Math-Net.Ru
Общероссийский математический портал

Г. И. Ивченко, Ю. И. Медведев, О структуре случайных многочленов над конечными полями,
Тр. по дискр. матем., 2000, том 3, 111–138

https://www.mathnet.ru/tdm40

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
https://www.mathnet.ru/rus/agreement

Параметры загрузки:
IP: 18.97.14.85
9 декабря 2025 г., 13:40:34

Труды по дискретной математике
Том 3, с. 111–138
М.: ФИЗМАТЛИТ, 2000

О СТРУКТУРЕ СЛУЧАЙНЫХ МНОГОЧЛЕНОВ НАД КОНЕЧНЫМИ ПОЛЯМИ

Г. И. ИВЧЕНКО, Ю. И. МЕДВЕДЕВ

Рассматриваются многочлены вида $f(x) = x^n + a_1x^{n-1} + \ldots + a_n$ над произвольным конечным полем $\mathrm{GF}(q)$, где q — простое или степень простого числа. Коэффициенты $a_1, \ldots, a_n$ этих многочленов являются независимыми случайными величинами с равномерным распределением на $\mathrm{GF}(q)$. Вводятся понятия локальной структуры случайного многочлена, связанной с разложением многочлена на неприводимые сомножители, и различных ее характеристик. Исследуются точные и асимптотические (при $n \to \infty$) свойства распределений различных структурных характеристик случайного многочлена.

§ 1. ВВЕДЕНИЕ. ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ И ПОСТАНОВКА ЗАДАЧ

Пусть F_n есть множество всех нормированных (т.е. с единичным старшим коэффициентом) многочленов степени $n > 0$ над произвольным конечным полем $\mathrm{GF}(q)$, q — простое число или степень простого числа (все необходимые алгебраические и теоретико-числовые сведения можно найти, например, в [1]):

$$F_n = \{f : f(x) = x^n + a_1x^{n-1} + \ldots + a_n,\ a_i \in \mathrm{GF}(q)\}. \tag{1}$$

Известно, что каждый такой многочлен однозначно представим в виде произведения

$$f = f_1^{e_1} f_2^{e_2} \ldots f_m^{e_m}, \tag{2}$$

где $f_1, \ldots, f_m$ — различные нормированные неприводимые над полем $\mathrm{GF}(q)$ многочлены, а $e_1, \ldots, e_m$ — натуральные числа. Представление (2) называется *каноническим разложением* многочлена f.

Занумеруем в некотором порядке все нормированные неприводимые многочлены степени i:

$$\phi_{i1}, \phi_{i2}, \ldots, \phi_{i\psi_i}, \qquad i = 1, 2, \ldots$$

© Г. И. Ивченко, Ю. И. Медведев, 2000

Здесь $\psi_i = \psi_i(q)$ обозначает число всех неприводимых многочленов степени i над полем $\mathrm{GF}(q)$ (вид и свойства этих чисел приведены в Приложении).

Запишем каноническое разложение (2) многочлена f через ϕ_{ij}:

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_n = \prod_{i=1}^{n} \prod_{j=1}^{\psi_i} \phi_{ij}^{k_{ij}}(x), \tag{4}$$

где $k_{ij} \geq 0$ — кратность вхождения ϕ_{ij} в разложение (4). Набор

$$K_n = \left\{k_{ij},\, i = 1, \ldots, n,\, j = 1, \ldots, \psi_i\right\} \tag{5}$$

будем называть *локальной структурой* многочлена f, а величины k_{ij} — *элементами локальной структуры*. В частности, величины k_{1j}, $j = 1, \ldots$ $\ldots, \psi_1 = q$, суть *линейные элементы* локальной структуры. Ясно, что

$$\sum_{i=1}^{n} i \sum_{j=1}^{\psi_i} k_{ij} = n. \tag{6}$$

Другие структурные характеристики многочлена f выражаются через элементы локальной структуры k_{ij}. Отметим наиболее важные из них. Величина

$$k_i = \sum_{j=1}^{\psi_i} k_{ij}, \qquad i = 1, \ldots, n, \tag{7}$$

определяет общее число сомножителей степени i в (4) с учетом их кратностей. Составленный из этих величин вектор

$$\bar{k} = (k_1, k_2, \ldots, k_n) \tag{8}$$

будем называть *интегральной структурой* или просто *структурой многочлена* f, а величину k_i — *i-м элементом* структуры многочлена f. Величину

$$i_{\max} = \max\left\{i : k_i \neq 0\right\}$$

— максимальную степень неприводимых сомножителей в каноническом разложении многочлена f — назовем *показателем сложности* многочлена f. В отличие от k_i величина

$$r_i = \sum_{j=1}^{\psi_i} I(k_{ij} \geq 1),$$

где $I(\cdot)$ — индикатор события, определяет число *различных* сомножителей степени i в (4). Величина r_1 равна числу элементов поля $\mathrm{GF}(q)$, являющихся корнями многочлена f.

Аналогичным способом вводятся величины

$k = \sum_{i=1}^{n} k_i = \sum_{i=1}^{n} \sum_{j=1}^{\psi_i} k_{ij}$ — общее число сомножителей в (4),

$r = \sum_{i=1}^{n} r_i$ — общее число различных сомножителей в (4).

Далее мы будем рассматривать многочлены со случайными коэффициентами, считая, что в (4) $a_1, \ldots, a_n$ являются независимыми случайными величинами с равномерным распределением на множестве $\mathrm{GF}(q)$. В таком случае f становится случайным многочленом, выбираемым с равной вероятностью из множества всех q^n многочленов степени n, а его локальная структура становится случайным вектором, который мы будем обозначать

$$\bar{\xi}' = \{\xi_{ij},\, i = 1, \ldots, n,\, j = 1, \ldots, \psi_i\}.$$

Случайными становятся и все характеристики локальной структуры: интегральная структура $\bar{k}$, сложность $i_{\max}$ и другие.

Данная статья посвящена исследованию локальной структуры $\bar{\xi}'$ случайных многочленов и ее основных характеристик, указанных выше. Интерес к исследованию подобных объектов объясняется возросшим в настоящее время вниманием к многочленам в конечных полях, вопросам их разложимости на неприводимые множители, логарифмированию в конечных полях и группах и т.п. Первые результаты в указанной проблематике были получены В. Е. Степановым, рассматривавшим характеристики интегральной структуры (в нашей терминологии) для случая $q = 2$. В. Н. Сачков другим методом распространил эти результаты на произвольное поле $\mathrm{GF}(q)$ и разработал аппарат производящих функций для перечисления многочленов с различными ограничениями на структуру канонического разложения. Ряд результатов по анализу случайной величины $i_{\max}$ в случае $q = 2$ получен Одлижко [4]. Все упомянутые результаты будут отмечены по тексту. В работе [8] разработан оригинальный метод получения аппроксимации для совместных распределений характеристик интегральной структуры случайных многочленов над конечными полями посредством установления верхних границ для расстояний по вариации до более простых распределений. В этой работе систематически проводится параллель между проблемами факторизации случайных многочленов и цикловой структурой случайных подстановок, отмеченная также и в работах В. Е. Степанова и В. Н. Сачкова и прослеживаемая в работах [4], [7]–[9].

Заметим, что не представляет большого труда переход от рассмотрения случайных многочленов степени n над полем $\mathrm{GF}(q)$ (назовем эту постановку моделью F_n) к рассмотрению многочленов, выбираемых с равной вероятностью из множества всех нормированных многочленов степени ниже n, т.е. из множества

$$F_{<h} = \bigcup_{k<n} F_k$$

(эту постановку назовем моделью $F_{<n}$). Число таких многочленов есть

$$|F_{<n}| = \sum_{k<n} q^k = \frac{q^n - 1}{q - 1}.$$

Ниже мы будем детально анализировать модель F_n, параллельно отмечая соответствующие результаты для модели $F_{<n}$.

§ 2. ПРОИЗВОДЯЩИЕ ФУНКЦИИ

В работе В. Л. Гончарова [2] было показано, что аппарат производящих функций в совокупности с использованием теории вычетов и метода перевала является эффективным средством исследования комбинаторных объектов сложной структуры.

