Math-Net.Ru

Общероссийский математический портал

В. Н. Сачков, Вероятностные распределения на линейном векторном пространстве над полем Галуа и множествах подстановок, *Дискрет. матем.*, 1997, том 9, выпуск 3, 20–35

DOI: <https://doi.org/10.4213/dm489>

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: 52.90.164.192

26 апреля 2023 г., 06:10:33

Вероятностные распределения на линейном векторном пространстве над полем Галуа и множествах подстановок

© 1997 г. В. Н. Сачков

В статье найдены точное и предельные при $n \rightarrow \infty$ распределения числа векторов из некоторого объединения подпространств n -мерного векторного пространства V_n над полем Галуа $\text{GF}(q)$, попадающих в случайную систему из d , $1 \leq d \leq n$, линейно независимых векторов этого пространства. Для случайной величины, равной числу мест непротиворечивости случайной равновероятной подстановки с d -сужением m попарно противоречивых подстановок степени n , показано, что ее предельное распределение при $n \rightarrow \infty$ и фиксированном m является пуассоновским с параметром m . Отсюда в качестве следствия получено простое доказательство асимптотической формулы для числа латинских прямоугольников размера $m \times n$ при фиксированном m и $n \rightarrow \infty$.

1. Введение

В статье Джони и Рота [1] на основе использования конечных симплициальных комплексов и формул обращения Мёбиуса [2] проводится глубокая аналогия между известной теорией перечисления подстановок с ограниченными позициями, начало которой положено работами Капланского и Риордана [3, 4], и перечислением некоторых конфигураций в n -мерном векторном пространстве V_n над полем Галуа $\text{GF}(q)$. В качестве конфигураций рассматриваются неупорядоченные базисы пространства V_n , а свойство, соответствующее ограничению на позиции в подстановках, заключается в том, что элементы базиса не принадлежат некоторому подмножеству пространства V_n . Аналогия состоит в том, что в решении перечислительных задач в пространстве V_n так же, как и для подстановок с ограничениями, задача сводится в обоих случаях к определению числа граней с k элементами в соответствующих симплициальных комплексах.

В данной работе соответствующая аналогия проводится с вероятностной точки зрения. Конфигурациями в пространстве V_n над полем $\text{GF}(q)$ являются системы из d , $1 \leq d \leq n$, линейно независимых векторов, причем на множестве таких конфигураций задается равномерное вероятностное распределение. В качестве подмножества рассматривается объединение $W_{m_1} \cup \dots \cup W_{m_s}$, причем пространство V_n является прямой суммой своих подпространств $W_{m_1}, \dots, W_{m_s}, W_{m_{s+1}}$ размерностей $m_1, \dots, m_s, m_{s+1}$, $m_1 + \dots + m_s + m_{s+1} = n$.

Случайная величина $\xi_{n\bar{m}}(d)$, $\bar{m} = (m_1, \dots, m_s)$, равная числу элементов в случайной системе линейно независимых векторов $(v_1, v_2, \dots, v_d)$, $v_i \in V_n$, $1 \leq i \leq d$, принадлежащих $W_{m_1} \cup \dots \cup W_{m_s}$, называется числом включений. Для $\xi_{n\bar{m}}(d)$ найдены точное и весь спектр предельных распределений при $n \rightarrow \infty$. Предельные распределения оказываются четырех типов: биномиальное, пуассоновское, нормальное и вырожденное.

На совокупности S_n всех подстановок степени n , действующих на множестве $X = \{1, 2, \dots, n\}$, рассматривается система попарно противоречивых подстановок $s_1, \dots, s_m$, то есть таких, что $s_\mu(i) \neq s_\nu(i)$, $\mu \neq \nu$, $1 \leq i \leq n$. Задано некоторое d -подмножество $Y \subseteq X$. Будем говорить, что для подстановки $s \in S_n$ элемент $i \in Y$ является местом непротиворечивости d -сужению системы попарно противоречивых подстановок $s_1, \dots, s_m$, если существует такое ν , $1 \leq \nu \leq m$, что $s(i) = s_\nu(i)$. На множестве подстановок S_n задано равномерное вероятностное распределение и определена случайная величина $\eta_{nm}(d)$, равная числу мест непротиворечивости случайной подстановки с d -сужением системы из m попарно противоречивых подстановок. Для $m = 1$ приведено точное распределение $\eta_{nm}(d)$. При $n \rightarrow \infty$, $m/d \rightarrow 0$, $dm/n \rightarrow \lambda$ предельное распределение $\eta_{nm}(d)$ является пуассоновским с параметром λ . В качестве следствия установлено, что случайная величина η_{nm} , равная числу мест непротиворечивости случайной подстановки $s \in S_n$ с системой попарно противоречивых подстановок $s_1, \dots, s_m$ степени n , имеет при $n \rightarrow \infty$ и фиксированном m в качестве предельного распределение Пуассона с параметром m . Из этого результата, в свою очередь, в качестве следствия вытекает простое доказательство асимптотической формулы для числа латинских прямоугольников размера $m \times n$ при фиксированном m и $n \rightarrow \infty$.

Сравнение результатов по определению точных распределений случайных величин $\xi_{n\bar{m}}(d)$ и $\eta_{nm}(d)$ показывает, что в обоих случаях дело сводится к отысканию соответствующих биномиальных моментов, причем для $\eta_{nm}(d)$ эта задача сложнее. Если для $\xi_{n\bar{m}}(d)$ удастся определить весь спектр предельных распределений, то для $\eta_{nm}(d)$ придется ограничиться пуассоновским случаем. Впрочем, это обстоятельство не является неожиданным, так как отыскание асимптотических распределений $\eta_{nm}(d)$ фактически является, в некотором смысле, частью известной проблемы определения асимптотики числа латинских прямоугольников размера $m \times n$, когда m растет достаточно быстро с ростом n .

