Math-Net.Ru
All Russian mathematical portal

G. I. Ivchenko, Yu. I. Medvedev, Extremal characteristics of random polynomial over a finite field,
Tr. Diskr. Mat., 2001, Volume 4, 71–82

https://www.mathnet.ru/eng/tdm56

Use of the all-Russian mathematical portal Math-Net.Ru implies that you have read and agreed to these terms of use
https://www.mathnet.ru/eng/agreement

Download details:
IP: 18.97.14.86
January 17, 2026, 15:45:13

Труды по дискретной математике
Том 4, с. 71 – 82
М.: ФИЗМАТЛИТ, 2001

ЭКСТРЕМАЛЬНЫЕ ХАРАКТЕРИСТИКИ СЛУЧАЙНОГО МНОГОЧЛЕНА НАД КОНЕЧНЫМ ПОЛЕМ

Г.И. ИВЧЕНКО, Ю.И. МЕДВЕДЕВ

Для случайного многочлена

$$f_n(x) = x^n + a_1 x^{n-1} + \ldots + a_n$$

с коэффициентами из конечного поля $\mathbf{GF}(q)$, выбираемого с равной вероятностью из множества всех q^n таких многочленов, исследуются асимптотические при $n \to \infty$ распределения экстремальных характеристик, связанных с его каноническим разложением в произведение неприводимых множителей (типа максимальной кратности, максимальной и минимальной степени множителей и др.).

§ 1. ВВЕДЕНИЕ

Рассматриваются нормированные (т.е. со старшим коэффициентом 1) многочлены степени n над произвольным конечным полем $\mathbf{GF}(q)$ ($q \geq 2$ — простое число или степень простого числа). Пусть

$$f_n(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n, \quad a_i \in \mathbf{GF}(q),$$

есть случайный многочлен, выбранный с равной вероятностью из множества всех q^n таких многочленов, и

$$f_n(x) = \prod_{i=1}^{n} \prod_{j=1}^{s_i} \Phi_{ij}^{k_{ij}(n)}(x) \tag{1.1}$$

есть его каноническое разложение в произведение неприводимых (над полем $\mathbf{GF}(q)$) сомножителей. Здесь $\Phi_{i1}, \ldots, \Phi_{is_i}$ — занумерованные в произвольном порядке все нормированные неприводимые многочлены степени i, $s_i = s_i(q)$ — число таких многочленов и $k_{ij}(n)$ — кратность вхождения Φ_{ij} в (1.1). Набор этих кратностей образует таблицу $\mathcal{K}_n = \{k_{ij}(n), i = 1, \ldots, n, j = 1, \ldots, s_i\}$, называемую *локальной структурой* (ЛС) многочлена f_n. Любой функционал от $\mathcal{K}_n$ называется его *структурной характеристикой*.

Понятие локальной структуры введено в предыдущих работах авторов [1, 2], где исследованы (в точной и асимптотической при $n \to \infty$ постановках) свойства распределений ряда структурных характеристик случайного многочлена f_n, а также изложена история вопроса и приведена соответствующая библиография. Настоящая работа явля-

© Г.И. Ивченко, Ю.И. Медведев, 2001

ется продолжением этих исследований и посвящена анализу экстремальных характеристик ЛС $\mathcal{K}_n$.

В модели случайного многочлена $f_n(x)$ имеются два типа экстремальных характеристик, связанных с его каноническим разложением (1.1): экстремальные (т.е. минимальное и максимальное) значения степеней неприводимых множителей, присутствующих в разложении (1.1), и экстремальные значения кратностей этих множителей. Чтобы перейти к точным формулировкам, введем некоторые понятия и обозначения.

Сами элементы таблицы $\mathcal{K}_n$, т. е. случайные величины (с. в.) $k_{ij}(n)$, называются *локальными кратностями*, а их суммы по строкам

$$k_i(n) = \sum_{j=1}^{s_i} k_{ij}(n), \quad i = 1, \dots, n,$$

— интегральными кратностями (так что $k_i(n)$ — это общее число множителей (с учетом кратностей) степени i в (1.1));

$$L_r(n) = \sum_{i=1}^{n} \mathrm{I}\left(k_i(n) \geq r\right)$$

— число степеней, представленных в (1.1) по крайней мере r сомножителями каждая, в частности, $L_1(n)$ — число различных степеней, присутствующих в (1.1) (здесь и далее $\mathrm{I}(A)$ — индикатор события A);

$$M_r(n) = L_r(n) - L_{r+1}(n) = \sum_{i=1}^{n} \mathrm{I}\left(k_i(n) = r\right)$$

— число степеней, представленных ровно r сомножителями каждая, $r = 1, 2, \dots$

Все указанные характеристики детально исследованы в работе [2]. Объектами внимания в данной статье будут следующие характеристики: максимальная кратность в ЛС $\mathcal{K}_n$

$$\overline{k}(n) = \max_{i,j} k_{ij}(n),$$

вариационный ряд интегральных кратностей, получаемый расположением чисел $k_i(n)$, $i = 1, \dots n$, в порядке их возрастания

$$k_{(1)}(n) \leq k_{(2)}(n) \leq \dots \leq k_{(n)}(n),$$

минимальная степень неприводимого многочлена в (1.1)

$$J_{\min}(n) = \min\left\{i\colon\ k_i(n) \neq 0\right\},$$

максимальная степень неприводимого многочлена в (1.1)

$$J_{\max}(n) = \max\left\{i\colon\ k_i(n) \neq 0\right\},$$

вариационный ряд различных степеней неприводимых множителей в разложении (1.1)

$$J_{\min}(n) \equiv J_{(1)}(n) < J_{(2)}(n) < \dots < J_{\max}(n),$$

число множителей, соответственно, с минимальной и максимальной степенью $k_{\min}(n)$ и $k_{\max}(n)$.