Для случайного и равновероятного многочлена $f \in F_n$ элементы локальной структуры k_{ij} являются случайными величинами и обозначаются $\xi_{ij} = \xi_{ij}(n)$. Для их совместной производящей функции имеем

$$\begin{aligned} A_n\{t_{ij},\, i=1,\dots,n,\, j=1,\dots,\psi_i\} &\equiv \mathbf{E}\prod_{i,j} t_{ij}^{\xi_{ij}(n)} = \\ &= \frac{1}{q^n}\sum_{L_n}\prod_{i=1}^{n}\prod_{j=1}^{\psi_i} t_{ij}^{k_{ij}} = \operatorname{coef}_{z^n}\left[\sum_{n=0}^{\infty}\left(\frac{z}{q}\right)^n \sum_{L_n}\prod_{i,j} t_{ij}^{k_{ij}}\right] = \\ &= \operatorname{coef}_{z^n}\left[\prod_{i\geq 1}\prod_{j=1}^{\psi_i}\sum_{k_{ij}=0}^{\infty}\left(t_{ij}\left(\frac{z}{q}\right)^i\right)^{k_{ij}}\right] = \operatorname{coef}_{z^n}\left[\prod_{i\geq 1}\prod_{j=1}^{\psi_i}\left(1-t_{ij}\left(\frac{z}{q}\right)^i\right)^{-1}\right] \end{aligned} \tag{9}$$

(здесь L_n обозначает множество всех наборов $\{k_{ij}\}$, удовлетворяющих условию (6)). В частности, полагая в (9) все $t_{ij} = 1$, получаем равенство

$$\frac{1}{1-z} = \prod_{i\geq 1}\prod_{j=1}^{\psi_i}\left(1-\left(\frac{z}{q}\right)^i\right)^{-1},$$

поэтому выражение для производящей функции (9) можно записать следующим образом:

$$A_n(\{t_{ij}\}) = \operatorname{coef}_{z^n}\frac{1}{1-z}\prod_{i\geq 1}\prod_{j=1}^{\psi_i}\frac{1-(z/q)^i}{1-t_{ij}(z/q)^i}. \tag{10}$$

Это — основная производящая функция локальной структуры случайного многочлена $f \in F_n$. Выбирая соответствующим образом значения t_{ij}, из (10) можно получать производящие функции интересующих нас характеристик этой структуры. Так, например, полагая в (10) все $t_{ij} = 1$ при $i > r$, получаем совместную производящую функцию для ξ_{ij}, $i = 1,\dots,r$, $j = 1,\dots,\psi_i$:

$$\mathbf{E}\prod_{i=1}^{r}\prod_{j=1}^{\psi_i} t_{ij}^{\xi_{ij}} = \operatorname{coef}_{z^n}\frac{1}{1-z}\prod_{i=1}^{r}\prod_{j=1}^{\psi_i}\frac{1-(z/q)^i}{1-t_{ij}(z/q)^i},$$

откуда следует, что при $n \to \infty$ и любом фиксированном $r \geq 1$

$$\mathbf{E}\prod_{i=1}^{r}\prod_{j=1}^{\psi_i} t_{ij}^{\xi_{ij}} \longrightarrow \prod_{i=1}^{r}\prod_{j=1}^{\psi_i}\frac{1-q^{-i}}{1-t_{ij}q^{-i}}.$$

З а м е ч а н и е. Если рассматривать модель $F_{<n}$ (с равномерным распределением на множестве многочленов степени ниже n), то надо ввести производящую функцию

$$A_{<n}\{t_{ij},\, i=1,\dots,n-1,\, j=1,\dots,\psi_i\} =$$

$$= \mathbf{E}\prod_{ij} t_{ij}^{\xi_{ij}(n)} = \left(\frac{q^n-1}{q-1}\right)^{-1} \sum_{M_n} \prod_{i=1}^{n-1}\prod_{j=1}^{\psi_i} t_{ij}^{k_{ij}},$$

где

$$M_n = \left\{\{k_{ij}, i=1,\dots,n-1, j=1,\dots,\psi_i\} : k_{ij}\ge 0,\ \sum_{i=1}^{n-1} i \sum_{j=1}^{\psi_i} k_{ij} < n\right\}. \qquad (6')$$

Отсюда получаем (см. определение L_k в (9))

$$\sum_{n=1}^{\infty} \frac{1-q^{-n}}{q-1} z^n A_{<n}(\{t_{ij}\}) = \sum_{n=1}^{\infty}\left(\frac{z}{q}\right)^n \sum_{k=1}^{n-1}\sum_{L_k}\prod_{i=1}^{k}\prod_{j=1}^{\psi_i} t_{ij}^{k_{ij}} =$$

$$= \frac{z}{q}\sum_{n=0}^{\infty}\sum_{k=0}^{n}\left(\frac{z}{q}\right)^{n-k}\sum_{L_k}\prod_{i,j}\left(t_{ij}\left(\frac{z}{q}\right)^i\right)^{k_{ij}} =$$

$$= \frac{z}{q}\sum_{n=0}^{\infty}\left(\frac{z}{q}\right)^n \prod_{i\ge 1}\prod_{j=1}^{\psi_i}\sum_{k_{ij}=0}^{\infty}\left(t_{ij}\left(\frac{z}{q}\right)^i\right)^{k_{ij}} = \frac{z}{q-z}\prod_{i\ge 1}\prod_{j=1}^{\psi_i}\left(1-t_{ij}\left(\frac{z}{q}\right)^i\right)^{-1}$$

и, окончательно,

$$A_{<n}(\{t_{ij}\}) = \frac{q-1}{1-q^{-n}}\,\mathrm{coef}_{z^{n-1}}\,\frac{1}{q-z}\prod_{i\ge 1}\prod_{j=1}^{\psi_i}\left(1-t_{ij}\left(\frac{z}{q}\right)^i\right)^{-1}. \qquad (9')$$

Сравнивая (9′) с (9), делаем вывод, что все представления для производящих функций любых структурных характеристик в модели $F_{<n}$ отличаются от соответствующих представлений в модели F_n лишь заменой выражения $\mathrm{coef}_{z^n}(\cdot)$ выражением

$$\frac{q-1}{1-q^{-n}}\,\mathrm{coef}_{z^{n-1}}\,\frac{1}{q-z}\,(\cdot).$$

Это обстоятельство мы используем в последующем рассмотрении.

§ 3. ЛИНЕЙНЫЕ СОМНОЖИТЕЛИ ЛОКАЛЬНОЙ СТРУКТУРЫ

Особенный интерес в локальной структуре представляют линейные сомножители в каноническом разложении (4), определяемые вектором $(\xi_{11},\dots,\xi_{1q})$. Для получения его производящей функции надо положить в представлении (10) все $t_{ij}=1$ при $i\ge 2$. Имеем (считаем $|t_{1j}|\le 1$, $|z|<1$ при любом j)

$$\mathbf{E}t_{11}^{\xi_{11}}\dots t_{1q}^{\xi_{1q}} = \operatorname{coef}_{z^n}\frac{1}{1-z}\prod_{j=1}^{q}\frac{1-z/q}{1-t_{ij}z/q} = \\ = \sum_{m_1,\dots,m_q} t_{11}^{m_1}\dots t_{1q}^{m_q}\frac{1}{q^m 2\pi i}\oint\frac{(1-z/q)^q}{1-z}\frac{dz}{z^{n-m+1}}, \tag{10'}$$

где $m = m_1 + \ldots + m_q$. Контурный интеграл легко вычисляется методом вычетов. В итоге получаем

$$\mathbf{E}\prod_{i=1}^{q} t_{1i}^{\xi_{1i}} = \sum_{m_1,\dots,m_q}\frac{1}{q^m}\sum_{j=0}^{n-m}\left(-\frac{1}{q}\right)^j\binom{q}{j}t_{11}^{m_1}\dots t_{1q}^{m_q}, \qquad \sum_{i=1}^{q} m_i = m,$$

$0 \le m \le n$, а распределение вероятностей имеет вид

$$\mathbf{P}\left\{\xi_{11} = m_1,\dots,\xi_{1q} = m_q\right\} = \frac{1}{q^m}\sum_{j=0}^{n-m}\binom{q}{j}\left(-\frac{1}{q}\right)^j, \qquad \sum_{i=1}^{q} m_i = m, \tag{11}$$

$0 \le m \le n$.

Таким образом, случайные величины $\xi_{11},\dots,\xi_{1q}$ симметрично зависимы (перестановочны), т.е. все $q!$ перестановок величин $\xi_{11},\dots,\xi_{1q}$ имеют одно и то же совместное распределение. В частности, если $n - m \ge q$, то распределение получает простой вид:

$$\mathbf{P}\left\{\xi_{11} = m_1,\dots,\xi_{1q} = m_q\right\} = \frac{1}{q^m}\left(1-\frac{1}{q}\right)^q, \qquad \sum_{i=1}^{q} m_i = m, \qquad m+q \le n.$$

Маргинальные распределения компонент рассматриваемого вектора (например, ξ_{11}) легко получаются из соотношения (10′), где следует положить $t_{12} = \ldots = t_{1q} = 1$:

$$Q_{\xi_{11}}(t_{11}) \equiv \mathbf{E}t_{11}^{\xi_{11}} = \sum_{j=0}^{n-1}\left(1-\frac{1}{q}\right)\left(\frac{t_{11}}{q}\right)^j + \left(\frac{t_{11}}{q}\right)^n. \tag{12}$$

Значит,

$$\mathbf{P}\left\{\xi_{11} = s\right\} = \begin{cases}(1-1/q)\,q^{-s}, & s = 0,\dots,n-1,\\ q^{-n}, & s = n.\end{cases} \tag{13}$$

Таким образом, распределение случайной величины ξ_{11} есть усеченное сверху в точке n геометрическое распределение с параметром q^{-1}. Очевидно, при $n \to \infty$ и фиксированном q предельное распределение случайной величины ξ_{11} есть геометрическое распределение с параметром q^{-1}.

Подсчитаем моменты распределения случайной величины ξ_{11}. Продифференцировав r раз по t_{11} функцию (12), получим

$$Q_{\xi_{11}}^{(r)}(t_{11}) = \frac{1}{2\pi i}\oint\frac{1-z/q}{1-z}\frac{r!}{(1-t_{11}z/q)^{r+1}q^r}\frac{dz}{z^{n-r+1}}$$

и, стало быть,

$$\mathbf{E}\xi_{11}^{[r]} = Q_{\xi_{11}}^{(r)}(1) = \frac{r!}{q^r}\sum_{m=0}^{n-r}\binom{r+m-1}{m}\frac{1}{q^m} =$$

$$= \frac{r!}{(q-1)^r}\sum_{m=0}^{n-r}\binom{r+m-1}{m}\left(\frac{1}{q}\right)^m\left(1-\frac{1}{q}\right)^r = \tag{14}$$

$$= \frac{r!}{(q-1)^r}F\left(n-r; r, 1-\frac{1}{q}\right), \qquad r = 1, \ldots, n,$$

где

$$x^{[r]} = x(x-1)\ldots(x-r+1)$$

и $F(x; r, q)$ — значение в точке x функции распределения отрицательного биномиального закона с параметрами r и q.