2. Точное распределение числа включений

Пусть $W_{m_1}, \dots, W_{m_s}$ — фиксированные подпространства n -мерного векторного пространства V_n над полем Галуа $\text{GF}(q)$ размерностей $m_1, \dots, m_s$, соответственно, причем $V_n = W_{m_1} + \dots + W_{m_s} + W_{m_{s+1}}$ — прямая сумма подпространств и $W = W_{m_1} \cup \dots \cup W_{m_s}$. На множестве из $(q^n - 1)(q^n - q) \dots (q^n - q^{d-1})$ систем $(v_1, \dots, v_d)$, $1 \leq d \leq n$, линейно независимых векторов в пространстве V_n зададим равномерное вероятностное распределение. Для случайной системы $(v_1, \dots, v_d)$ рассмотрим случайную величину $\xi_{n\bar{m}}(d)$, $\bar{m} = (m_1, \dots, m_s)$, равную числу векторов из W , принадлежащих этой системе. Эту случайную величину будем называть числом включений в систему $(v_1, \dots, v_d)$.

Теорема 1. Точное распределение случайной величины $\xi_{n\bar{m}}(d)$ имеет вид

$$\mathbf{P}(\xi_{n\bar{m}}(d) = r) = \sum_{k=r}^{\langle m, d \rangle} (-1)^{k-r} \binom{k}{r} B_k(n, \bar{m}, d), \quad r = 0, 1, \dots, \langle m, d \rangle, \quad (1)$$

где

$$m = \min(m_1, \dots, m_s), \quad \langle m, d \rangle = \min(m, d),$$

и $B_k(n, \bar{m}, d)$ — биномиальные моменты $\xi_{n\bar{m}}(d)$, определяемые формулой

$$B_k(n, \bar{m}, d) = \frac{1}{q^{nk}} \binom{d}{k} \prod_{j=n-k+1}^n \left(1 - \frac{1}{q^j}\right)^{-1} \sum_{k_1 + \dots + k_s = k} \frac{k!}{k_1! \dots k_s!} q^{\sum_{i=1}^s m_i k_i} \times \prod_{i=1}^s \prod_{j=m_i-k_i+1}^{m_i} \left(1 - \frac{1}{q^j}\right), \quad k = 0, 1, \dots, \langle m, d \rangle. \quad (2)$$

Доказательство. Для $\bar{k} = (k_1, \dots, k_s)$ обозначим через $Q_{nd}(\bar{m}, \bar{k})$ число способов выбора систем линейно независимых векторов $(v_1, \dots, v_d)$, $1 \leq d \leq n$, содержащих k_i векторов из подпространства W_{m_i} , $1 \leq i \leq s$, на фиксированных k_i местах. Так как $W_{m_1}, \dots, W_{m_s}$ являются слагаемыми прямой суммы $V_n = W_{m_1} + \dots + W_{m_s} + W_{m_s+1}$, то

$$Q_{nd}(\bar{m}, \bar{k}) = (q^n - q^k)(q^n - q^{k+1}) \dots (q^n - q^{d-1}) \times \prod_{i=1}^s (q^{m_i} - 1)(q^{m_i} - q) \dots (q^{m_i} - q^{k_i-1}), \quad (3)$$

где $k = k_1 + \dots + k_s$, $k_i \geq 0$, $1 \leq i \leq s$, и полагаем $(q^{m_i} - 1)(q^{m_i} - q) \dots (q^{m_i} - q^{k_i-1}) = 1$ при $k_i = 0$.

Обозначим через A_i событие, состоящее в том, что вектор v_i , $1 \leq i \leq d$, в случайной системе линейно независимых векторов $(v_1, \dots, v_d)$ принадлежит множеству $W = W_{m_1} \cup \dots \cup W_{m_s}$. Из формулы (3) следует, что

$$\mathbf{P}(A_{i_1} \cap \dots \cap A_{i_k}) = \frac{1}{(q^n - 1)(q^n - q) \dots (q^n - q^{k-1})} \sum_{k_1 + \dots + k_s = k} \frac{k!}{k_1! \dots k_s!} \times \prod_{i=1}^s (q^{m_i} - 1)(q^{m_i} - q) \dots (q^{m_i} - q^{k_i-1}), \quad 1 \leq i_1 < \dots < i_k \leq d. \quad (4)$$

С использованием равенства (4) и формулы (см., например, [10])

$$B_k(n, \bar{m}, d) = \sum_{1 \leq i_1 < \dots < i_k \leq d} \mathbf{P}(A_{i_1} \cap \dots \cap A_{i_k}), \quad k = 0, 1, \dots, \langle m, d \rangle, \quad (5)$$

получаем выражение для биномиальных моментов вида (2). Формула (1) является стандартным выражением распределения случайной величины через ее биномиальные моменты [10].

Следствие 1. Распределение случайной величины $\xi_{nm}(d)$ выражается через коэффициенты Гаусса [9]

$$\begin{bmatrix} m \\ k \end{bmatrix}_q = \frac{(q^m - 1)(q^{m-1} - 1) \dots (q^{m-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1) \dots (q^{k-1} - 1)} \quad (6)$$

в следующем виде:

$$\begin{aligned} \mathbf{P}(\xi_{nm}(d) = r) &= \sum_{k=r}^{\langle m, d \rangle} (-1)^{k-r} \binom{k}{r} \binom{d}{k} \sum_{k_1 + \dots + k_s = k} \frac{k!}{k_1! \dots k_s!} q^{-\sum_{j=1}^s \sum_{\nu=1}^{j-1} k_\nu} \\ &\times \prod_{i=1}^s \begin{bmatrix} m_i \\ k_i \end{bmatrix}_q \bigg/ \begin{bmatrix} n - \sum_{j=1}^{i-1} k_\nu \\ k_i \end{bmatrix}_q, \quad r = 0, 1, \dots, \langle m, d \rangle. \end{aligned} \quad (7)$$

где $\sum_{\nu=1}^{i-1} k_\nu = 0$ при $i = 1$.

Следствие 2. Пусть $\xi_{nm}(d)$ — число включений векторов из подпространства W_m размерности m в случайную равновероятную систему из d линейно независимых векторов $(v_1, \dots, v_d)$ из пространства V_n над полем $\text{GF}(q)$. Тогда

$$\mathbf{P}(\xi_{nm}(d) = r) = \sum_{k=r}^{\langle m, d \rangle} (-1)^{k-r} \binom{k}{r} B_k(n, m, d), \quad r = 0, 1, \dots, \langle m, d \rangle, \quad (8)$$

где $B_k(n, m, d)$ есть k -й биномиальный момент $\xi_{nm}(d)$, определяемый формулой

$$B_k(n, m, d) = \binom{d}{k} \frac{(q^m - 1)(q^{m-1} - 1) \dots (q^{m-k+1} - 1)}{(q^n - 1)(q^{n-1} - 1) \dots (q^{n-k+1} - 1)}, \quad k = 0, 1, \dots, \langle m, d \rangle. \quad (9)$$

Распределение (8) следующим образом выражается через коэффициенты Гаусса:

$$\mathbf{P}(\xi_{nm}(d) = r) = \sum_{k=r}^{\langle m, d \rangle} (-1)^{k-r} \binom{k}{r} \binom{d}{k} \begin{bmatrix} m \\ k \end{bmatrix}_q \bigg/ \begin{bmatrix} n \\ k \end{bmatrix}_q, \quad r = 0, 1, \dots, \langle m, d \rangle. \quad (10)$$

Следствие 2 вытекает из теоремы 1 и следствия 1 при $s = 1$.