При исследовании этих структурных характеристик мы будем существенно опираться на результаты работы [2], где, в частности, установлены следующие общие особенности асимптотического строения ЛС $\mathcal{K}_n$: ее верхняя зона $\mathcal{K}_{n,b} = \{k_{ij}(n), i \leq b\}$

до уровней $b = O(n/\ln n)$ асимптотически при $n \to \infty$ устроена так же, как соответствующая совокупность $\mathcal{K}_b^l = \{k_{ij},\, i = 1, \ldots, b,\, j = 1, \ldots, s_i\}$ независимых с. в., где с. в. k_{ij}, расположенные в строке $i, i = 1, \ldots, b$, имеют геометрическое распределение с параметром q^{-i},

$$\mathbf{P}\{k_{ij} = r\} = q^{-ir}(1 - q^{-i}), \quad r = 0, 1, \ldots .$$

В нижней же зоне $\mathcal{K}_n^b = \{k_{ij}(n), i > b\}$ для таких уровней b, что $b = b(n) \to \infty$ при $n \to \infty$, с вероятностью, стремящейся к 1, присутствуют лишь нули и единицы, причем ненулевых элементов будет относительно немного (порядка $\ln(n/b)$) и они будут разбросаны по разным строкам. Если же уровень b имеет порядок $n (b \sim \alpha n, 0 < \alpha < 1)$, то число ненулевых строк в $\mathcal{K}_n^b$

$$L_1^b(n) = \sum_{i>b}^{n} I\left(k_i(n) \geq 1\right)$$

имеет в пределе некоторое дискретное распределение со средним $-\ln \alpha$, именно,

$$\mathbf{P}\left\{L_1^b(n) \leq m - 1\right\} \to F_m(\alpha) = 1 - \sum_{m \leq k < 1/\alpha} \frac{(-1)^{k-m}}{k(m-1)!(k-m)!} J_k(\alpha), \quad 1 \leq m \leq 1/\alpha, \tag{1.2}$$

где

$$J_k(\alpha) = \int\limits_{\substack{x_1 + \ldots + x_k \leq 1, \\ x_1, \ldots, x_k \geq \alpha}} \frac{dx_1 \ldots dx_k}{x_1 \ldots x_k}, \quad k = 1, 2, \ldots$$

Далее, общее число $L_1(n)$ ненулевых строк в $\mathcal{K}_n$ так же, как и число $M_1(n)$ строк лишь с одной единицей, асимптотически нормально $\mathcal{N}(\ln n, \ln n)$, а с. в. $L_r(n)$ и $M_r(n)$ при $r \geq 2$ сходятся по распределению при $n \to \infty$ к собственным с. в., соответственно,

$$L_r = \sum_{i=1}^{\infty} \mathrm{I}\left(k_i \geq r\right), \qquad M_r = \sum_{i=1}^{\infty} \mathrm{I}\left(k_i = r\right), \tag{1.3}$$

где

$$k_i = \sum_{j=1}^{s_i} k_{ij}, \quad i = 1, 2, \ldots$$

Добавим к этому еще, что маргинальные распределения локальных кратностей $k_{ij}(n)$ имеют вид

$$\mathbf{P}\{k_{ij}(n) \geq s\} = q^{-is}\mathrm{I}(is \leq n), \tag{1.4}$$

а числа s_i удовлетворяют неравенству $is_i < q^i$, которое становится асимптотическим равенством, когда $i \to \infty$.

§ 2. ПРЕДЕЛЬНОЕ РАСПРЕДЕЛЕНИЕ МАКСИМАЛЬНОЙ КРАТНОСТИ

Содержание данного раздела составляет доказательство следующего утверждения.

ТЕОРЕМА 1. *Если $n \to \infty$, то для любого фиксированного целого $r \geq 2$*

$$\mathbf{P}\left\{\overline{k}(n) < r\right\} \to 1 - q^{-r+1}. \tag{2.1}$$

Введем с. в.

$$D_r(n) = \sum_{i=1}^{n} \sum_{j=1}^{s_i} \mathrm{I}\left(k_{ij}(n) \geq r\right), \quad r \geq 2,$$

представляющую собой число элементов ЛС $\mathcal{K}_n$, принявших значение, не меньшее r, и аналогичную с. в.

$$D_r = \sum_{i=1}^{\infty} \sum_{j=1}^{s_i} \mathrm{I}\left(k_{ij} \geq r\right)$$

для бесконечной совокупности $\mathcal{K}' = \{k_{ij},\, i = 1, 2, \ldots,\, j = 1, \ldots, s_i\}$ независимых геометрически распределенных с. в. и докажем предварительно следующую лемму.