Отсюда получаем, что при $n \to \infty$ и фиксированном q

$$\mathbf{E}\xi_{11}^{[r]} \longrightarrow \frac{r!}{(q-1)^r}, \qquad r \geq 1. \tag{15}$$

§ 4. ЧИСЛО КОРНЕЙ СЛУЧАЙНОГО МНОГОЧЛЕНА

Случайная величина

$$\kappa_i \equiv \kappa_i(n, q) = \sum_{j=1}^{\psi_i} I(\xi_{ij} \geq 1)$$

равна числу *различных* сомножителей степени i в каноническом разложении случайного многочлена. В этом разделе изучается распределение характеристики

$$\kappa_1 = \sum_{j=1}^{q} I(\xi_{1j} \geq 1), \tag{16}$$

которая равна числу элементов поля $\mathrm{GF}(q)$, являющихся корнями случайного многочлена.

Событие $\{\kappa_1 = s\}$, $s = 0, \ldots, q$, означает, что случайный вектор $(\xi_{11}, \ldots, \xi_{1q})$ содержит ровно s координат, отличных от нуля, и $q - s$ координат, равных нулю. В силу перестановочности случайных величин ξ_{1i}, $i = 1, \ldots, q$,

$$\mathbf{P}\{\kappa_1 = s\} = \binom{q}{s}\mathbf{P}\{\xi_{11} > 0, \ldots, \xi_{1,s} > 0, \xi_{1,s+1} = 0, \ldots, \xi_{1q} = 0\}. \tag{17}$$

По формуле включения-исключения

$$\mathbf{P}\{\xi_{11} > 0, \ldots, \xi_{1,s} > 0, \xi_{1,s+1} = 0, \ldots, \xi_{1q} = 0\} =$$

$$= \sum_{j=0}^{s}\binom{s}{j}(-1)^j\mathbf{P}\{\xi_{1,s-j+1} = 0, \ldots, \xi_{1p} = 0\}. \tag{18}$$

Остается заметить, что вероятность $\mathbf{P}\{\xi_{1,s-j+1} = 0, \ldots, \xi_{1q} = 0\}$ есть не что иное, как значение производящей функции $\mathbf{E}\prod_{j=1}^{q} t_{1j}^{\xi_{1j}}$ при $t_{11} = \ldots = t_{1,s-j} = 1, t_{1,s-j+1} = \ldots = t_{1q} = 0$. Подставляя указанные значения t_{1j} в (10′), получаем

$$\mathbf{P}\{\xi_{1,s-j+1} = 0, \ldots, \xi_{1q} = 0\} =$$

$$= \frac{1}{2\pi i}\oint \frac{(1-z/q)^{q-s+j}}{1-z}\,\frac{dz}{z^{n+1}} = \sum_{m=0}^{n}\binom{q-s+j}{m}\left(-\frac{1}{q}\right)^m. \tag{19}$$

Объединение (17)–(19) дает

$$\begin{aligned}\mathbf{P}\{\kappa_1 = s\} &= \binom{q}{s}\sum_{j=0}^{s}(-1)^{s-j}\binom{s}{j}\sum_{m=0}^{n}\binom{q-j}{m}\left(-\frac{1}{q}\right)^m = \\ &= \binom{q}{s}\sum_{m=0}^{n}\left(-\frac{1}{q}\right)^m(-1)^s\sum_{j=0}^{s}(-1)^j\binom{s}{j}\binom{q-j}{m}.\end{aligned} \tag{20}$$

Так как

$$\binom{q-j}{m} = \operatorname{coef}_{z^m}(1+z)^{q-j},$$

то внутренняя сумма в (20) равна $\binom{q-s}{m-s}$. Окончательно получаем

$$\mathbf{P}\{\kappa_1 = s\} = \binom{q}{s}(-1)^s\sum_{m=s}^{n}\left(-\frac{1}{q}\right)^m\binom{q-s}{m-s} = \binom{q}{s}q^{-s}\sum_{j=0}^{n-s}\left(-\frac{1}{q}\right)^j\binom{q-s}{j}, \tag{21}$$

$s = 0, \ldots, q$.

Формулу (21) можно представить следующим образом:

$$\mathbf{P}\{\kappa_1 = s\} = \binom{q}{s}q^{-s}\left(1-\frac{1}{q}\right)^{q-s} - \Delta_n = b\left(s; q, \frac{1}{q}\right) - \Delta_n, \tag{22}$$

$s = 0, \ldots, q$, где $b(s; q, 1/q)$ — вероятность биномиального закона распределения (в точке s) с числом испытаний q и вероятностью успеха $1/q$, а

$$\Delta_n = \binom{q}{s}q^{-s}\sum_{j=n-s+1}^{q-s}\left(-\frac{1}{q}\right)^j\binom{q-s}{j} \tag{23}$$

— "добавок", который равен нулю, когда $n \geq q$. Таким образом, случайная величина κ_1 имеет биномиальный закон распределения при $n \geq q$ и несколько отличающийся от него при $n < q$. Подчеркнем, что при $n \to \infty$ и фиксированном q добавок Δ_n всегда равен нулю, следовательно, распределение случайной величины κ_1 сходится к биномиальному распределению с параметрами q и q^{-1}.

Моменты распределения этой величины удобно получать из производящей функции для κ_1. В самом деле, из (21) имеем

$$\mathbf{E}x^{\kappa_1} = \sum_{s=0}^{q} \binom{q}{s} \cdot \frac{x^s}{q^s} \frac{1}{2\pi i} \oint \frac{(1-z/q)^{q-s}}{1-z} \frac{dz}{z^{n-s+1}} =$$

$$= \frac{1}{2\pi i} \oint \frac{(1-z(1-x)/q)^q}{1-z} \frac{dz}{z^{n+1}}.$$

Дифференцируя m раз это выражение по x в точке $x = 1$, получаем

$$\mathbf{E}\kappa_1^{[m]} = \frac{1}{2\pi i} \oint \frac{q^{[m]} z^m}{q^m (1-z)} \frac{dz}{z^{n+1}} = \begin{cases} q^{[m]} q^{-m}, & m = 0, \ldots, n, \\ 0, & m > n, \end{cases}$$

как и для биномиального распределения с параметрами q и $1/q$, но только для значений m, не превосходящих n. При $n < q$ в отличие от биномиального случая моменты порядков от $m = n+1$ до $m = q$ равны нулю. В частности, $\mathbf{E}\kappa_1 = 1$, т.е. при любых n и q в среднем лишь один элемент поля $\mathrm{GF}(q)$ является корнем случайного многочлена n-й степени.

§ 5. ИНТЕГРАЛЬНАЯ СТРУКТУРА СЛУЧАЙНОГО МНОГОЧЛЕНА

В настоящем параграфе рассмотрим случайный вектор

$$\bar{\xi}(n) = (\xi_1(n), \ldots, \xi_n(n)),$$

где $\xi_r(n) = \sum_{j=1}^{\psi_r} \xi_{rj}(n)$ — *число сомножителей степени* r (с учетом их кратностей) в каноническом разложении случайного многочлена n-й степени на неприводимые сомножители. Данный вектор называется *интегральной структурой* (или просто структурой) случайного многочлена.

Производящая функция распределения случайного вектора $\bar{\xi}(n)$ получается из основной производящей функции (9) или (10) заменами $t_{ij} = t_i$ при любых i, j:

$$A_n(t_1, \ldots, t_n) = \mathbf{E} \prod_i t_i^{\xi_i(n)} = \mathrm{coef}_{z^n} \prod_{i \geq 1} \left(1 - t_i \left(\frac{z}{q}\right)^i\right)^{-\psi_i} \tag{24}$$

или

$$A_n(t_1, \ldots, t_n) = \mathrm{coef}_{z^n} \frac{1}{1-z} \prod_{i \geq 1} \left(\frac{1-(z/q)^i}{1-t_i(z/q)^i}\right)^{\psi_i}. \tag{25}$$

Данное представление впервые было получено В. Е. Степановым (для $q = 2$) и распространено на случай произвольных q В. Н. Сачковым.