Следствие 3. Если ξ_{nm} — число элементов упорядоченного случайного равновероятного базиса пространства V_n , принадлежащих подпространству W_m , то

$$\mathbf{P}(\xi_{nm} = r) = \sum_{k=r}^m (-1)^{k-r} \binom{k}{r} \binom{n}{k} \begin{bmatrix} m \\ k \end{bmatrix}_q \bigg/ \begin{bmatrix} n \\ k \end{bmatrix}_q, \quad k = 0, 1, \dots, m. \quad (11)$$

В частности, вероятность того, что случайный базис V_n не содержит векторов из подпространства W_m , равна

$$\mathbf{P}(\xi_{nm} = 0) = \sum_{k=0}^m (-1)^k \binom{n}{k} \begin{bmatrix} m \\ k \end{bmatrix}_q \bigg/ \begin{bmatrix} n \\ k \end{bmatrix}_q. \quad (12)$$

Следствие 3 вытекает из следствия 2 при $d = n$.

Следствие 4. Для среднего и дисперсии случайной величины $\xi_{n\bar{m}}(d)$ имеют место формулы

$$\begin{aligned} \mathbf{M}\xi_{n\bar{m}}(d) &= \frac{d}{q^n - 1} \sum_{i=1}^s (q^{m_i} - 1), \\ \mathbf{D}\xi_{n\bar{m}}(d) &= \frac{d}{q^n - 1} \sum_{i=1}^s (q^{m_i} - 1) \\ &\quad \times \left(1 - \frac{q^n - d(q-1) - 1}{(q^n - 1)(q^n - q)} \sum_{i=1}^s (q^{m_i} - 1) - \frac{(d-1)(q-1)}{q^n - q} \right). \end{aligned} \quad (13)$$

Среднее и дисперсия $\xi_{nm}(d)$ имеют вид

$$\begin{aligned} \mathbf{M}\xi_{nm}(d) &= \frac{d(q^m - 1)}{q^n - 1}, \\ \mathbf{D}\xi_{nm}(d) &= \frac{d(q^m - 1)}{q^n - 1} \left(1 - \frac{(q^m - 1)(q^n - d(q-1) - 1)}{(q^n - 1)(q^n - q)} - \frac{(d-1)(q-1)}{q^n - 1} \right). \end{aligned} \quad (14)$$

Формулы (13) следуют из выражений для среднего и дисперсии через биномиальные моменты

$$\begin{aligned} \mathbf{M}\xi_{n\bar{m}}(d) &= B_i(n, \bar{m}, d), \\ \mathbf{D}\xi_{n\bar{m}}(d) &= 2B_2(n, \bar{m}, d) + B_1(n, \bar{m}, d) - B_1^2(n, \bar{m}, d) \end{aligned}$$

и формулы (2). Формулы (14) следуют из формул (13) при $s = 1$.

В соответствии с формулами (14), как и следовало ожидать,

$$\mathbf{D}\xi_{nn}(d) = 0,$$

то есть распределение $\xi_{nn}(d)$ является вырожденным.

3. Предельные распределения числа включений

Предварительно докажем следующую лемму, определяющую асимптотические оценки биномиальных моментов $\xi_{n\bar{m}}(d)$.

Лемма. Если $n \rightarrow \infty$ и $\langle m, d \rangle \rightarrow \infty$, то

$$B_k(n, \bar{m}, d) = \frac{1}{q^{nk}} \binom{d}{k} \left(\sum_{i=1}^s q^{m_i} \right)^k \left(1 + O\left(\frac{1}{\langle m, d \rangle} \right) \right), \quad (15)$$

где остаточный член стремится к нулю равномерно для всех значений $k = 0, 1, \dots, \langle m, d \rangle - \log_q \langle m, d \rangle$. Кроме того, существует такая постоянная $C = C(q)$, зависящая только от q , что

$$B_k(n, \bar{m}, d) \leq \frac{C}{q^{nk}} \binom{d}{k} \left(\sum_{i=1}^s q^{m_i} \right)^k, \quad k = 0, 1, \dots, \langle m, d \rangle. \quad (16)$$

Доказательство. Для доказательства леммы рассмотрим величины

$$Q_k(n, m) = \prod_{j=m-k+1}^{n-k} \left(1 - \frac{1}{q^j}\right), \quad k = 0, 1, \dots, m, \quad m \leq n. \quad (17)$$

Нетрудно установить, что

$$1 - \frac{1}{q-1} \frac{1}{q^{m-k}} \leq Q_k(n, m) \leq 1 - \frac{1}{q} \frac{1}{q^{m-k}}, \quad k = 0, 1, \dots, m. \quad (18)$$

Применяя неравенства (18) к оценке правой части равенства (2), приходим к асимптотической формуле (15). Неравенство (16) получается также путем применения верхней оценки (18) к правой части равенства (2).