Лемма. *Если $n \to \infty$, то для любого фиксированного целого $r \geq 2$*

$$\mathcal{L}\left(D_r(n)\right) \to \mathcal{L}\left(D_r\right).$$

Доказательство. Прежде всего отметим, что по теореме о двух рядах (см., например, [3, с. 373]) D_r является собственной с. в., поскольку ряд из дисперсий слагаемых в данном случае мажорируется рядом из соответствующих средних, который, в свою очередь, сходится:

$$\sum_{i=1}^{\infty} \sum_{j=1}^{s_i} \mathbf{P}\left\{k_{ij} \geq r\right\} = \sum_{i=1}^{\infty} s_i q^{-ri} < \sum_{i=1}^{\infty} \frac{1}{i} q^{-(r-1)i} < \infty.$$

Рассмотрим далее поведение части суммы $D_r(n)$ при больших i, правый хвост для $D_r(n)$,

$$D_r^b(n) = \sum_{i>b}^{n} \sum_{j=1}^{s_i} \mathrm{I}\left(k_{ij}(n) \geq r\right)$$

и аналогичный правый хвост D_r^b для D_r. Поскольку (см. (1.4))

$$\mathbf{P}\left\{D_r^b(n) > 0\right\} \leq \mathbf{E}\, D_r^b(n) = \sum_{i>b} s_i\, \mathbf{P}\left\{k_{ij}(n) \geq r\right\} \leq \sum_{i>b} s_i q^{-ri},$$

по предыдущему, эта вероятность может быть сделана сколь угодно малой за счет выбора b. Аналогичное заключение, очевидно, справедливо и для D_r^b.

Таким образом, достаточно показать, что распределения с. в.

$$D_r(n) - D_r^b(n) = \sum_{i \leq b} \sum_{j=1}^{s_i} \mathrm{I}\left(k_{ij}(n) \geq r\right)$$

и аналогичной с. в. $D_r - D_r^b$ близки при больших n для всех b, в том числе и растущих вместе с n. Это следует из отмеченного выше факта асимптотической близости распределений совокупностей $\mathcal{K}_{n,b}$ и $\mathcal{K}'_b$ при $b = O\left(n/\ln n\right)$. Лемма доказана.

Доказательство теоремы 1 следует теперь из цепочки соотношений

$$\mathbf{P}\left\{\overline{k}(n) < r\right\} = \mathbf{P}\left\{k_{ij}(n) < r \forall (i,j)\right\} = \mathbf{P}\left\{D_r(n) = 0\right\} \to$$

$$\to \mathbf{P}\left\{D_r = 0\right\} = \prod_{i=1}^{\infty} \prod_{j=1}^{s_i} \mathbf{P}\left\{k_{ij} < r\right\} = \prod_{i=1}^{\infty} (1 - q^{-ri})^{s_i}$$

и тождества (см. [1])

$$\prod_{i=1}^{\infty}\left(1-\left(\frac{z}{q}\right)^{i}\right)^{s_i}=1-z, \quad |z|<1.$$

Теорема 1 позволяет, в частности, оценить вероятность того, что случайный многочлен f_n будет свободен от квадратов, т.е. будет раскладываться в произведение различных неприводимых множителей. Это событие эквивалентно событию $\{\overline{k}(n)=1\}$ (линейная структура $\mathcal{K}_n$ будет состоять лишь из 0 и 1), поэтому из (2.1) при $r=2$ следует, что

$$\mathbf{P}\{f_n \text{ свободен от квадратов }\} \to 1-\frac{1}{q}.$$

Общий результат (2.1) можно интерпретировать как асимптотическое соотношение для вероятности события, состоящего в том, что f_n свободен от r кратностей.

Добавим к сказанному еще несколько достаточно простых утверждений относительно

$$\overline{k}_i(n)=\max_j k_{ij}(n), \quad i=1,2,\ldots,$$

— максимальных кратностей множителей степени i в каноническом разложении случайного многочлена f_n. Ясно, что асимптотическое распределение с. в. $\overline{k}_i(n)$ такое же, как распределение с. в. $\overline{k}_i$ — максимума s_i независимых одинаково распределенных геометрических с параметром q^{-i} с. в., т. е. для любого фиксированного целого $r\geq 1$

$$\mathbf{P}\left\{\overline{k}_i<r\right\} \to \mathbf{P}\left\{\overline{k}_i<r\right\}=\left(1-q^{-ir}\right)^{s_i}. \tag{2.2}$$

Отметим, что с. в. $\overline{k}_i$ стохастически убывает с ростом индекса i (более вероятно, что бо́льшие кратности будут иметь множители меньших степеней), и с ростом i с. в. $\overline{k}_i$ вырождается в 0; более точно, при $n\to\infty$

$$\mathbf{P}\left\{\overline{k}_i=0\right\}=1-\frac{1}{i}+o\left(\frac{1}{i}\right).$$

§ 3. АСИМПТОТИЧЕСКОЕ СТРОЕНИЕ ВАРИАЦИОННОГО РЯДА ИНТЕГРАЛЬНЫХ КРАТНОСТЕЙ

В этом разделе мы рассматриваем вариационный ряд (в. р.)

$$k_{(1)}(n)\leq\ldots\leq k_{(n-m+1)}(n)\leq\ldots<k_{(n)}(n) \tag{3.1}$$

интегральных кратностей $k_i(n), i=1,\ldots,n$. Для m-го максимума $k_{(n-m+1)}(n)$ можно записать соотношение

$$\mathbf{P}\left\{k_{(n-m+1)}(n)<r\right\}=\mathbf{P}\left\{L_r(n)<m\right\}, \tag{3.2}$$

справедливое для любых натуральных m и r. Действительно, событие $\left\{k_{(n-m+1)}(n)\geq r\right\}$ означает, что среди чисел $k_i(n), i=1,\ldots,n$, найдется по крайней мере m чисел, больших либо равных r, что совпадает с событием

$$\left\{\sum_{i=1}^{n}\mathrm{I}\left(k_i(n)\geq r\right)\geq m\right\}.$$

Соотношение (3.2) позволяет перенести изложенные во введении результаты для с. в. $L_r(n)$ на в.р. (3.1) и описать его асимптотическое строение.