Преобразуем произведение в (24) следующим образом (далее $|z| < 1$, $|t_i| \leq 1$ при любом i):

$$\prod_{i=1}^{\infty}\left(1-t_i\left(\frac{z}{q}\right)^i\right)^{-\psi_i} = \exp\left\{\sum_{i=1}^{\infty}\psi_i\sum_{j=1}^{\infty}\frac{t_i^j}{j}\left(\frac{z}{q}\right)^{ij}\right\} =$$

$$= \exp\left\{\sum_{m=1}^{\infty}\left(\frac{z}{q}\right)^m m^{-1}\sum_{i\,|\,m} i\psi_i t_i^{m/i}\right\} =$$

$$= \frac{1}{1-z}\exp\left\{\sum_{m=1}^{\infty}\left(\frac{z}{q}\right)^m m^{-1}\sum_{i\,|\,m} i\psi_i\left(t_i^{m/i}-1\right)\right\}$$

(последнее равенство получается с помощью соотношения (П.1), указанного в приложении). Таким образом,

$$A_n(t_1,\ldots,t_n) = \operatorname{coef}_{z^n}\frac{1}{1-z}\exp\left\{\sum_{m=1}^{\infty}\left(\frac{z}{q}\right)^m m^{-1}\sum_{i\,|\,m} i\psi_i\left(t_i^{m/i}-1\right)\right\}. \quad (26)$$

З а м е ч а н и е. В модели $F_{<n}$ аналогом производящей функции (24) является представление

$$A_{<n}(t_1,\ldots,t_{n-1}) = \frac{q-1}{1-q^{-n}}\operatorname{coef}_{z^{n-1}}\frac{1}{q-z}\prod_{i\geq 1}\left(1-t_i\left(\frac{z}{q}\right)^i\right)^{-\psi_i}. \quad (24')$$

При заданных $1\leq r_1<\ldots<r_s\leq n$, полагая в (24) $t_i=1$, $i\neq r_1,\ldots,r_s$, получаем маргинальную производящую функцию

$$\mathbf{E}\, t_{r_1}^{\xi_{r_1}}\ldots t_{r_s}^{\xi_{r_s}} = \operatorname{coef}_{z^n}\frac{1}{1-z}\prod_{j=1}^{s}\left(\frac{1-(z/q)^{r_j}}{(1-t_j(z/q)^{r_j}}\right)^{\psi_{r_j}}. \quad (27)$$

§ 6. ЧИСЛО $\xi_r(n)$ СОМНОЖИТЕЛЕЙ СТЕПЕНИ r В КАНОНИЧЕСКОМ РАЗЛОЖЕНИИ СЛУЧАЙНОГО МНОГОЧЛЕНА

Разлагая производящую функцию (см. (27) при $s=1$)

$$Q_r(t) \equiv \mathbf{E}t^{\xi_r(n)} = \frac{1}{2\pi i}\oint\frac{1}{1-z}\left(\frac{1-(z/q)^r}{1-t(z/q)^r}\right)^{\psi_r}\frac{dz}{z^{n+1}} \quad (28)$$

случайной величины $\xi_r(n)$ в ряд по степеням t, получаем

$$Q_r(t) = \sum_{m=0}^{[n/r]}\binom{\psi_r+m-1}{m}q^{-rm}\sum_{j=0}^{[n/r]-m}\binom{\psi_r}{j}\left(-q^{-r}\right)^j t^m. \quad (29)$$

Значит,

$$\mathbf{P}\left\{\xi_r = m\right\} = \binom{\psi_r + m - 1}{m} q^{-rm} \sum_{j=0}^{[n/r]-m} \binom{\psi_r}{j} \left(-q^{-r}\right)^j,$$

$m = 0, \ldots, [n/r]$. Добавляя и вычитая члены с j от $[n/r] - m$ до ψ_r (если $[n/r] - m < \psi_r$), окончательно получаем

$$\mathbf{P}\left\{\xi_r = m\right\} = f\left(m, \psi_r, 1 - q^{-r}\right) - \Delta_{m,n,q,r}, \qquad m = 0, \ldots, \left[\frac{n}{r}\right], \tag{30}$$

где главный член $f\left(m, \psi_r, 1 - q^{-r}\right)$ есть вероятность отрицательного биномиального распределения, т.е. вероятность того, что ψ_r-й "успех" в испытаниях Бернулли с вероятностью "успеха" $1 - q^{-r}$ появится в $(\psi_r + m)$-м испытании, а

$$\Delta_{m,n,q,r} = \binom{\psi_r + m - 1}{m} q^{-rm} \sum_{j=[n/r]-m+1}^{\psi_r} \binom{\psi_r}{j} \left(-q^{-r}\right)^j$$

— "дополнительный" член, равный нулю для всех значений $m \le [n/r] - \psi_r$. Заметим, что "главный член" не зависит от n и полностью определяет распределение случайной величины ξ_r при больших n; от n зависит лишь "дополнительный" член.

Моменты случайной величины $\xi_r(n)$ находим, дифференцируя в точке $t = 1$ производящую функцию (28):

$$\begin{aligned} Q_r^{(l)}(1) = \mathbf{E}\xi_r^{[l]} &= \frac{(\psi_r + l - 1)^{[l]}}{q^{rs}} \frac{1}{2\pi i} \oint \frac{1}{1-z} \left(1 - \left(\frac{z}{q}\right)^r\right)^{-l} \frac{dz}{z^{n-rl+1}} = \\ &= \frac{(\psi_r + l - 1)^{[l]}}{q^{rl}} \sum_{j=0}^{[n/r]-l} \binom{l + j - 1}{j} q^{-rj} = \\ &= \frac{(\psi_r + l - 1)^{[l]}}{(q^r - 1)^l} \sum_{j=0}^{[n/r]-l} f\left(j; l, 1 - \frac{1}{q^r}\right) = \\ &= \frac{(\psi_r + l - 1)^{[l]}}{(q^r - 1)^l} F\left(\left[\frac{n}{r}\right] - l; l, 1 - q^{-r}\right), \end{aligned} \tag{31}$$

где $F(x; l, 1 - q^{-r})$ — функция распределения отрицательного биномиального закона с параметрами l и $1 - q^{-r}$.

Полученную формулу можно записать и так:

$$\begin{aligned} \mathbf{E}\xi_r^{[l]} &= (\psi_r + l - 1)^{[l]} \left(\frac{1/q^r}{1 - 1/q^r}\right) F\left(\left[\frac{n}{r}\right] - l; l, 1 - q^{-r}\right) = \\ &= \mathbf{E}\eta_r^{[l]} \cdot F\left(\left[\frac{n}{r}\right] - l; l, 1 - q^{-r}\right), \qquad l = 1, \ldots, \left[\frac{n}{r}\right], \end{aligned}$$

где η_r — случайная величина, распределенная по отрицательному биномиальному закону с параметрами ψ_r и $1 - q^{-r}$. Это распределение будем далее обозначать $\overline{\mathrm{Bi}}\left(\psi_r, q^{-r}\right)$. Отсюда, в частности, получаем

$$\mathbf{E}\xi_r(n) = \frac{\psi_r}{q^r-1}\left(1-q^{-r[n/2]}\right),$$

$$\mathbf{D}\xi_r(n) = \frac{\psi_r}{q^r-1}\left(1-q^{-r[n/r]}\right) +$$

$$+\frac{\psi_r}{(q^r-1)^2}\left(1-\frac{n}{r}q^{-r([n/r]-1)}+\left(\frac{n}{r}-1\right)q^{-r[n/r]}\right) -$$

$$-\frac{\psi_r^2}{(q^r-1)^2}\left(\frac{n}{r}q^{-r([n/r]-1)}-\left(\frac{n}{r}+1\right)q^{-r[n/r]}+q^{-2r[n/r]}\right).$$

При $n\to\infty$ и фиксированном $r\geq 1$

$$\mathbf{E}\xi_r(n) = \frac{\psi_r}{q^r-1}+O\left(q^{-n}\right), \qquad \mathbf{D}\xi_r(n) = \frac{q^r\psi_r}{(q^r-1)^2}+O\left(nq^{-n}\right). \tag{32}$$

Более того, учитывая оценки (П.3), (П.4), можно заключить, что уже для небольших r справедливы приближения

$$\mathbf{E}\xi_r(n)\approx\mathbf{D}\xi_r(n)\approx\frac{1}{r}.$$

Аналогичными рассуждениями с использованием производящей функции (27) можно найти и

$$\sigma_{rs}(n) = \operatorname{cov}\left(\xi_r(n),\xi_s(n)\right), \qquad r\neq s.$$

Так как

$$\mathbf{E}\xi_r(n)\,\xi_s(n) = \psi_r\psi_s\operatorname{coef}_{z^n}\frac{1}{1-z}\,\frac{(z/q)^{r+s}}{(1-(z/q)^r)(1-(z/q)^s)} =$$

$$= \frac{\psi_r\psi_s}{q^{r+s}}\sum_{\substack{i,j\geq 0:\\ ri+sj\leq n-r-s}} q^{-ri-sj},$$

то, используя промежуточный результат в (31), получаем, что

$$\sigma_{rs}(n) = -\frac{\psi_r\psi_s}{q^{r+s}}\sum_{\substack{i,j\geq 0:\\ ri\leq n-r\\ sj\leq n-s\\ sj+ri>n-r-s}} q^{-ri-sj}. \tag{33}$$

Сумма здесь не превосходит $n^2(rs)^{-1}q^{-n+r+s}$; поэтому

$$|\sigma_{rs}(n)| < \psi_r\psi_s\frac{n^2}{rs}q^{-n},$$

откуда следует асимптотическая некоррелированность случайных величин $\xi_r(n)$ и $\xi_s(n)$ при $n\to\infty$ и фиксированных r и s.