Полагая $m_i = m_i(n)$, $1 \leq i \leq s$, определим функцию γ_n равенством

$$d \sum_{i=1}^s q^{m_i} = q^{n+\gamma_n}. \quad (19)$$

Если

$$\hat{m} = \max_{1 \leq i \leq s} m_i, \quad m = \min_{1 \leq i \leq s} m_i, \quad \varkappa_n = \hat{m} - m,$$

то из соотношения (19) следует, что

$$n\varkappa_n - \log_q d + \gamma_n - \log_q s \leq m \leq n. \quad (20)$$

Ниже будут использоваться обозначения

$$a = a_n = q^{\gamma_n}, \quad \sigma^2 = \sigma_n^2 = q^{\gamma_n} (1 - q^{\gamma_n}/d). \quad (21)$$

Теорема 2. При $n \rightarrow \infty$ случайная величина $\xi_{n\bar{m}}(d)$ имеет следующие предельные распределения:

- (a) при $\gamma_n \rightarrow -\infty$ предельное распределение является вырожденным, а именно $\mathbf{P}(\xi_{n\bar{m}}(d) = 0) \rightarrow 1$;
- (b) при $\gamma_n \rightarrow \gamma$, $-\infty < \gamma < \infty$, если $m, d \rightarrow \infty$, то $\xi_{n,\bar{m}}(d)$ в пределе имеет распределение Пуассона с параметром $\lambda = q^\gamma$; если $m \rightarrow \infty$, а d фиксировано, то предельным является биномиальное распределение с вероятностью успеха $p = q^\gamma/\alpha$;
- (c) при $\gamma_n \rightarrow \infty$, если для достаточно большого n выполнены неравенства

$$\gamma_n < C \log_q d, \quad 0 < C < 1, \quad \varkappa_n \leq \alpha n^\varepsilon, \quad \log_q s = o(n^\varepsilon),$$

где $0 < \varepsilon < 1$ и α — некоторая постоянная величина, то случайная величина $\xi_{n\bar{m}}(d) = (\xi_{n\bar{m}}(d) - q^{\gamma_n})\sigma^{-1}$ имеет в пределе нормальное распределение с параметрами $(0, 1)$.

Доказательство. Из оценки (16) леммы следует, что

$$B_k(n, \bar{m}, d) \leq \frac{C}{k!} (q^{\gamma_n})^k, \quad k = 0, 1, \dots, \langle m, d \rangle,$$

и, следовательно, при выполнении условия (а) теоремы $B_k(n, \bar{m}, d) \rightarrow 0$ для всех $k = 1, 2, \dots, \langle m, d \rangle$, то есть утверждение пункта (а) теоремы справедливо.

В соответствии с формулой (15) при $\gamma_n \rightarrow \gamma$, $-\infty < \gamma < \infty$, если $m, d \rightarrow \infty$, то имеет место соотношение

$$B_k(n, \bar{m}, d) \rightarrow \frac{1}{k!} (q^\gamma)^k, \quad k = 0, 1, \dots \quad (22)$$

Отсюда следует, что предельное распределение является пуассоновским с параметром $\lambda = q^\gamma$. Если же $d < \infty$ и $m \rightarrow \infty$, то аналогично формуле (15) можно установить, что

$$B_k(n, \bar{m}, d) = \binom{d}{k} \left(\frac{q^\gamma}{d} \right)^k \left(1 + O\left(\frac{1}{m} \right) \right), \quad (23)$$

с равномерной оценкой остаточного члена. Отсюда следует, что $\xi_{n\bar{m}}(d)$ имеет в пределе биномиальное распределение с вероятностью успеха $p = q^\gamma/d$.

Из соотношения (19) вытекают неравенства

$$n - n^\varepsilon + \gamma_n - \log_q d - \log_q s \leq m \leq n. \quad (24)$$

Из этих неравенств и условий пункта (с) теоремы следует, что $m, d \rightarrow \infty$ при $n \rightarrow \infty$.

Получим асимптотическое представление производящей функции $\xi_{n\bar{m}}(d)$

$$P_{nm}(x; d) = \sum_{k=0}^{\langle m, d \rangle} B_k(n, \bar{m}, d) (x-1)^k \quad (25)$$

в некоторой δ -окрестности точки $x = 1$.

При получении этого представления рассмотрим два случая. В первом случае $\langle m, d \rangle = d$, во втором случае $\langle m, d \rangle = m$.

В первом случае из равенства (25), формулы (15) и неравенства (16) леммы находим, что

$$P_{nm}(x; d) = \sum_{k=0}^d \binom{d}{k} \left(\frac{q^{\gamma_n}}{d} \right)^k (x-1)^k \left(1 + O\left(\frac{1}{d} \right) \right) + S_1 - S_2, \quad (26)$$

где

$$S_1 \leq C \sum_{k=d-\log_q d+1}^d \binom{d}{k} \left(\frac{\delta q^{\gamma_n}}{d} \right)^k,$$

$$S_2 \leq \sum_{k=d-\log_q d+1}^d \binom{d}{k} \left(\frac{\delta q^{\gamma_n}}{d} \right)^k,$$

равномерно для всех x таких, что $1 - \delta < x < 1 + \delta$, $0 < \delta < 1$.

Из очевидной оценки

$$S_1 + S_2 \leq (1 + C) \left(\frac{\delta q^{\gamma_n}}{d} \right)^{d - \log_q d} \sum_{k=0}^{\log_q d} \binom{d}{k}$$

следует, что

$$S_1 + S_2 \leq (1 + C) q^{-H_n(d)},$$

где

$$H_n(d) = d \log_q \left(\frac{d}{\delta q^{\gamma_n}} \right) - \log_q d \left(\log_q d + \log_q \frac{d}{\delta q^{\gamma_n}} \right) - \log_q \log_q d. \quad (27)$$

Так как для достаточно больших n справедлива оценка $q^{\gamma_n}/d \leq C < 1$, то $S_1 + S_2 \rightarrow 0$ при $n \rightarrow \infty$, и, следовательно, из равенства (26) вытекает асимптотическое представление

$$P_{nm}(x; d) = \left(1 + \frac{q^{\gamma_n}}{d} (x - 1) \right)^d (1 + o(1)) + o(1) \quad (28)$$

равномерно для всех x , $1 - \delta < x < x + \delta$, $0 < \delta < 1$.