Прежде всего отметим, что в ряду (3.1) будут идти сначала нули, именнотак будет, когда $m = m(n)$ удовлетворяет условию $(m - \ln n)/\sqrt{\ln n} \to \infty$. Действительно, из асимптотической нормальности $\mathcal{N}(\ln n, \ln n)$ с.в $L_1(n)$ и (3.2) при $r = 1$ следует, что для таких значений m

$$\mathbf{P}\left\{k_{(n-m+1)}(n) = 0\right\} = \mathbf{P}\left\{\frac{L_1(n) - \ln n}{\sqrt{\ln n}} < \frac{m - \ln n}{\sqrt{\ln n}}\right\} \to 1.$$

Отрыв от нуля, т.е. появление единицы в в.р. (3.1) будет наблюдаться лишь при значениях $m = \ln n + x\sqrt{\ln n}$, $|x| \le c < \infty$, так как тогда

$$\mathbf{P}\left\{k_{(n-m+1)}(n) = 0\right\} \sim \Phi(x) = \frac{1}{\sqrt{2\pi}} \int\limits_{-\infty}^{x} e^{-t^2/2} dt,$$

т.е. с положительной вероятностью $1 - \Phi(x)$ с. в. $k_{(n-m+1)}(n)$ принимает (асимптотически) положительные значения. Наконец, члены ряда (3.1) становятся положительными, когда $(m - \ln n)/\sqrt{\ln n} \to -\infty$. Проанализируем теперь, как устроена эта зона ряда (3.1). Здесь в силу (3.2) при $r = 2$

$$\mathbf{P}\left\{k_{(n-m+1)}(n) \le 1\right\} = \mathbf{P}\left\{L_2 < m\right\} \sim \mathbf{P}\left\{L_2(n) < m\right\} \to 1,$$

если $m = m(n) \to \infty$ как угодно медленно, поскольку предельная с. в. L_2 (см. (1.3)) является собственной. Таким образом, за исключением лишь некоторого числа крайних правых членов, остальные члены ряда (3.1) в рассматриваемой зоне будут равны 1. Значения же, большие 1, асимптотически с положительной вероятностью могут присутствовать лишь на правом краю ряда (3.1). Более точно, при $n \to \infty$ для фиксированных $m \ge 1$

$$\mathbf{P}\left\{k_{(n-m+1)}(n) < r\right\} = \mathbf{P}\left\{L_r < m\right\}, \quad r \ge 2, \tag{3.3}$$

где с. в. L_r определена в (1.3). В частности, для максимальной кратности $k_{(n)}(n)$ имеет место предельное соотношение

$$\mathbf{P}\left\{k_{(n)}(n) < r\right\} \to \mathbf{P}\left\{L_r = 0\right\} = \mathbf{P}\left\{k_i < r\ \forall i\right\} =$$
$$= \prod_{i=1}^{\infty} \mathbf{P}\left\{k_i < r\right\} = \prod_{i=1}^{\infty} \sum_{j<r} \binom{s_i + j - 1}{j} q^{-ij}(1 - q^{-i})^{s_i},$$

а вероятность того, что весь ряд (3.1) состоит лишь из 0 и 1, есть

$$\mathbf{P}\left\{k_{(n)}(n) = 1\right\} \to \mathbf{P}\left\{L_2 = 0\right\} = \prod_{i=1}^{\infty} (1 - q^{-i})^{s_i}(1 + s_i q^{-i}) = a(q), \tag{3.4}$$

при этом

$$a(2) = 0{,}4039\ldots, \quad a(3) = 0{,}48349\ldots$$

Последний результат можно также интерпретировать как асимптотическое представление вероятности события, состоящего в том, что f_n раскладывается в произведение различных, множителей различных степеней.

Добавим к сказанному, что число членов ряда (3.1) на его правом краю, принявших значение r, есть с. в. $M_r(n)$, имеющая собственный предел M_r, указанный в (1.3), $r = 2, 3, \ldots$

Подведем итог в виде следующего утверждения.

ТЕОРЕМА 2. *Если $n \to \infty$, то первые $n - \ln n + x\sqrt{\ln n}$ членов ряда* (3.1) *при $x = x(n) \to -\infty$ с вероятностью, стремящейся к единице, принимают значение* 0; *при $|x| \le c < \infty$*

$$\mathbf{P}\left\{k_{(n-\ln n+x\sqrt{\ln n})}(n) = 0\right\} \sim 1 - \mathbf{P}\left\{k_{(n-\ln n+x\sqrt{\ln n})}(n) = 1\right\} \sim \Phi(-x);$$

при $x \to \infty$, $\ln n - x\sqrt{\ln n} \to \infty$

$$\mathbf{P}\left\{k_{(n-\ln n+x\sqrt{\ln n})}(n) = 1\right\} \to 1;$$

наконец, при фиксированном $m \ge 1$ для с. в. $k_{(n-m+1)}(n)$ выполняется предельное соотношение (3.3).