З а м е ч а н и е. Воспользовавшись представлением (24′), аналогично можно исследовать моменты случайных величин $\xi_r(n)$ и в модели $F_{<n}$. Так, например,

$$\mathbf{E}\xi_r(n) = \frac{1-q^{-1}}{1-q^{-n}}\,\frac{\psi_r}{q^r-1}\sum_{k=0}^{n-1} q^{-n+k+1}\left(1-q^{r[k/r]}\right) =$$

$$= \frac{\psi_r}{q^r-1}\left(1+O\left(nq^{-n}\right)\right) \longrightarrow \frac{\psi_r}{q^r-1}, \qquad n\to\infty,$$

т.е. главный член асимптотики здесь такой же, как в модели F_n. Такое же заключение справедливо и для вторых моментов случайных величин $\xi_r(n)$.

§ 7. ПРЕДЕЛЬНЫЕ ТЕОРЕМЫ

Этот и последующие разделы посвящены предельным теоремам для структурных характеристик при больших значениях степени n случайного многочлена.

Исследуем сначала маргинальные распределения случайных величин $\xi_j(n)$, $j=1,\dots,r$, в случаях, когда $n\to\infty$ и r либо фиксировано, либо растет вместе с n, но не слишком быстро. Асимптотическое поведение этих случайных величин описывается следующим утверждением.

Теорема 1. *Если $n\to\infty$, то для любого фиксированного r случайные величины $\xi_j(n)$, $j=1,\dots,r$, асимптотически независимы, распределение случайной величины $\xi_j(n)$ и ее моменты сходятся соответственно к отрицательному биномиальному распределению $\overline{\mathrm{Bi}}(\psi_j, q^{-j})$:*

$$\mathbf{P}\left\{\xi_j(n)=k\right\} \longrightarrow \binom{\psi_j+k-1}{k} q^{-jk}\left(1-q^{-j}\right)^{\psi_j}, \qquad k=0,1,\dots, \tag{34}$$

и его моментам. Более того, если $r=r(n)\to\infty$ так, что $r=O(n/\ln n)$, то $\xi_1(n),\dots,\xi_r(n)$ тоже являются асимптотически независимыми, а распределение $\xi_j(n)$ при растущем j сближается с распределением Пуассона $\Pi(1/j)$.

Д о к а з а т е л ь с т в о. Утверждения теоремы для отдельной величины $\xi_j(n)$ при фиксированном j следуют из точных формул (30) и (31).

Обозначим

$$f(t_1,\dots,t_r;z) = \prod_{j=1}^{r}\left(\frac{1-(z/q)^j}{1-t_j(z/q)^j}\right)^{\psi_j},$$

тогда

$$A_n(t_1,\dots,t_r) = \mathbf{E}\prod_{j=1}^{r} t_j^{\xi_j(n)} = \mathrm{coef}_{z^n}\,\frac{1}{1-z}\,f(t_1,\dots,t_r;z).$$

Функция f является дробно-рациональной относительно переменной z, все полюса f при $|t_j|\le 1$, $j=1,\dots,r$, лежат в области $|z|\ge q\,(\ge 2)$. Поэтому при фиксированном r и $n\to\infty$

$$A_n(t_1,\ldots,t_r) \longrightarrow f(t_1,\ldots,t_r;1) = \prod_{j=1}^{r}\left(\frac{1-q^{-j}}{1-t_jq^{-j}}\right)^{\psi_j},$$

что доказывает первую часть теоремы.

Утверждение об асимптотической независимости случайных величин $\xi_1(n),\ldots,\xi_r(n)$ при $n\to\infty$ и $r=O(n/\ln n)$ следует из установленной в работе [8] оценки для расстояния по вариации d_{TV} между совместным распределением $\xi_1(n),\ldots,\xi_r(n)$ и распределением независимых случайных величин $\widetilde{\xi}_1,\ldots,\widetilde{\xi}_r$, где $\widetilde{\xi}_j$ имеет распределение $\overline{\mathrm{Bi}}(\psi_j,q^{-j})$:

$$d_{\mathrm{TV}}\left(L(\xi_1(n),\ldots,\xi_r(n)),L(\widetilde{\xi}_1,\ldots,\widetilde{\xi}_r)\right) = O\left(r\exp\left\{-\frac{n}{2r}\ln\frac{4}{3}\right\}\right)$$

при любом $r\geq 1$ (здесь $L(\cdot)$ обозначает распределение соответствующих случайных величин).

Наконец, утверждение об асимптотической пуассоновости случайной величины $\xi_j(n)$ при растущем j следует из соотношения (П.4). Теорема полностью доказана.

Замечание 1. Сходимость распределения случайной величины $\xi_j(n)$ при фиксированном j к отрицательному биномиальному распределению для случая $q=2$ была впервые доказана В. Е. Степановым и обобщена на случай произвольного q В. Н. Сачковым.

Замечание 2. Такой же результат справедлив и в модели $F_{<n}$.

§ 8. ПОКАЗАТЕЛЬ СЛОЖНОСТИ И ДРУГИЕ ХАРАКТЕРИСТИКИ СЛУЧАЙНОГО МНОГОЧЛЕНА

Под показателем сложности случайного многочлена мы понимаем случайную величину $\mu_{\max}(n)$, равную максимальной степени неприводимых сомножителей в каноническом разложении многочлена f.

Так как

$$\mathbf{P}\left\{\mu_{\max}(n)\leq s\right\} = \mathbf{P}\left\{\xi_i(n)=0,\ i>s\right\},$$

то, полагая в (24) и (26) $t_1=\ldots=t_s=1$ и $t_i=0$ при $i>s$, получаем представления

$$\begin{aligned}\mathbf{P}\left\{\mu_{\max}(n)\leq s\right\} &= \operatorname{coef}_{z^n}\prod_{i=1}^{s}\left(1-\left(\frac{z}{q}\right)^i\right)^{-\psi_i} = \\ &= \operatorname{coef}_{z^n}\exp\left\{\sum_{m\geq 1}\frac{(z/q)^m}{m}\sum_{i\,|\,m,\,i\leq s} i\psi_i\right\}.\end{aligned} \tag{35}$$

Далее, полагая в (25) $t_i=0$ при $i\leq s$ и $t_i=1$ при $i>s$, получаем следующее соотношение для минимальной степени $\mu_{\min}$ неприводимого многочлена в каноническом разложении:

$$\mathbf{P}\left\{\mu_{\min}(n)>s\right\}=\mathbf{P}\left\{\xi_i(n)=0,\ i\le s\right\}=\operatorname{coef}_{z^n}\frac{1}{1-z}\prod_{i=1}^{s}\left(1-\left(\frac{z}{q}\right)^i\right)^{\psi_i}. \quad (36)$$

Следующее утверждение о распределении минимальной степени сомножителя в каноническом разложении является прямым следствием теоремы 1 и представления (36).

Теорема 2. *Для любого натурального r при $n\to\infty$*

$$\mathbf{P}\left\{\mu_{\min}(n)\le r\right\}=1-\prod_{j=1}^{r}\left(1-q^{-j}\right)^{\psi_j}+o(1). \quad (37)$$

Вообще, пусть

$$\mu_{\min}(n)=\mu_{(1)}(n)\le\mu_{(2)}(n)\le\ldots\le\mu_{\max}(n) \quad (38)$$

есть вариационный ряд из степеней неприводимых сомножителей в разложении случайного многочлена $f\in F_n$. Тогда при $n\to\infty$ и фиксированных m и r

$$\mathbf{P}\left\{\mu_{(m)}(n)>r\right\}=\mathbf{P}\left\{\xi_1(n)+\ldots+\xi_r(n)<m\right\}\sim\sum_{k=0}^{m-1}\operatorname{coef}_{t^k}\prod_{j=1}^{r}\left(\frac{1-q^{-j}}{1-tq^{-j}}\right)^{\psi_j};$$

если же $m=m(n)\to\infty$, то

$$\mathbf{P}\left\{\mu_{(m)}(n)\le r\right\}=\mathbf{P}\left\{\xi_1(n)+\ldots+\xi_r(n)\ge m\right\}\longrightarrow 0,$$

т.е. $\mu_{(m)}(n)\to_P\infty$.

Эти результаты говорят о том, что начальные члены вариационного ряда (38) имеют невырожденные предельные распределения с бесконечными средними, поскольку при $n\to\infty$ (см. (П.4))

$$\mathbf{P}\left\{\mu_{\min}(n)>r\right\}\sim\prod_{j=1}^{r}\left(1-q^{-j}\right)^{\psi_j}=\exp\left\{-\sum_{j=1}^{r}\frac{\psi_j}{q^j}+O(1)\right\}=$$

$$=\exp\left\{-\sum_{j=1}^{r}\frac{1}{j}+O(1)\right\}=O\left(\frac{1}{r}\right).$$

Аналогично, отправляясь от соотношения

$$\mathbf{P}\left\{\mu_{\min}(n)=r,\ \xi_r(n)=k\right\}=\mathbf{P}\left\{\xi_j(n)=0,\ j<r,\ \xi_r(n)=k\right\},$$

справедливого для натуральных r и k, можно исследовать и асимптотическое поведение числа сомножителей $\xi_{\min}(n)$ минимальной степени в каноническом разложении случайного многочлена.