Рассмотрим теперь второй случай, когда $\langle m, d \rangle = m$. В этом случае из равенства (25) следует, что равномерно для всех x , $1 - \delta < x < 1 + \delta$, $0 < \delta < 1$,

$$P_{nm}(x; d) = \sum_{k=0}^d \binom{d}{k} \left(\frac{q^{\gamma_n}}{d} \right)^k (x - 1)^k \left(1 + O \left(\frac{1}{m} \right) \right) + S'_1 - S'_2,$$

где

$$S'_1 \leq C \sum_{k=m - \log_q m + 1}^d \binom{d}{k} \left(\frac{\delta q^{\gamma_n}}{d} \right)^k,$$

$$S'_2 \leq \sum_{k=m - \log_q m + 1}^d \binom{d}{k} \left(\frac{\delta q^{\gamma_n}}{d} \right)^k.$$

Очевидно, что

$$S'_1 + S'_2 \leq (1 + C) \left(\frac{\delta q^{\gamma_n}}{d} \right)^{m - \log_q m} \sum_{k=0}^{d - m + \log_q m} \binom{d}{k}.$$

Из условий пункта (с) теоремы следует, что при $n \rightarrow \infty$

$$m - \log_q m \geq n(1 + o(1)),$$

$$d - m + \log_q m \leq n^\varepsilon (1 + o(1)).$$

Следовательно,

$$S'_1 + S'_2 \leq (1 + C) q^{-\tilde{H}_n(q)},$$

где

$$\tilde{H}_n(q) = n(1 + o(1)) \log_q \left(\frac{d}{\delta q^{\gamma_n}} \right) - n^\varepsilon (1 + o(1)) \log_q d - \varepsilon \log_q n.$$

Так как для достаточно больших n справедлива оценка $q^{\gamma_n}/d < 1$, то $S'_1 + S'_2 \rightarrow 0$ при $n \rightarrow \infty$ и, следовательно, для $P_{nm}(x; d)$ имеет место асимптотическое представление вида (28).

Производящая функция моментов случайной величины $\xi'_{nm}(d)$ имеет следующее выражение через производящую функцию $\xi_{nm}(d)$:

$$M_{nm}(t; d) = e^{-at/\sigma} P_{nm}(e^{t/\sigma}; d), \quad (29)$$

где a и σ определяются формулами (21). При выполнении условий пункта (с) теоремы $\sigma = \sigma_n \rightarrow \infty$ при $n \rightarrow \infty$. Следовательно, из асимптотического представления (28) следует, что при $n \rightarrow \infty$ для любого t

$$M_{nm}(t; d) = e^{-at/\sigma} \left(1 + (e^{t/\sigma} - 1) \frac{q^{\gamma_n}}{d} \right)^d (1 + o(1)) + o(1). \quad (30)$$

Учитывая, что $q^{\gamma_n} < d$, получаем асимптотическое разложение при $n \rightarrow \infty$

$$d \ln \left(1 + \frac{q^{\gamma_n}}{d} (e^{t/\sigma} - 1) \right) = \frac{q^{\gamma_n}}{\sigma} t + \frac{t^2}{2\sigma^2} q^{\gamma_n} \left(1 - \frac{q^{\gamma_n}}{d} \right) + O \left(d \left(\frac{q^{\gamma_n}}{d\sigma} \right)^3 \right).$$

Из этого разложения и равенства (30) с учетом формул (21) при выполнении условий пункта (с) теоремы находим, что при $n \rightarrow \infty$ для любого t

$$M_{nm}(t; d) \rightarrow e^{t^2/2}.$$

Отсюда на основании теоремы Куртисса [10] следует справедливость пункта (с) теоремы.

В заключение отметим, что нормировки a и σ в пункте (с) теоремы являются естественными, так как из формул (13) при $n \rightarrow \infty$ следуют соотношения

$$\begin{aligned} \mathbf{M}\xi_{nm}(d) &= q^{\gamma_n} (1 + o(1)), \\ \mathbf{D}\xi_{nm}(d) &= q^{\gamma_n} (1 - q^{\gamma_n}/d) (1 + o(1)). \end{aligned} \quad (31)$$

Следствие 5. Пусть $m = m(n)$ и γ_n определяется соотношением

$$\gamma_n = \log_q d - n + m. \quad (32)$$

Тогда при $m < n$ и $n \rightarrow \infty$ случайная величина $\xi_{nm}(d)$, равная числу включений векторов из подпространства W_m пространства V_n над полем $\text{GF}(q)$ в случайной системе линейно независимых векторов $(v_1, \dots, v_d)$, имеет следующие предельные распределения:

- (а) при $\gamma_n \rightarrow -\infty$ предельное распределение является вырожденным, а именно $\mathbf{P}(\xi_{nm}(d) = 0) \rightarrow 1$;
- (б) при $\gamma_n \rightarrow \gamma$, $-\infty < \gamma < \infty$, если $d \rightarrow \infty$, то $\xi_{n,m}(d)$ имеет в пределе распределение Пуассона с параметром $\lambda = q^\gamma$; если d фиксировано, то предельным является биномиальное распределение с вероятностью успеха $p = q^\gamma/d$;

(с) при $\gamma_n \rightarrow \infty$ случайная величина

$$\xi'_{nm}(d) = (\xi_{nm}(d) - a)\sigma^{-1},$$

где

$$a = a_n = q^{\gamma_n}, \quad \sigma = \sigma_n^2 = q^{\gamma_n}(1 - q^{\gamma_n}/d),$$

имеет в пределе нормальное распределение с параметрами $(0, 1)$.

Следствие вытекает из теоремы 2 при $s = 1$, причем в этом случае некоторые условия теоремы 2 выполняются автоматически. Так, из условия (32), которое является следствием соотношения (19), при выполнении условия (b) следствия при $n \rightarrow \infty$ следует, что $m \rightarrow \infty$. При выполнении условия (с) следствия, если $\gamma_n < \log_q d$, то остальные условия следуют автоматически.

В теореме 2 важную роль играет предположение о том, что для достаточно большого n выполнено условие $q^{\gamma_n} < d$, так как при $q^{\gamma_n} = d$ в соответствии с формулами (31) распределение $\xi_{n\bar{m}}(d)$ является асимптотически вырожденным и $P(\xi_{n\bar{m}}(d) = d) \rightarrow 1$. Примером определенных выше подпространств $W_{m_1}, \dots, W_{m_s}$ являются рассматриваемые в следующем параграфе так называемые стандартные подпространства.

4. Стандартные системы подпространств

Пусть V_n есть n -мерное векторное пространство над полем $\text{GF}(q)$, представляющее собой совокупность вектор-строк $(v_1, \dots, v_n)$, где $v_i \in \text{GF}(q)$, $1 \leq i \leq n$. Подпространство W_m пространства V_n , имеющее размерность m называется стандартным, если оно представляет собой совокупность всех векторов V_n , у которых $n - m$ фиксированных координат равны нулю, $1 \leq m \leq n$.