Из этой теоремы следует, что важнейшими характеристиками ряда (3.1) являются номера первой η_n и последней $\varkappa_n$ единиц в нем. Поскольку, очевидно, $\eta_n = n - L_1(n) + 1$, $\varkappa_n = n - L_2(n)$, для этих с. в. при $n \to \infty$ выполняются соотношения

$$\mathcal{L}\left(\frac{n - \ln n - \eta_n}{\sqrt{\ln n}}\right) \to \mathcal{N}(0,1) \qquad \text{и} \qquad \mathbf{P}\{n - \varkappa_n = s\} \to \mathbf{P}\{L_2 = s\} \tag{3.5}$$

при любых фиксированных $s = 0, 1, \ldots$ В частности, $\mathbf{P}\{\varkappa_n = n\}$ имеет предел $a(q)$, указанный в (3.4).

В этих терминах строение ряда (3.1) можно описать следующим образом: первые $\eta_n - 1 = n - L_1(n)$ его членов являются нулевыми, затем идут $\varkappa_n - \eta_n + 1 = L_1(n) - L_2(n) = M_1(n)$ членов, равных единице, затем (при условии, что $\varkappa_n < n$) $M_2(n)$ двоек, $M_3(n)$ троек и т.д.; ряд заканчивается серией длины $M_r(n)$, состоящей из членов, равных r, если $k_{(n)}(n) = r \ge 2$. При этом длина $M_1(n)$ серии из единиц асимптотически нормальна $\mathcal{N}(\ln n, \ln n)$, ее начало η_n удовлетворяет асимптотическому соотношению (3.5), а финальные серии (когда они присутствуют) асимптотически конечны.

Наконец, отметим, что асимптотически ряд (3.1) устроен так же, как в.р. совокупности $\{k_1, k_2, \ldots, k_n\}$ независимых с. в., где (см. (1.3)) k_i имеет отрицательное биномиальное распределение с параметрами (s_i, q^{-i}), $i = 1, 2, \ldots$ Это следует из того, что все характеристики $L_r(n)$ и $M_r(n)$, $r \ge 1$ асимптотически распределены так же, как соответствующие характеристики совокупности $\{k_i, i = 1, \ldots, n\}$ (см. [2]).

§ 4. ВАРИАЦИОННЫЙ РЯД РАЗЛИЧНЫХ СТЕПЕНЕЙ КАНОНИЧЕСКОГО РАЗЛОЖЕНИЯ

Этот раздел посвящен асимптотическому анализу структуры ряда

$$J_1(n) < J_2(n) < \ldots < J_{L_1(n)}(n), \tag{4.1}$$

представляющему собой расположенные в возрастающем порядке значения степеней неприводимых множителей, присутствующих в каноническом разложении (1.1) случайного многочлена f_n. Согласно этому определению все члены ряда (4.1) различны, заключены между 1 и n и их число есть с. в.

$$L_1(n) = \sum_{i=1}^{n} I(k_i(n) \ge 1).$$

Приведем формальное определение этих чисел:

$$J_1(n) = J_{\min}(n) = \min\{i\colon\ k_i(n) \neq 0\},$$

$$J_m(n) = \min\{i > J_{m-1}(n)\colon\ k_i(n) \neq 0\}, \quad m = 2, 3, \ldots,$$

$$J_{L_1(n)}(n) = J_{\max}(n) = \max\{i\colon\ k_i(n) \neq 0\},$$

так что $J_{\min}(n)$ и $J_{\max}(n)$ — соответственно, минимальная и максимальная степень неприводимого множителя в каноническом разложении многочлена f_n.

Совместное распределение с. в. $J_j(n)$ имеет вид

$$\begin{aligned}&\mathbf{P}\{J_j(n) = r_j, j = 1, \ldots, m\} = \\ &\qquad = \mathbf{P}\{k_j(n) > 0, j = r_1, \ldots, r_m; k_i(n) = 0, i \neq r_1, \ldots, r_{m-1}, i < r_m\},\end{aligned} \tag{4.2}$$

где $m \geq 1$ и $1 \leq r_1 < \ldots < r_m \leq n$. Поскольку интегральные кратности $\{k_1(n), \ldots, k_b(n)\}$ при $b = O(n/\ln n)$ асимптотически независимы и при этом асимптотически с. в. $k_i(n)$ распределена как $k_i, i = 1, \ldots, b$, из (4.2) получаем вид предельного совместного распределения крайних левых членов ряда (4.1).

ТЕОРЕМА 3. *Для любых фиксированных натуральных m и $r_1 < r_2 < \ldots < r_m$ при $n \to \infty$*

$$\mathbf{P}\{J_j(n) = r_j, j = 1, \ldots, m\} \to \prod_{\substack{i=1\\ i\neq r_1,\ldots,r_{m-1}}}^{r_m-1} (1 - q^{-i})^{s_i} \prod_{j=1}^{m} \left(1 - (1 - q^{-r_j})^{s_{r_j}}\right).$$

Утверждение теоремы 3 для минимальной степени принимает вид

$$\mathbf{P}\{J_1(n) = r\} \to \prod_{i=1}^{r-1} (1 - q^{-i})^{s_i} \left(1 - (1 - q^{-r})^{s_r}\right), \quad r \geq 1,$$

или

$$\mathbf{P}\{J_1(n) \leq r\} \to 1 - \prod_{i=1}^{r} (1 - q^{-i})^{s_i}. \tag{4.3}$$

Отметим, что предельное распределение в (4.3) имеет бесконечное среднее, поскольку ряд

$$\sum_{r=1}^{\infty} \prod_{i=1}^{r} (1 - q^{-i})^{s_i},$$

как нетрудно видеть, расходится.