Теорема 3. *Для любых натуральных r и k при $n\to\infty$*

$$\mathbf{P}\left\{\mu_{\min}(n)=r,\ \xi_r(n)=k\right\}=\binom{\psi_r+k-1}{k}q^{-rk}\prod_{j=1}^{r}\left(1-q^{-j}\right)^{\psi_j}+o(1). \quad (39)$$

В свою очередь, из (39) и (37) следует, что условная вероятность

$$\mathbf{P}\left\{\xi_{\min}(n)=k\,|\,\mu_{\min}(n)=r\right\} = \frac{\mathbf{P}\left\{\mu_{\min}(n)=r,\,\xi_r(n)=k\right\}}{\mathbf{P}\left\{\mu_{\min}(n)=r\right\}} \longrightarrow$$

$$\longrightarrow \binom{\psi_r+k-1}{k}\frac{q^{-rk}\,(1-q^{-r})^{\psi_j}}{1-(1-q^{-r})^{\psi_r}}, \qquad k\geq 1,$$

т.е.

$$\mathcal{L}(\xi_{\min}(n)\,|\,\mu_{\min}(n)=r) \longrightarrow \mathcal{L}(\xi_r\,|\,\xi_r>0), \tag{40}$$

где $\mathcal{L}(\xi_r)=\overline{\mathrm{Bi}}\,(\psi_r,q^{-r})$.

Из (39) также следует предельное соотношение

$$\mathbf{P}\left\{\xi_{\min}(n)=k\right\} \longrightarrow \sum_{r\geq 1}\binom{\psi_r+k-1}{k}q^{-rk}\prod_{j=1}^{r}\left(1-q^{-j}\right)^{\psi_j}, \qquad k\geq 1. \tag{41}$$

Кроме того, в силу (32)

$$\mathbf{E}\xi_{\min}(n) \longrightarrow \sum_{r\geq 1}\frac{\psi_r}{q^r-1}\prod_{j=1}^{r-1}\left(1-q^{-j}\right)^{\psi_j}. \tag{42}$$

Последний ряд сходится (см. (П.4)) и, таким образом, при $n\to\infty$ среднее число сомножителей с минимальной степенью ограничено.

Метод разложения дробно-рациональной функции на простейшие дроби для вычисления коэффициентов в ее разложении в степенной ряд можно использовать также для исследования асимптотического (при $n\to\infty$) поведения вероятностей

$$P_n(s)=\mathbf{P}\left\{\mu_{\max}(n)\leq s\right\} \tag{43}$$

при конечных $s\geq 1$. Обозначим

$$V_s(z)=\prod_{i=1}^{s}\left(1-\left(\frac{z}{q}\right)^i\right)^{\psi_i},$$

тогда (см. (35))

$$P_n(s)=\mathrm{coef}_{z^n}V_s^{-1}(z).$$

Рассмотрим сначала случай $s=1$. Здесь

$$P_n(1)=\mathrm{coef}_{z^n}\left(1-\frac{z}{q}\right)^{-\psi_1}=\binom{n+\psi_1-1}{\psi_1-1}q^{-n},$$

и (так как $\psi_1=q$, см. (П.2)) при $n\to\infty$ справедлива асимптотика

$$P_n(1)\sim\frac{n^{p-1}}{(q-1)!}\,q^{-n}.$$

При $s\geq 2$ многочлен $V_s(z)$ помимо корня $z_1=q$ имеет и другие корни z_j, $j\geq 2$, которые все лежат на окружности $|z|=q$, но их кратности r_j будут меньше

$$r_1 = \tau_s = \sum_{i=1}^{s} \psi_i$$

— кратности корня z_1. Из алгебры известно, что в этом случае $V_s^{-1}(z)$ разлагается в конечную сумму простейших дробей

$$V_s^{-1}(z) = \sum_{j\geq 1} \sum_{k=0}^{r_j-1} \frac{c_k^{(j)}}{(1-z/z_j)^{r_j-k}},$$

которые вносят в суммарный коэффициент при z^n соответствующие вклады $c_k^{(j)}\binom{n+r_j-k-1}{r_j-k-1} z_j^{-n}$. Поскольку при конечном s число этих слагаемых конечно, то их сумма при $n \to \infty$ асимптотически эквивалентна одному слагаемому $c_0^{(1)}\binom{n+t_s-1}{t_s-1} q^{-n}$. Константа $c_0^{(1)}$ находится из цепочки соотношений

$$c_0^{(1)} = a_s = \left(1-\frac{z}{q}\right)^{t_s} V_s^{-1}(z)\Bigg|_{z=p} = \lim_{z\to q} \prod_{i=2}^{s} \left(\frac{1-z/q}{1-(z/q)^i}\right)^{\psi_j}\Bigg|_{z=q} = \prod_{i=2}^{s} i^{-\psi_i}.$$

В итоге мы можем сформулировать следующий результат.

Теорема 4. *При $n \to \infty$ для любого конечного $s \geq 1$ справедлива асимптотика*

$$P_n(s) = a_s \binom{n+t_s-1}{t_s-1} q^{-n}\left(1+O\left(\frac{1}{n}\right)\right) = a_s \frac{n^{t_s-1}}{(t_s-1)!} q^{-n}\left(1+O\left(\frac{1}{n}\right)\right), \quad (44)$$

где

$$t_s = \sum_{i=1}^{s} \psi_i, \qquad a_s = \prod_{i=1}^{s} i^{-\psi_i}.$$

Замечание. Из (44) следует, что при $n \to \infty$ и $s = \mathrm{const}$

$$\mathbf{P}\left\{\mu_{\max}(n) = s\right\} = P_n(s) - P_n(s-1) \sim P_n(s). \quad (45)$$

Эта теорема позволяет исследовать асимптотику условных вероятностей

$$\mathbf{P}\left\{\xi_i(n) = k_i,\, i = 1,\ldots,s \,|\, \mu_{\max}(n) = s\right\} = \\ = \frac{\mathbf{P}\left\{\xi_i(n) = k_i,\, i = 1,\ldots,s,\, \xi_i(n) = 0,\, i > s\right\}}{\mathbf{P}\left\{\mu_{\max}(n) = s\right\}} \quad (46)$$

при $n \to \infty$ и фиксированном $s > 1$.

Действительно, числитель дроби в правой части (46) есть коэффициент при $t_1^{k_1}\ldots t_s^{k_s}$ функции $A_n(t_1,\ldots,t_s,0,\ldots,0)$, т.е. он равен (см. (24))

$$\prod_{i=1}^{s} \binom{\psi_i+k_i-1}{k_i} q^{-n}, \qquad \text{где} \qquad n = \sum_{i=1}^{s} ik_i.$$

Если при $n \to \infty$ все $k_i \to \infty$ так, что $ik_i/n \to x_i$, $0 < x_i < 1$, $x_1 + \ldots + x_s = 1$, то в силу (44) и (45) правая часть (46) асимптотически эквивалентна величине

$$\frac{s!}{n^{s-1}} \frac{(t_s - 1)!}{\prod\limits_{i=1}^{s} (\psi_i - 1)!} \prod_{i=1}^{s} \left(\frac{ik_i}{n}\right)^{\psi_i - 1} \sim \frac{s!}{n^{s-1}} g(x_1, \ldots, x_s;\, \psi_1, \ldots, \psi_s),$$

где

$$g(x_1, \ldots, x_s;\, \psi_1, \ldots, \psi_s) = \frac{\Gamma(t_s)}{\Gamma(\psi_1) \ldots \Gamma(\psi_s)} \prod_{i=1}^{s} x_i^{\psi_i - 1} \tag{47}$$

есть плотность распределения Дирихле $\mathcal{D}(\psi_1, \ldots, \psi_s)$.

Таким образом, имеет место следующее утверждение.

Теорема 5. *Пусть $n, k_1, \ldots, k_s \to \infty$ так, что $ik_i/n \to x_i$, $0 < x_i < 1$, $x_1 + \ldots + x_s = 1$ ($s > 1$ фиксировано). Тогда*

$$\begin{aligned} &\mathbf{P}\left\{\xi_i(n) = k_i,\, i = 1, \ldots, s \,|\, \mu_{\max}(n) = s\right\} = \\ &\qquad = \frac{s!}{n^{s-1}} g(x_1, \ldots, x_s;\, \psi_1, \ldots, \psi_s)(1 + o(1)), \end{aligned} \tag{48}$$

где функция g определена в (47).

Это локальный вариант предельного соотношения

$$\mathcal{L}\left(\frac{i\xi_i(n)}{n},\, i = 1, \ldots, s \,|\, \mu_{\max}(n) = s\right) \longrightarrow \mathcal{D}(\psi_1, \ldots, \psi_s), \tag{49}$$

говорящего, в частности о том, что при условии $\{\mu_{\max}(n) = s\}$ число сомножителей каждой степени $i = 1, \ldots, s$ в каноническом разложении f имеет порядок $O(n/i)$.

Из (48) и (49) следуют также утверждения о сходимости к бета-распределению $\mathrm{Be}(\psi_s, t_{s-1})$ условного распределения числа $\xi_{\max}(n)$ сомножителей максимальной степени в каноническом разложении f: если $n, k \to \infty$ так, что $sk/n \to x$, $0 < x < 1$, то

$$\mathbf{P}\left\{\xi_{\max}(n) = k \,|\, \mu_{\max}(n) = s\right\} \sim \frac{s}{n} \beta(x; \psi_s, t_{s-1}),$$

где

$$\beta(x; a, b) = \frac{\Gamma(a+b)}{\Gamma(a)\,\Gamma(b)} x^{a-1}(1-x)^{b-1}, \qquad a, b > 0,$$

— плотность бета-распределения; кроме того,

$$\mathcal{L}\left(\frac{s\xi_{\max}(n)}{n} \,|\, \mu_{\max}(n) = s\right) \longrightarrow \mathrm{Be}(\psi_s, \tau_{s-1}).$$

Замечание. Нетрудно видеть, что эти утверждения остаются в силе при замене условия $\mu_{\max}(n) = s$ условием $\mu_{\max}(n) \le s$.

