_1 &= \frac{N!}{k_0! k_2! \dots k_s!} p_0^{k_0} p_2^{k_2} \dots p_{s-1}^{k_{s-1}} (1 - p_0 - p_1 - \dots - p_{s-1})^{k_s}, \\ C_2 &= \frac{\mathbf{P}\{\xi_1^{(s)} + \dots + \xi_{N-k}^{(s)} = rm - 2k_2 - \dots - (s-1)k_{s-1}\}}{\mathbf{P}\{\xi_1 + \dots + \xi_N = rm\}}. \end{aligned}$$

Преобразуем первый множитель. Легко видеть, что

$$C_1 P_2^{k_2} \dots P_s^{k_s} = Q_s^N \frac{N!}{k_0! k_2! \dots k_s!} q_0^{k_0} q_2^{k_2} \dots q_s^{k_s},$$

где

$$\begin{aligned} q_0 &= \frac{p_0}{Q_s}, \quad q_i = \frac{p_i P_i}{Q_s}, \quad i = 2, \dots, s-1, \\ q_s &= P_s R_s / Q_s. \end{aligned}$$

Полагая

$$u_i = \frac{k_i - Nq_i}{\sqrt{Nq_i}}, \quad i = 0, 2, 3, \dots, s,$$

и используя нормальное приближение для полиномиального распределения, получаем, что

$$\begin{aligned} & \frac{N!}{k_0! k_2! \dots k_s!} q_0^{k_0} q_2^{k_2} \dots q_s^{k_s} \\ &= \frac{1}{(2\pi N)^{(s-1)/2} \sqrt{q_0 q_2 \dots q_s}} \exp\{-(u_0^2 + u_2^2 + \dots + u_s^2)/2\} (1 + o(1)) \end{aligned}$$

равномерно относительно целых k_i , для которых u_i , $i = 0, 2, 3, \dots, s$, лежат в любых фиксированных конечных интервалах.

Выберем λ так, что

$$Nq_s \mathbf{E} \xi_1^{(s)} = rm - 2Nq_2 - \dots - (s-1)Nq_{s-1}.$$

Используя явное выражение для $\mathbf{E} \xi_1^{(s)}$, находим, что λ следует выбрать так, что

$$x = q_s R_{s-1} / R_s + 2q_2 + \dots + (s-1)q_{s-1}. \quad (6)$$

Применяя локальную предельную теорему о сходимости к нормальному распределению, получаем, что для такого значения параметра λ

$$\begin{aligned} \mathbf{P}\{\xi_1^{(s)} + \dots + \xi_{N-k}^{(s)} = rm - 2k_2 - \dots - (s-1)k_{s-1}\} \\ = \frac{1}{\sigma \sqrt{2\pi Nq_s}} \exp \left\{ -\frac{1}{2\sigma^2 q_s} (2\sqrt{q_2}u_2 + \dots + (s-1)\sqrt{q_{s-1}}u_{s-1})^2 \right\} (1 + o(1)) \end{aligned}$$

равномерно относительно целых k_i , для которых u_i , $i = 2, \dots, s-1$, лежат в любых фиксированных конечных интервалах.

Остается заметить, что

$$\begin{aligned} \mathbf{P}\{\xi_1 + \dots + \xi_N = rm\} &= \frac{(\lambda N)^{rm} e^{-\lambda N}}{(rm)!} \\ &= \frac{\lambda^{xN} e^{-\lambda N}}{x^{xN} \sqrt{2\pi xN} e^{-xN}} (1 + o(1)). \end{aligned}$$

Объединяя полученные оценки, приходим к выражению, указанному в лемме.

Лемма 4. Если $m, N \rightarrow \infty$ так, что $rm/N = x$, где x — фиксированная постоянная, то

$$P_r^{(s)}(m, N) = Q_s^N \left(\frac{x}{\lambda} \right)^{xN} e^{-xN + \lambda N} a_s(x, \lambda) (1 + o(1)),$$

где $a_i(x, \lambda)$ — непрерывная функция, не обращающаяся в нуль для всех допустимых x и λ .

Доказательство. Оценивая обычным образом (см. [1, 5]) хвосты суммы, представляющей $P_r^{(s)}(m, N)$, используя лемму 3 и заменяя суммирование интегрированием, получаем утверждение леммы.

Используя представление (3) и лемму 2, находим, что

$$\sum_{m=1}^T \binom{T}{m} (q-1)^m P_r^{(2s-1)}(m, N) \leq \mathbf{E} S(A_r) \leq \sum_{m=1}^T \binom{T}{m} (q-1)^m P_r^{(2s)}(m, N). \quad (7)$$

Положим $a = T/N$. Тогда при $N, T \rightarrow \infty$

$$\binom{T}{m} = \frac{ar}{\sqrt{2\pi x(ar-x)aN}} \left(\frac{(ar)^{ar} (ar-x)^x}{x^x (ar-x)^{ar}} \right)^{N/r} (1 + o(1)) \quad (8)$$