Рассмотрим более детально маргинальное распределение m-го минимального члена $J_m(n)$. Поскольку событие $\{J_m(n) > r\}$ означает, что среди первых r интегральных кратностей $k_i(n), i = 1, \ldots, r$, число положительных кратностей меньше m, то для любых натуральных m и r выполняется соотношение

$$\mathbf{P}\{J_m(n) \geq r\} = \mathbf{P}\left\{\sum_{i=1}^{r} \mathrm{I}(k_i(n) \geq 1) < m\right\}, \tag{4.4}$$

которое позволяет получить следующий результат.

ТЕОРЕМА 4. *Для любых фиксированных натуральных m и r при $n \to \infty$*

$$\mathbf{P}\{J_m(n) \le r\} = \mathbf{P}\left\{\sum_{i=1}^{r} \mathrm{I}(k_i \ge 1) \ge m\right\} + o(1).$$

При $m = 1$ этот результат может быть записан также в форме (4.3).

Соотношение (4.4) позволяет исследовать предельные распределения и средних членов ряда (4.1). Так как число $\mathcal{L}_1(n)$ членов ряда имеет порядок $\ln n$, под средними членами следует понимать с. в. $J_m(n)$ с номерами m порядка $t \ln n$, $0 < t < 1$. Для них справедлива теорема о логарифмической нормальности.

ТЕОРЕМА 5. *При $n \to \infty$ и $m = t \ln n + O(\sqrt{\ln n})$, $0 < t < 1$ с. в. $\ln J_m(n)$ асимптотически нормальна $\mathcal{N}(m, m)$.*

Доказательство. Положим

$$L_{1r}(n) = \sum_{i \le r} \mathrm{I}(k_i(n) \ge 1), \quad r = \exp\{m + x\sqrt{m}\}.$$

Как показано в работе [2], при $r = n^t$ с. в. $L_{1r}(n)$ асимптотически нормальна $\mathcal{N}(\ln r, \ln r)$, поэтому в рассматриваемом случае для любого фиксированного x из (4.4)

$$\mathbf{P}\left\{\frac{\ln J_m(n) - m}{\sqrt{m}} > \frac{\ln r - m}{\sqrt{m}} = x\right\} = \mathbf{P}\left\{\frac{L_{1r}(n) - \ln r}{\sqrt{\ln r}} < \frac{m - \ln r}{\sqrt{\ln r}} = -x + o(1)\right\},$$

что имеет своим пределом $\Phi(-x)$. Теорема доказана.

Перейдем теперь к рассмотрению максимальных членов ряда (4.1). Перепишем равенство (4.4) для m-го максимума $J'_m(n) = J_{L_1(n)-m+1}(n), m \ge 1$, в виде

$$\mathbf{P}\{J'_m(n) \le b\} = \mathbf{P}\left\{\sum_{i=1}^{b} \mathrm{I}(k_i(n) \ge 1) \ge L_1(n) - m + 1\right\} = \mathbf{P}\left\{L_1^b(n) \le m - 1\right\}, \tag{4.5}$$

где

$$L_1^b(n) = \sum_{i > b}^{n} \mathrm{I}(k_i(n) \ge 1).$$

Если $b = b(n)$ растет так, что $b \sim \alpha n$, $0 < \alpha < 1$, то с. в. $L_1^b(n)$ имеет предельное распределение, указанное в (1.2). Этот результат с учетом соотношения (4.5) позволяет сформулировать следующее общее утверждение об асимптотическом поведении распределений крайних правых членов ряда (4.1).

ТЕОРЕМА 6. *При $n \to \infty$ для любого фиксированного $m \ge 1$*

$$\mathbf{P}\left\{\frac{1}{n} J'_m(n) \le \alpha\right\} \to \begin{cases} F_m(\alpha), & 0 < \alpha < 1/m, \\ 1, & \alpha \ge 1/m, \end{cases}$$

где функция $F_m(\alpha)$ определена в (1.2).

В частности, для максимальной степени $J_{\max}(n) = J'_1(n)$ выполняется предельное соотношение

$$\mathbf{P}\left\{\frac{1}{n} J_{\max}(n) \le \alpha\right\} \to F_1(\alpha) = \begin{cases} 1 - \displaystyle\sum_{1 \le k < 1/\alpha} \frac{(-1)^{k-1}}{k!} J_k(\alpha), & 0 < \alpha < 1, \\ 1, & \alpha \ge 1. \end{cases} \tag{4.6}$$

Справедлива также и соответствующая локальная предельная теорема, многомерный вариант которой формулируется следующим образом.

ТЕОРЕМА 7. *Пусть* $r \geq 1$ *и* $0 < \alpha_r < \alpha_{r-1} < \ldots < \alpha_1 < 1$ *таковы, что* $0 < \alpha_1 + \ldots + \alpha_r < 1$. *Тогда*

$$\lim_{n\to\infty} n^r \mathbf{P}\left\{J_j'(n) = [n\alpha_j], j = 1, \ldots, r\right\} = \frac{1}{\alpha_1 \ldots \alpha_r} F_1\left(\frac{\alpha_r}{1 - \alpha_1 - \ldots - \alpha_r}\right), \quad (4.7)$$

где функция F_1 определена в (4.6).