Исследованию вероятностей $P_n(s)$ при $s = s(n) \to \infty$, когда $n \to \infty$, посвящен следующий раздел.

§ 9. АСИМПТОТИЧЕСКОЕ ПОВЕДЕНИЕ СЛУЧАЙНОЙ ВЕЛИЧИНЫ $\mu_{\max}(n)$ (ПРОДОЛЖЕНИЕ)

Максимальная степень неприводимого сомножителя в каноническом разложении случайного многочлена $f \in F_n$ представляет собой одну из его наиболее интересных и важных для приложений структурных характеристик. Некоторые асимптотики для ее распределения, выводимые элементарными методами, представлены в предыдущем разделе. Из соотношения (44) следует, что при конечных s вероятность

$$P_n(s) = \mathbf{P}\{\mu_{\max}(n) \le s\} \to 0 \qquad \text{при} \qquad n \to \infty,$$

т.е. с ростом n случайная величина $\mu_{\max}(n)$ по вероятности неограниченно возрастает. Следовательно, ее распределение асимптотически сосредоточено в "далеких" зонах изменения s. В этом разделе мы исследуем поведение вероятностей $P_n(s)$ в различных зонах изменения $s = s(n) \to \infty$ при $n \to \infty$ с помощью второго представления в (35), метода перевала и других методов асимптотического анализа. Для этого прежде всего, учитывая формулу (П.1), запишем показатель экспоненты в (35) в виде $u_s(z) + v_s(z)$, где

$$u_s(z) = \sum_{m=1}^{s} \frac{z^m}{m}, \qquad v_s(z) = \sum_{m>s} \frac{(z/q)^m}{m} \sum_{i|m, i\le s} i\psi_i.$$

Тогда по формуле Коши

$$P_n(s) = \frac{1}{2\pi i} \oint F_s(z)\, e^{u_s(z)} \frac{dz}{z^{n+1}}, \tag{50}$$

где $F_s = e^{v_s(z)}$ и интегрирование ведется по любому замкнутому контуру, обходящему точку $z = 0$. Асимптотическое поведение этого интеграла при $n, s \to \infty$ можно исследовать с помощью стандартного метода перевала (см., например, [5]); при этом анализ интеграла в (50) можно заменить аналогичной задачей для более простого интеграла

$$\widetilde{P}_n(s) = \frac{1}{2\pi i} \oint e^{u_s(z)} \frac{dz}{z^{n+1}}. \tag{51}$$

Асимптотическая эквивалентность интегралов (50) и (51) при $n, s \to \infty$ следует из того факта, что в силу соотношения (П.5) ряд Тейлора для функции $v_s(z)$ сходится в круге $|z| \le \delta\sqrt{q}$ для произвольного $\delta \in (0,1)$, т.е. функция $v_s(z)$ является аналитической и, более того, в этом круге

$$v_s(z) = O\left(\sum_{m>\delta} \frac{1}{m}\left(\frac{z}{\sqrt{q}}\right)^m\right) \longrightarrow 0 \qquad \text{при} \qquad s \longrightarrow \infty$$

равномерно по z. Отсюда следует, что в этой области $F_s(z) \to 1$ при $s \to \infty$ равномерно по z, и если контур интегрирования в (50) и (51) выбрать в виде $|z| = r$ при $r < \delta\sqrt{q}$, то интегралы будут асимптотически эквивалентны:

$$P_n(s) \sim \widetilde{P}_n(s). \tag{52}$$

В связи с соотношением (52) отметим следующие замечательные обстоятельства. Во-первых, интеграл (51) не зависит от параметра q, и потому упомянутые во введении результаты В. Е. Степанова и А. М. Одлижко для случая $q = 2$ переносятся на случай произвольного $q \geq 2$. Во-вторых, $\widetilde{P}_n(s)$ представляет собой известную в теории случайных подстановок величину: вероятность того, что длина максимального цикла в случайной равновероятной подстановке степени n (обозначим ее $\widetilde{\mu}_{\max}(n)$) не превосходит s (см. [3]).

Для случая $s/n \to \alpha$, $0 < \alpha < 1$, эта вероятность исследовалась рядом авторов (см. [2] и комментарии в [3, § 1.14]), в том числе и В. Е. Степановым, который использовал метод перевала. Как показано в [6], точка перевала лежит около $z = 1 - 1/s$, следовательно, в зоне ее влияния $F_s(z) \to 1$ при $s \to \infty$, и потому справедливо соотношение (52). Далее, в этом случае (см., например, [3, § 1.14])

$$\widetilde{P}_n(s) \longrightarrow F(\alpha) = 1 - \sum_{1 \leq k < 1/\alpha} \frac{(-1)^{k-1}}{k!} J_k(\alpha), \tag{53}$$

где

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

и $\mathrm{E}\widetilde{\mu}_{\max}(n)/n \to 0,6243\ldots$ Тем самым доказано следующее утверждение.

Теорема 6. *При $n \to \infty$ случайная величина $\mu_{\max}(n)/n$ имеет собственное предельное распределение с функцией распределения $F(\alpha)$, указанной в (53), и $\mathrm{E}\mu_{\max}(n)/n \to 0,6243\ldots$*

Приведем также и альтернативный вариант доказательства, одновременно дополнив утверждение теоремы оценкой скорости сходимости. Для этого заметим, что вероятность $P_n(s-1)$ можно записать также в виде (см. (35) и (П.1))

$$P_n(s-1) = \mathrm{coef}_{z^n} \frac{1}{1-z} \exp\left\{ -\sum_{m \geq s} \frac{z^m}{m} a_m(s) \right\},$$

где используется обозначение

$$a_m(s) = q^{-m} \sum_{i \mid m, i \geq s} i\psi_i.$$

Отсюда имеем

$$P_n(s-1) = 1 - \sum_{1 \leq k \leq n/s} \frac{(-1)^k}{k!} S_k(n, s), \tag{54}$$

где

$$S_k(n,s) = \sum_{\substack{m_1,\dots,m_k \geq s \\ m_1+\dots+m_k \leq n}} \frac{a_{m_1}(s)\dots a_{m_k}(s)}{m_1\dots m_k},$$

Представление (54) удобно для асимптотического анализа, если $n, s \to \infty$ таким образом, что их отношение остается заключенным между постоянными пределами. При этом, если $r \leq n/s < r+1$ при некотором $r = 1, 2, \dots$, то сумма в (54) содержит лишь r слагаемых, асимптотическое поведение которых находится прямыми методами.

Пусть сначала $s > n/2$. Тогда из (54) следует, что

$$P_n(s-1) = 1 - S_1(n,s),$$

и здесь

$$S_1(n,s) = \sum_{m=s}^{n} \frac{a_m(s)}{m}.$$

Из соотношений (П.1) и (П.5) следует, что $a_m(s) = 1 + O(q^{-m/2})$ при $m \geq s$, поэтому, используя известное асимптотическое разложение

$$\sum_{m=1}^{n} \frac{1}{m} = \ln n + \gamma + \frac{1}{2n} + O\left(\frac{1}{n^2}\right), \qquad n \to \infty$$

(здесь γ — константа Эйлера), находим, что

$$S_1(n,s) = \ln\frac{n}{s} + \frac{1}{2n}\left(1 + \frac{n}{s}\right) + O\left(\frac{1}{n^2}\right). \tag{55}$$

Итак, при $n \to \infty$ и $s > n/2$

$$P_n(s-1) = 1 - \ln\frac{n}{s} - \frac{1}{2n}\left(1 + \frac{n}{s}\right) + O\left(\frac{1}{n^2}\right). \tag{56}$$

Полученный результат можно записать также в следующем виде: если $n \to \infty$, то при $\alpha > 1/2$

$$\mathbf{P}\left\{\frac{\mu_{\max}(n)}{n} < \alpha\right\} = 1 + \ln\alpha + O\left(n^{-1}\right). \tag{56'}$$

Рассмотрим теперь другую зону изменения s, определяемую условиями $n/3 < s \leq n/2$. Здесь (см. (54))

$$P_n(s-1) = 1 - S_1(n,s) + \frac{1}{2}S_2(n,s)$$

и

$$S_2(n,s) = \sum_{\substack{m_1,m_2 \geq s \\ m_1+m_2 \leq n}} \frac{a_{m_1}(s)\,a_{m_2}(s)}{m_1 m_2} = \sum_{m_2=s}^{n-s} \frac{a_{m_2}(s)}{m_2} S_1(n-m_2,s).$$

Используя оценки для чисел $a_m(s)$ и соотношение (55), можно заключить, что при $n \to \infty$

$$S_2(n,s)=\sum_{m=s}^{n-s}\frac{1}{m}\ln\frac{n-m}{s}+O\left(\frac{1}{n}\right)=\int\limits_{s/n}^{1-s/n}\frac{1}{x}\ln\frac{1-x}{s/n}\,dx+O\left(\frac{1}{n}\right).$$

В итоге получаем в рассматриваемой зоне асимптотическое представление

$$P_n(s-1)=1+\ln\frac{s}{n}+\frac{1}{2}\int\limits_{s/n}^{1-s/n}\frac{1}{x}\ln\frac{1-x}{s/n}\,dx+O\left(\frac{1}{n}\right), \tag{57}$$

которому можно придать следующую форму: если $n\to\infty$, то при $1/3<\alpha\le 1/2$

$$\mathbf{P}\left\{\frac{\mu_{\max}(n)}{n}<\alpha\right\}=1+\ln\alpha+\frac{1}{2}\int\limits_{\alpha}^{1-\alpha}\frac{1}{x}\ln\frac{1-x}{\alpha}\,dx+O\left(\frac{1}{n}\right). \tag{57'}$$

Продолжая аналогичным образом (т.е. рассматривая зоны $n/(r+1)<s\le n/r$) и учитывая, что при $n,s\to\infty$, $s/n\to\alpha$, $0<\alpha<1$, для любого фиксированного $k\ge 1$

$$S_k(n,s)=J_k(\alpha)+O\left(\frac{1}{n}\right),$$

где $J_k(\alpha)$ указаны в (53), получаем искомое предельное соотношение

$$\mathbf{P}\left\{\frac{\mu_{\max}(n)}{n}<\alpha\right\}=F(\alpha)+O\left(\frac{1}{n}\right),$$

конкретизациями которого для двух "верхних" зон изменения α: $1/(r+1)<\alpha\le 1/r$, $r=1,2$, являются соотношения (56′) и (57′).