Стандартные подпространства W_{m_1} и W_{m_2} имеют в пересечении единственный вектор, являющийся нулевым, тогда и только тогда, когда для любых векторов $w_1 \in W_{m_1}$ и $w_2 \in W_{m_2}$ скалярное произведение $(w_1, w_2) = 0$, то есть векторы w_1 и w_2 ортогональны. Будем говорить, что в этом случае стандартные подпространства W_{m_1} и W_{m_2} взаимно ортогональны.

Система стандартных подпространств $W_{m_1}, \dots, W_{m_s}$ пространства V_n является стандартной, если для любых $1 \leq i < j \leq s$ пересечение $W_{m_i} \cap W_{m_j}$ содержит только нулевой вектор, причём $s \leq m_1 + \dots + m_s \leq n$. Ясно, что система $W_{m_1}, \dots, W_{m_s}$ стандартная тогда и только тогда, когда входящие в нее стандартные подпространства являются попарно ортогональными и $s \leq m_1 + \dots + m_s \leq n$.

Обозначим через $D_n(m_1, \dots, m_s)$ число стандартных систем подпространств V_n размерностей $m_1, \dots, m_s$. Нетрудно установить, что

$$D_n(m_1, \dots, m_s) = \frac{(n)_{m_1 + \dots + m_s}}{m_1! m_2! \dots m_s!}, \quad s \leq m_1 + \dots + m_s \leq n. \quad (33)$$

Если $D_n(m, s)$ — число стандартных систем подпространств $W_{m_1}, \dots, W_{m_s}$ пространства V_n таких, что $m_1 + \dots + m_s = m$, $s \leq m \leq n - 1$, то из формулы для чисел Стирлинга $\sigma(m, s)$ второго рода [11]

$$\sigma(m, s) = \sum \frac{m!}{m_1! m_2! \dots m_s!},$$

где суммирование ведется по $m_1, \dots, m_s \geq 1$, $m_1 + \dots + m_s = m$, следует формула

$$D_n(m, s) = \binom{n}{m} \sigma(m, s), \quad 1 \leq s \leq m \leq n. \quad (34)$$

Обозначим теперь через $D_n(m)$ число стандартных систем подпространства V_n , сумма размерностей которых равна m .

Из формулы, выражающей числа Белла T_m через числа Стирлинга второго рода [9]

$$T_m = \sum_{s=1}^m \sigma(m, s), \quad m \geq 1,$$

находим, что

$$D_n(m) = \begin{cases} \binom{n}{m} T_m, & 1 \leq m \leq n-1, \\ T_n - 1, & m = n. \end{cases} \quad (35)$$

Используя соотношение для чисел Белла [9]

$$T_{n+1} = \sum_{m=0}^n \binom{n}{m} T_{n-m}, \quad T_0 = 1,$$

получаем формулу для общего числа D_n стандартных систем подпространств пространства V_n

$$D_n = T_{n+1} - 2. \quad (36)$$

Следует отметить, что формула (36) дает еще одну, не встречавшуюся ранее, комбинаторную интерпретацию чисел Белла.

Определение стандартной системы подпространств V_n не зависит от q , поэтому, не ограничивая общности, можно положить $q = 2$. Для $n = 2$ имеются три стандартные системы подпространств V_2 вида $W_1 = \{(z, 0)\}$, $W_2 = \{(0, z)\}$ и W_1, W_2 , где z принимает всевозможные значения из поля $\text{GF}(q)$. Этот результат согласуется с тем, что $T_3 = 5$.

Для чисел Белла известна формула Добинского

$$T_n = \frac{1}{e} \sum_{k=0}^{\infty} \frac{k^n}{k!}$$

и асимптотика при $n \rightarrow \infty$

$$T_n = \frac{1}{\sqrt{r+1}} e^{n(r+1/r-1)-1} (1 + o(1)),$$

где r — единственное решение уравнения $re^r = n$ [9].

5. Распределение числа мест непротиворечивости случайной подстановки

Пусть S_n — множество всех подстановок степени n , действующих на множестве $X = \{1, 2, \dots, n\}$. Подстановки s и s' такие, что $s, s' \in S_n$ и $s(i) \neq s'(i)$, $i = 1, 2, \dots, n$, называются противоречивыми.

Рассмотрим систему $s_1, s_2, \dots, s_m$ попарно противоречивых подстановок, $s_1, \dots, s_m \in S_n$, $1 \leq m \leq n$. Определим отображение F такое, что

$$F(j) = \{s_1(j), s_2(j), \dots, s_m(j)\}, \quad j = 1, 2, \dots, n.$$

Для d -подмножества $Y \subseteq X$ определим d -сужение отображения F равенством

$$F(j) = \{s_1(j), s_2(j), \dots, s_m(j)\}, \quad j \in Y. \quad (37)$$

На множестве S_n подстановок степени n зададим равномерное вероятностное распределение. Обозначим через $\eta_{nm}(d)$ случайную величину, значения которой для случайной подстановки $s \in S_n$ определяются равенством

$$\eta_{nm}(\alpha) = |\{j: \{s(j) = s_1(j)\} \cup \dots \cup \{s(j) = s_m(j)\}, j \in Y\}|,$$

где Y есть d -подмножество X и $\{s(j) = s_i(j)\}$ — событие, состоящее в том, что $s(j) = s_i(j)$, $1 \leq i \leq m$. Будем называть $\eta_{nm}(d)$ числом мест непротиворечивости случайной подстановки $s \in S_n$ для d -сужения отображения F , определяемого системой попарно противоречивых подстановок $s_1, \dots, s_m$ степени n , $1 \leq d \leq n$.

При заданных попарно противоречивых подстановках $s_1, \dots, s_m$, фиксированном d -множестве Y , $Y \subseteq X$, для случайной подстановки $s \in S_n$ определим md случайных событий

$$A_{ij} = \{s(j) = s_i(j)\}, \quad i = 1, 2, \dots, m, \quad j \in Y. \quad (38)$$

События $A_{i_1 j_1}, \dots, A_{i_k j_k}$, $1 \leq i_1, \dots, i_k \leq m$, $j_1, j_2, \dots, j_k \in Y$, называются совместными, по отношению к d -сужению отображения F , определяемого попарно противоречивыми подстановками $s_1, \dots, s_m$, если

$$s(j_1) = s_{i_1}(j_1), \dots, s(j_k) = s_{i_k}(j_k).$$

В противном случае события $A_{i_1 j_1}, \dots, A_{i_k j_k}$ называются несовместными.