Доказательство. Для любых целых $m_1, \ldots, m_r$, удовлетворяющих условиям

$$1 \leq m_r < m_{r-1} < \ldots < m_1 \leq n, \qquad m \equiv m_1 + \ldots + m_r \leq n,$$

справедливо соотношение

$$\mathbf{P}\left\{J_j'(n) = m_j, j = 1, \ldots, r\right\} = \\ = \mathbf{P}\left\{k_{m_j}(n) > 0, j = 1, \ldots, r; k_i(n) = 0, m_r < i \neq m_{r-1}, \ldots, m_1\right\}.$$

Как отмечено во введении, при $n \to \infty$ и $b = b(n) \to \infty$ в последовательности $\{k_i(n), i > b\}$ с вероятностью, стремящейся к единице, присутствуют лишь нули и единицы, и потому вероятность события $\{k_{m_j}(n) > 0, j = 1, \ldots, r\}$ при $n \to \infty$ и $m_r = m_r(n) \to \infty$ асимптотически эквивалентна вероятности события $\{k_{m_j}(n) = 1, j = 1, \ldots, r\}$. Поэтому достаточно оценить вероятность события

$$A_n = \left\{k_{m_j}(n) = 1, j = 1, \ldots, r; k_i(n) = 0, m_r < i \neq m_{r-1}, \ldots, m_1\right\}.$$

Совместная производящая функция интегральных кратностей $\{k_i(n), i \geq m_r\}$ имеет вид (см. [1])

$$\Phi(t_i, i \geq m_r) = \mathbf{E} \prod_{i \geq m_r} t_i^{k_i(n)} = [z^n] \frac{1}{1-z} \prod_{i \geq m_r} \left(\frac{1 - (z/q)^i}{1 - t_i (z/q)^i}\right)^{s_i},$$

где $[z^n] f(z) = \operatorname{coef}_{z^n} f(z)$. Следовательно,

$$\mathbf{P}\{A_n\} = \left.\frac{\partial^r \Phi(t_i, i \geq m_r)}{\partial t_{m_1} \ldots \partial t_{m_r}}\right|_{t_i = 0, i \geq m_r} = [z^n] \frac{1}{1-z} \prod_{j=1}^{r} s_{m_j} \left(\frac{z}{q}\right)^{m_j} \prod_{i \geq m_r} \left(1 - \left(\frac{z}{q}\right)^i\right)^{s_i} = \\ = \prod_{j=1}^{r} \frac{s_{m_j}}{q^{m_j}} [z^{n-m}] \frac{1}{1-z} \prod_{i \geq m_r} \left(1 - \left(\frac{z}{q}\right)^i\right)^{s_i}. \quad (4.8)$$

Заметим теперь, что результату (4.6) можно придать такую форму

$$\mathbf{P}\left\{J_1'(n) \leq [n\alpha]\right\} = \mathbf{P}\left\{k_i(n) = 0, i > [n\alpha]\right\} = \Phi\left(t_i, i > [n\alpha]\right)\big|_{t=0} = \\ = [z^n] \frac{1}{1-z} \prod_{i > [n\alpha]} \left(1 - \left(\frac{z}{q}\right)^i\right)^{s_i},$$

где последнее выражение стремится к $F_1(\alpha)$ при $n \to \infty$. Поэтому в условиях теоремы при $m_j = [n\alpha_j], j = 1, \ldots, r$, для второго сомножителя в (4.8) справедливо соотношение

$$[z^{n-m}] \frac{1}{1-z} \prod_{i > m_r} \left(1 - \left(\frac{z}{q}\right)^i\right)^{s_i} = \mathbf{P}\left\{J_1'(n-m) < m_r\right\} \to F_1\left(\frac{\alpha_r}{1 - \alpha_1 - \ldots - \alpha_r}\right).$$

Для первого же сомножителя выполняется асимптотическое соотношение

$$\prod_{j=1}^{r} \frac{s_{m_j}}{q^{m_j}} \sim \prod_{j=1}^{r} \frac{1}{m_j} \sim \frac{1}{n^r \alpha_1 \ldots \alpha_r},$$

что в итоге дает (4.7). Теорема доказана.

При $r = 1$ из (4.7) следует локальный вариант результата (4.6):

$$\lim_{n\to\infty} n\,\mathbf{P}\left\{J_{\max}(n) = [n\alpha]\right\} = \varphi(\alpha) = \frac{1}{\alpha} F_1\left(\frac{\alpha}{1-\alpha}\right), \quad 0 < \alpha < 1. \tag{4.9}$$

Из вида функции F_1 (см. (4.6)) следует, что при $1/2 \le \alpha < 1$ предельная плотность $\varphi(\alpha)$ в (4.9) есть α^{-1}, при $1/3 \le \alpha < 1/2$ она равна

$$\varphi(\alpha) = \frac{1}{\alpha}\left(1 - \ln\frac{1-\alpha}{\alpha}\right)$$

и, вообще, при $1/(s+1) \le \alpha < 1/s$

$$\varphi(\alpha) = \frac{1}{\alpha}\sum_{k=0}^{s-1} \frac{(-1)^k}{k!} J_k\left(\frac{\alpha}{1-\alpha}\right), \quad s = 1, 2, \ldots,$$

где $J_0(x) = 1$.