равномерно по m , $\delta \leq m/T \leq 1 - \delta$, и a , $0 < a_0 \leq a \leq a_1 < \infty$. Кроме того,

$$(q-1)^m = (q-1)^{xN/r} \quad (9)$$

Используя асимптотическое представление из леммы 4 и соотношения (8) и (9), получаем, что слагаемое суммы

$$\sum_{m=1}^T \binom{T}{m} (q-1)^m P_r^{(s)}(m, N)$$

имеет вид

$$(f_s(a, \lambda, x))^N c(a, \lambda, x) N^{-1/2} (1 + o(1)),$$

где

$$f_s(a, \lambda, x) = (q-1)^{x/r} Q_s \left(\frac{x}{\lambda} \right)^x e^{\lambda-x} \left(\frac{(ar)^{ar} (ar-x)^x}{x^x (ar-x)^{ar}} \right)^{1/r}$$

и $c(a, \lambda, x)$ — непрерывная функция, не обращающаяся в нуль для всех допустимых a, λ, x .

Оценивая обычным способом хвосты суммы в представлении (7) (см. [1]), нетрудно показать, что вне интервала $\delta \leq m/T \leq 1 - \delta$ выбором достаточно малого $\delta > 0$ сумма может быть сделана сколь угодно малой.

Рассуждая так же, как в [1] или [5], получаем, что точка $\alpha_r^{(s)}$ максимума слагаемого суммы по x , для которого $f_s(a, \lambda, x) = 1$, удовлетворяет системе уравнений

$$\begin{aligned} f_s(a, \lambda, x) &= 1, \\ (f_s(a, \lambda, x))'_x &= 0, \end{aligned}$$

где

$$x = q_s \lambda R_{s-1} / R_s + 2q_2 + \dots + (s-1)q_{s-1}.$$

Эта система может быть приведена к виду

$$\begin{aligned} (q-1)^{x/r} Q_s e^{\lambda-x} \left(\frac{x}{\lambda} \right)^x \left(\frac{(ar)^{ar} (ar-x)^x}{x^x (ar-x)^{ar}} \right)^{1/r} &= 1, \\ (q-1) \left(\frac{x}{\lambda} \right)^r \frac{ar-x}{x} &= 1, \\ q_s \lambda R_{s-1} / R_s + 2q_2 + \dots + (s-1)q_{s-1} &= x, \end{aligned}$$

эквивалентному указанному в теореме.

Так же, как в [1, 5], можно показать, что эта система имеет единственное решение, и если обозначить $\alpha_r^{(s)}$ первую координату этого решения, то ясно, что $\alpha_r^{(s)}$ при четном s дает нижнюю границу порогового значения α_r , если оно существует, а $\alpha_r^{(s)}$ при нечетном s дает верхнюю границу α_r . Ясно также, что $\{\alpha_r^{(2s)}\}$ и $\{\alpha_r^{(2s-1)}\}$ — монотонно возрастающая и монотонно убывающая последовательности, соответственно, и следовательно, сходятся к пределам при $s \rightarrow \infty$. Рассматривая систему уравнений как систему, зависящую от непрерывного параметра $t = (q-1)^{-s}$, нетрудно видеть, что решение непрерывно зависит от t , и поэтому эти последовательности

имеют общий предел, удовлетворяющий системе уравнений, получающейся переходом к пределу при $t \rightarrow 0$. При $t \rightarrow 0$

$$Q_s \rightarrow \frac{1}{q} + \frac{q-1}{q} e^{-\lambda q/(q-1)},$$

$$q_s \lambda R_{s-1}/R_s + 2q_2 + \dots + (s-1)q_{s-1} \rightarrow \frac{\lambda(1 - e^{-q\lambda/(q-1)})}{1 + (q-1)e^{-\lambda q/(q-1)}}.$$

Поэтому предельная система имеет вид, указанный в теореме 1. Численное решение этой системы дает величины критических констант, приведенные в таблице.

Настоящая статья является продолжением исследований, начатых в [6], где для $ES(A_r)$ были получены оценки сверху и снизу.

Заметим, что в [5] рассматривалась система вида

$$x_{i_1(t)} + \dots + x_{i_r(t)} = b_t, \quad t = 1, \dots, T. \quad (10)$$

Такая система получается, если в системе (2) положить $a_1^{(t)} = \dots = a_r^{(t)} = 1$. Хотя системы (2) и (10) различны, системы уравнений для пороговых значений параметров в этих случаях оказались одинаковыми.

Список литературы

1. Балакин Г. В., Колчин В. Ф., Хохлов В. И., Гиперциклы в случайном гиперграфе. *Дискретная математика* (1991) **3**, №3, 102–108.
2. Kolchin V. F., Random graphs and systems of linear equations in finite fields. *Random Structures and Algorithms* (1994) **5**, 135–146.
3. Колчин В. Ф., *Системы случайных уравнений*. МИЭМ, Москва, 1988.
4. Колчин В. Ф., *Случайные отображения*. Наука, Москва, 1984.
5. Колчин В. Ф., Хохлов В. И., Пороговый эффект для систем линейных уравнений специального вида. *Дискретная математика* (1995) **7**, №4, 29–39.
6. Колчин В. Ф., О пороговом эффекте для систем случайных уравнений. *Труды по дискретной математике* (1998) **2**, 183–190.

Статья поступила 20.02.1999.