Нетрудно видеть, что если события $A_{i_1 j_1}, \dots, A_{i_k j_k}$ совместны, то

$$\mathbf{P}(A_{i_1 j_1} \cap \dots \cap A_{i_k j_k}) = \frac{(n-k)!}{n!}, \quad (39)$$

в противном случае эта вероятность равна нулю.

Таким образом, если

$$S_k(n, m, d) = \sum_{1 \leq i_1, \dots, i_k \leq m, j_1, \dots, j_k \in Y} \mathbf{P}(A_{i_1 j_1} \cap \dots \cap A_{i_k j_k}), \quad (40)$$

то

$$S_k(n, m, d) = R_k(n, m, d) \frac{(n-k)!}{n!}, \quad (41)$$

где $R_k(n, m, d)$ — число способов выбора совокупностей, состоящих из k -совместных событий из общего множества вида (38).

Теорема 3. Точное распределение случайной величины $\eta_{nm}(d)$ имеет вид

$$\mathbf{P}(\eta_{nm}(d) = r) = \sum_{k=r}^d (-1)^{k-r} \binom{k}{r} R_k(n, m, d) \frac{(n-k)!}{n!}, \quad r = 0, 1, \dots, d. \quad (42)$$

Формула (42) находится путем стандартного применения метода включения-исключения [9].

Случайная величина η_{nm} , значения которой для случайной подстановки s из S_n определяются равенством

$$\eta_{nm} = |\{j: \{s(j) = s_1(j)\} \cup \dots \cup \{s(j) = s_m(j)\}, 1 \leq j \leq n\}|,$$

называется числом мест непротиворечивости подстановки s с попарно противоречивыми подстановками $s_1, \dots, s_m$. В этом случае события вида (38) определяются для всех $i = 1, 2, \dots, m$ и $j = 1, 2, \dots, n$, а число совместных событий обозначается через $R_k(n, m)$.

Следствие 6. Точное распределение случайной величины η_{nm} определяется формулой

$$\mathbf{P}(\eta_{nm} = r) = \sum_{k=r}^n (-1)^{k-r} \binom{k}{r} R_k(n, m) \frac{(n-k)!}{n!}, \quad r = 0, 1, \dots, n. \quad (43)$$

Формула (43) следует из формулы (42) при $d = n$. Формула (43) следует из известных результатов [3, 4], хотя значения $R_k(n, m)$ для любых противоречивых подстановок $s_1, \dots, s_m$ имеют удобные формулы только при $m \leq 2$. Например, при $m = 1$

$$R_k(n, 1) = \binom{n}{k}$$

и, следовательно,

$$\mathbf{P}(\eta_{n1} = r) = \frac{1}{r!} \sum_{k=0}^{n-r} \frac{(-1)^k}{k!}, \quad r = 0, 1, \dots, n. \quad (44)$$

Для $m = 2$ формулу можно найти в книге [7].

Из формулы (42) находим распределение для соответствующей случайной величины $\eta_{n1}(d)$

$$\mathbf{P}(\eta_{n1}(d) = r) = \frac{1}{r!} \sum_{k=0}^{d-r} \frac{(-1)^k}{k!} \frac{(d)_{k+r}}{(n)_{k+r}}, \quad r = 0, 1, \dots, d. \quad (45)$$

Теорема 4. При $n \rightarrow \infty$, $dm/n \rightarrow \lambda$, $m/d \rightarrow 0$ случайная величина $\eta_{nm}(d)$, равная числу мест непротиворечивости случайной подстановки $s \in S_n$ с d -сужением попарно противоречивых подстановок $s_1, \dots, s_m \in S_n$, имеет в пределе распределение Пуассона с параметром λ .

Доказательство. Известно, что для k -го биномиального момента $B_k(n, m, d)$ случайной величины $\eta_{nm}(d)$ имеет место равенство [10]

$$B_k(n, m, d) = S_k(n, m, d), \quad k = 0, 1, \dots, d, \quad (46)$$

то есть для его вычисления можно использовать формулу (41). В этой формуле найдем оценку сверху и снизу для величин $R_k(n, m, d)$.

Заметим, что в силу противоречивости подстановок s_μ и s_ν , $\mu \neq \nu$, $1 \leq \mu, \nu \leq m$, для совместности событий $A_{\mu i}$ и $A_{\nu j}$ необходимо выполнение условия $i \neq j$. Отсюда следует оценка сверху

$$R_k(n, m, d) \leq \binom{d}{k} m^k, \quad k = 0, 1, \dots, d. \quad (47)$$

Далее, заметим, что при выполнении условия $i \neq j$ события $A_{\mu i}$ и $A_{\nu j}$ совместны тогда и только тогда, когда $s_\mu(i) \neq s_\nu(j)$. Отсюда следует оценка снизу

$$R_k(n, m, d) \geq \frac{1}{k!} dm(dm - m^2) \dots (dm - (k - 1)m^2). \quad (48)$$

Из неравенств (47) и (48) находим, что

$$\frac{(dm)^k}{k!} \left(1 - \frac{mk^2}{d}\right) \leq R_k(n, m, d) \leq \frac{(dm)^k}{k!}, \quad k = 0, 1, \dots, d, \quad 1 \leq d \leq n. \quad (49)$$

Из формулы (41), равенства (46) и оценок (49) следует, что при выполнении условий теоремы выполнено соотношение

$$B_k(n, m, d) \rightarrow \frac{\lambda^k}{k!} \quad (50)$$

для любого фиксированного $k = 0, 1, \dots$. Отсюда следует справедливость теоремы 4.

Следствие 7. При $n \rightarrow \infty$ и любом фиксированном m случайная величина η_{nm} имеет в пределе распределение Пуассона с параметром $\lambda = m$.