Таким образом, плотность $\varphi(\alpha)$ составляется из счетного множества аналитических дуг; впервые она встречается в работе [4] в качестве плотности предельного (при $n \to \infty$) распределения длины максимального цикла случайной подстановки степени n, которое имеет такой же вид, как (4.6).

Замечание 1. Соотношение (4.9) выполняется и при $\alpha = 1$, так как при $n \to \infty$

$$\mathbf{P}\left\{J_{\max}(n) = n\right\} = \frac{\psi_n}{q^n} \sim \frac{1}{n}.$$

Завершая анализ асимптотического строения ряда (4.1), отметим очевидный факт, что с вероятностью, стремящейся к 1 при $n \to \infty$, в разложении (1.1) присутствует лишь один сомножитель с максимальной степенью $J_{\max}(n)$, т.е. с. в. $k_{\max}(n)$ вырождается в точке 1.

Что касается числа $k_{\min}(n)$ множителей с минимальной степенью $J_{\min}(n)$, то аналогично теореме 3 легко устанавливается, что для любого фиксированного натурального k

$$\mathbf{P}\left\{k_{\min}(n) = k\right\} = \sum_{i\ge1} \mathbf{P}\left\{J_{\min}(n) = i, k_i(n) = k\right\} =$$
$$= \sum_{i\ge1} \binom{s_i + k - 1}{k} q^{-ik} \prod_{j=1}^{i} (1 - q^{-j})^{s_j} + o(1).$$

Предельное распределение имеет конечное среднее

$$\mu(q) = \sum_{i\ge1} \frac{s_i}{q^i - 1} \prod_{j=1}^{i-1} (1 - q^{-j})^{s_j}.$$

Таким образом, если минимальная степень $J_{\min}(n)$ в среднем неограниченно растет с ростом n, то число $k_{\min}(n)$ множителей с минимальной степенью в среднем остается конечной величиной.

Завершая анализ асимптотического поведения членов ряда (4.1), отметим, что результаты для средних и максимальных членов (теоремы 5 и 6) в данном случае оказались идентичными аналогичным результатам для вариационного ряда длин циклов случайной подстановки степени n, (см., например, [5]), в то время как асимптотическое поведение минимальных членов и минимальных длин циклов существенно различается.

Замечание 2. В рассматриваемой модели можно построить также в. р. всех

$$k(n) = \sum_{i=1}^{n} k_i(n)$$

степеней канонического разложения (1.1), т.е. учитывая каждую входящую в него степень столько раз, какова ее интегральная кратность. Это был бы ряд

$$\tilde{J}_1(n) \leq \tilde{J}_2(n) \leq \ldots \tilde{J}_{k(n)}(n), \tag{4.10}$$

в котором возможны совпадения соседних членов. Однако из приведенных выше результатов легко заключить, что при $n \to \infty$ такого рода события могут наступать с положительной вероятностью лишь на левом краю ряда (4.10), что отразится соответствующим образом на виде предельных распределений его минимальных членов. Например, теперь вместо (4.4) имеет место соотношение

$$\mathbf{P}\left\{\tilde{J}_m(n) > r\right\} = \mathbf{P}\left\{\sum_{i=1}^{r} k_i < m\right\},$$

и аналогом теоремы 4 является следующее утверждение: при $n \to \infty$

$$\mathbf{P}\left\{\tilde{J}_m(n) \leq r\right\} = \mathbf{P}\left\{\sum_{i=1}^{r} k_i \geq m\right\} + o(1).$$

В то же время результат (4.3) для минимальной степени остается справедливым и для с. в. $\tilde{J}_1(n)$. Асимптотические результаты для средних и максимальных рядов (4.10) и (4.1) оказываются идентичными.

В связи с обсуждаемой темой отметим недавнюю работу [6], в которой для общих комбинаторных структур, включающих и модель случайного многочлена над конечным полем, получена многомерная локальная предельная теорема (аналог теоремы 7) для распределения максимальных членов в.р. типа (4.10).

Наш метод, использующий производящие функции, отличен от метода работы [6], и он позволяет получить в явной форме вид соответствующей предельной плотности в (4.7) и (4.9).

СПИСОК ЛИТЕРАТУРЫ

1. *Ивченко Г. И., Медведев Ю. И.* О структуре случайных многочленов над конечным полем. — В сб.: Труды по дискретной математике. Т. 3. — М.: ФИЗМАТЛИТ, 2000, С. 111–138.
2. *Ivchenko G. I., Medvedev Ju. I.* Local structure of random polinomials over finite fields. — In: Proceedings of the V-th International Conference on Probability Methods of Discrete Mathematics. — Utreht: VSP, 2001, P. 27–46.
3. *Ширяев А. Н.* Вероятность. — М.: Наука, 1980.
4. *Гончаров В. Л.* Из области комбинаторики. — Изв. АН СССР, 1944, Т. 8, С. 3–48.
4. *Колчин В. Ф.* Случайные отображения. — М.: Наука, 1984.
5. *Arratia R., Barbour A. D., Tavare S.* On Poisson-Dirichlet limits for random decomposable combinatorial structures. — Comb. Probab. Comp., 1999, V. 8, P. 193–208.