Следствие 7 вытекает из теоремы 4 при $d = n$, так как для биномиальных моментов $B_k(n, m)$ случайной величины η_{nm} при $n \rightarrow \infty$ выполнено соотношение

$$B_k(n, m) \rightarrow \frac{m^k}{k!}, \quad k = 0, 1, \dots \quad (51)$$

Следствие 8. При $n \rightarrow \infty$ и любом фиксированном m для числа $L(m, n)$ латинских прямоугольников размера $m \times n$ имеет место асимптотическая формула

$$L(m, n) = (n!)^m e^{-\binom{m}{2}} (1 + o(1)). \quad (52)$$

Доказательство. Латинскому прямоугольнику размера $m \times n$ ставится в соответствие упорядоченная совокупность из m попарно противоречивых подстановок $[s_1, s_2, \dots, s_m]_n$ степени n . В соответствии с теоремой существования латинских

прямоугольников [8] для любого латинского прямоугольника $[s_1, s_2, \dots, s_{m-1}]_n$ существует такая подстановка s_m степени n , противоречивая с каждой из подстановок $s_1, \dots, s_{m-1}$, что присоединение s_m к $[s_1, \dots, s_{m-1}]_n$ дает латинский прямоугольник $[s_1, s_2, \dots, s_m]_n$. Если $N_n(s_1, \dots, s_{m-1})$ — число способов выбора таких подстановок s_m , то

$$L(m, n) = \sum_{s_1, \dots, s_{m-1}} N_n(s_1, \dots, s_{m-1}), \quad (53)$$

где суммирование проводится по всем упорядоченным совокупностям $s_1, \dots, s_{m-1}$ попарно противоречивых подстановок степени n .

Из следствия 7 вытекает, что при $n \rightarrow \infty$ при любом фиксированном m

$$N_n(s_1, \dots, s_{m-1}) = n! \mathbf{P}(\eta_{nm} = 0) = n! e^{-(m-1)} (1 + o(1)). \quad (54)$$

Из равенств (53) и (54) получаем соотношение

$$L(m, n) = n! e^{-(m-1)} L(m-1, n) (1 + o(1)). \quad (55)$$

Применяя это соотношение многократно, приходим к формуле (52).

Формула (52) получена в работах [5, 6] для $m < n^{1/3-\varepsilon}$, $0 < \varepsilon < 1/3$. Оказывается, что соотношение (55) можно получить и для таких значений m , применяя использованный выше подход. Точнее говоря, можно показать, что при $n \rightarrow \infty$

$$L(m, n) = n! e^{-(m-1)} L(m-1, n) \left(1 + O\left(\frac{1}{n^\varepsilon}\right) \right), \quad (56)$$

для $m < n^{1/3-\varepsilon}$, $0 < \varepsilon < 1/3$. К сожалению, в данном случае из соотношения (56) не удастся получить при таких значениях m асимптотику вида (52) ввиду возрастания относительной погрешности в процессе многократного применения соотношения (56).

Для вывода соотношения (56) из формулы (43), применяя неравенство Бонферони, имеем

$$\left| \mathbf{P}(\eta_{nm} = 0) - \sum_{k=0}^{t-1} (-1)^k R_k(n, m) \frac{(n-k)!}{n!} \right| \leq R_t(n, m) \frac{(n-t)!}{n!}.$$

Из неравенства (47) при $d = n$ получаем оценку сверху

$$R_k(n, m) \frac{(n-k)!}{n!} \leq \frac{m^k}{k!}, \quad k = 0, 1, \dots, n.$$

Из оценки (48) при $d = n$ получаем оценку снизу

$$R_k(n, m) \frac{(n-k)!}{n!} \geq \frac{m^k}{k!} \left(1 - \frac{mk^2}{n} \right), \quad k = 0, 1, \dots, n.$$

Возьмем $t = [n^{1/3}]$. Тогда равномерно для всех $k = 0, 1, \dots, t-1$

$$R_k(n, m) \frac{(n-k)!}{n!} = \frac{m^k}{k!} \left(1 + O\left(\frac{1}{n^\varepsilon}\right) \right).$$

Кроме того, при $t = [n^{1/3}]$

$$R_t(n, m) \frac{(n-t)!}{n!} = O\left(\frac{1}{n^{\varepsilon n^{1/3}}}\right).$$

Таким образом, для $m = n^{1/3-\varepsilon}$, $0 < \varepsilon < 1/3$,

$$\mathbf{P}(\eta_{nm} = 0) = \sum_{k=0}^{[n^{1/3}]-1} (-1)^k \frac{m^k}{k!} \left(1 + O\left(\frac{1}{n^{\varepsilon}}\right)\right) + O\left(\frac{1}{n^{\varepsilon n^{1/3}}}\right).$$

Отсюда с учетом оценки

$$\sum_{n=[n^{1/3}]+1}^{\infty} \frac{m^k}{k!} \leq \frac{1}{n^{\varepsilon n^{1/3}}} \frac{n^{\varepsilon}}{n^{\varepsilon} - 1}$$

получаем, что

$$\mathbf{P}(\eta_{nm} = 0) = e^{-m} \left(1 + O\left(\frac{1}{n^{\varepsilon}}\right)\right) + O\left(\frac{1}{n^{\varepsilon n^{1/3}}}\right).$$

Теперь, используя равенство (53) и асимптотику

$$N_n(s_1, \dots, s_m) = n! e^{-(m-1)} \left(1 + O\left(\frac{1}{n^{\varepsilon}}\right)\right),$$

получаем соотношение (56).

Список литературы

1. Joni S. A., Rota G.-C. A vector space analog of permutations with restricted positions. *J. Comb. Theory, Ser. A* (1980) **29**, 59–73.
2. Rota G.-C. On the foundations of combinatorial theory I: theory of Möbius inversion. *Zeitschrift Wahrscheinlichkeitstheorie und Verw. Gebiete* (1964) **2**, 340–368.
3. Kaplansky J. Symbolic solution of certain problems in permutations. *Bull. Amer. Math. Soc.* (1944) **50**, 906–914.
4. Kaplansky J., Riordan J. The problem of rooks and its applications. *Duke Math. J.* (1946) **13**, 259–268.
5. Erdős P., Kaplansky J. The asymptotic number of Latin rectangles. *Amer. J. Math.* (1946) **68**, 230–236.
6. Yamamoto K. On asymptotic number of Latin rectangles. *Japan J. Math.* (1951) **21**, 113–119.
7. Риордан Дж. *Введение в комбинаторный анализ*. ИЛ, Москва, 1963.
8. Холл М. *Комбинаторика*. Мир, Москва, 1970.
9. Сачков В. Н. *Комбинаторные методы дискретной математики*. Наука, Москва, 1977.
10. Сачков В. Н. *Вероятностные методы в комбинаторном анализе*. Наука, Москва, 1978.
11. Сачков В. Н. *Введение в комбинаторные методы дискретной математики*. Наука, Москва, 1982.

Статья поступила 11.03.1997.