Теорема 6 позволяет оценивать вероятности $P_n(s)$, когда $n,s\to\infty$ так, что $s/n\to\alpha$, $0<\alpha<1$. Однако для приложений представляет интерес также поведение $P_n(s)$ и в зоне $s\to\infty$, $s/n\to 0$ (здесь $P_n(s)\to 0$, и речь, следовательно, идет о скорости убывания этих вероятностей). Мы конкретизируем задачу, предполагая далее выполненным условие

$$\frac{\ln s}{\ln n}\in[\varepsilon,1-\varepsilon],\qquad \text{где}\qquad \varepsilon>0$$

и произвольно мало. Точка перевала для интеграла в (51) находится из уравнения $zu_s'(z)=n$, или

$$z+z^2+\ldots+z^s=n. \tag{58}$$

Пусть $r=r(s,n)$ есть единственный положительный корень этого уравнения. Тогда, переписав (58) в виде

$$z\left(\frac{1-z^{-s}}{1-z^{-1}}\right)^{1/s}=n^{1/s}$$

и учитывая, что

$$n^{1/s} = 1 + s^{-1}\ln n(1 + o(1)),$$

видим, что $r = 1 + o(1)$. Методом итераций нетрудно установить, что в данном случае

$$r = 1 + \frac{1}{s}\left(\ln\frac{n}{s} + \ln\ln\frac{n}{s} + O\left(\frac{\ln\ln(n/s)}{\ln(n/s)}\right)\right). \tag{59}$$

Если выбрать в (51) контур интегрирования в виде $|z| = r$ с этим значением r, то в зоне влияния точки перевала функция $F_s(z) \to 1\,(s \to \infty)$ и потому соотношение (52) выполняется. Наконец, применение к $\widetilde{P}_n(s)$ стандартной техники метода перевала дает оценку

$$\widetilde{P}_n(s) = \frac{1}{\sqrt{2\pi ns}}\, e^{u_s(r)} r^{-n}. \tag{60}$$

Мы опускаем технические детали, поскольку они фактически приведены в [4], где (для случая $q = 2$ при $\varepsilon = 10^{-2}$) получена асимптотика числа

$$N(n, s) = 2^n P_n(s)$$

многочленов степени n, все неприводимые сомножители которых имеют степень не выше s.

Таким образом, справедлив следующий результат.

Теорема 7. *Если $n, s \to \infty$ так, что $\ln s/\ln n \in [\varepsilon, 1-\varepsilon]$, где $\varepsilon > 0$ произвольно мало, то для $P_n(s) \sim \widetilde{P}_n(s)$ имеет место асимптотика* (60).

Сделаем несколько замечаний по поводу этой теоремы. С помощью формулы (П.10) и представления (59) нетрудно получить для

$$H_{s,n} = u_s(r) - n\ln r$$

разложение

$$H_{s,n} = -\frac{n}{s}\ln\frac{n}{s} - \frac{n}{s}\ln\ln\frac{n}{s} + \frac{n}{s} + O\left(\frac{n\ln\ln(n/s)}{s\ln(n/s)}\right). \tag{61}$$

Далее, условие теоремы, ограничивающее характер изменения s, фактически означает, что s растет как некоторая степень n, при этом также и $n/s \to \infty$ степенным образом. Поэтому остаточный член в (61) хотя и мал по сравнению с другими слагаемыми, в действительности может быть весьма большим. В соответствии с этим множитель $(2\pi ns)^{-1/2}$ в (60), будучи переведенным в показатель экспоненты, дает там логарифмическое слагаемое, не влияющее на порядок остаточного члена, и потому может быть опущен. Итак, вместо (60) можно использовать формулу

$$P_n(s) = e^{H_{s,n}(1+o(1))}. \tag{62}$$

Наконец, отметим следующие полезные следствия соотношения (62), выводимые непосредственно из (61): при $k = \pm 1, \pm 2, \ldots$

$$\frac{P_{n+k}(s)}{P_n(s)} \sim \left(\frac{n}{s}\ln\frac{n}{s}\right)^{-k/s}, \qquad \frac{P_n(s+k)}{P_n(s)} \sim \left(\frac{n}{s}\ln\frac{n}{s}\right)^{kn/s^2}. \tag{63}$$

Замечание. В соответствии с замечанием раздела 2 в модели $F_{<n}$ соответствующая вероятность $P_{<n}(s)$ отличается от $P_n(s)$ лишь наличием дополнительного множителя

$$\frac{(q-1)\,z}{(1-q^{-n})(q-z)}$$

в подынтегральном выражении (50), который при $z = 1+o(1)$ приближается к 1. Поэтому утверждения последних двух теорем сохраняют свою силу и в модели $F_{<n}$.

ПРИЛОЖЕНИЕ

1. Приведем необходимые нам сведения о числах $\psi_r = \psi_r(q)$ (см. [1, гл. 3]). Основное соотношение для этих чисел имеет вид

$$\sum_{r\,|\,m} r\psi_r = q^m \tag{П.1}$$

(сумма берется по всем положительным делителям r числа m). Отсюда и из теоремы Мебиуса об обращении теоретико-числовых функций следует точная формула для числа нормированных неприводимых многочленов фиксированной степени над полем $\mathrm{GF}(q)$

$$\psi_r(q) = \frac{1}{r}\sum_{i\,|\,r}\mu(i)\,q^{r/i} = \frac{1}{r}\sum_{i\,|\,r}\mu\left(\frac{r}{i}\right)q^i, \tag{П.2}$$

где $\mu(n)$ — функция Мебиуса: $\mu(1) = 1$, $\mu(n) = (-1)^k$, если n — произведение k различных простых чисел, $\mu(n) = 0$, если n делится на квадрат какого-либо числа.

Числа $\psi_r(q)$ удовлетворяют следующим неравенствам:

$$\frac{q^r}{r}\left(1-\frac{q}{q-1}\,q^{-r/2}\right) < \frac{q^r}{r} - \frac{q}{r(q-1)}\left(q^{r/2}-1\right) \le \psi_r(q) \le \frac{q}{r}\left(q^{r-1}-1\right) < \frac{q^r}{r}, \tag{П.3}$$

откуда, в частности, следует, что

$$r\psi_r(q) = q^r + O\left(q^{r/2}\right). \tag{П.4}$$

Отметим также следующую полезную оценку: при $m > r$

$$\sum_{i\,|\,m,\,i\le r} i\psi_i \le \sum_{i\,|\,m,\,i<m} i\psi_i = \sum_{i\,|\,m} i\psi_i - m\psi_m \le \frac{q}{q-1}\left(q^{m/2}-1\right) < 2q^{m/2}. \tag{П.5}$$

Далее, из (П.2) имеем

$$\tau_s = \sum_{r=1}^{s} \psi_r = \sum_{i=1}^{s} q^i \sum_{r:i|r} \frac{1}{r} \mu\left(\frac{r}{i}\right) = \sum_{i=1}^{s} \frac{q^i}{i} \sum_{j=1}^{[s/i]} \frac{\mu(j)}{j} =$$
$$= \sum_{i=[s/2]+1}^{s} \frac{q^i}{i} + \sum_{i=1}^{[s/2]} \frac{q^i}{i} \sum_{j=1}^{[s/i]} \frac{\mu(j)}{j}. \tag{П.6}$$

Кроме того, из (П.3) следуют оценки

$$\sum_{r=1}^{s} \frac{q^r}{r} - \frac{q}{q-1} \sum_{r=1}^{s} \frac{q^{r/2}-1}{r} \le \tau_s \le \sum_{r=1}^{s} \frac{q^r}{r} - q \sum_{r=1}^{s} \frac{1}{r}. \tag{П.7}$$

При больших значениях s поведение чисел τ_s определяется суммой

$$u_s(q) = \sum_{r=1}^{s} \frac{q^r}{r}. \tag{П.8}$$

В свою очередь асимптотика $u_s(a)$ при $s \to \infty$ и любом действительном $a > 1$ может быть получена с помощью преобразования Абеля:

$$u_s(a) = A_s b_s + \sum_{i=1}^{s-1} A_i (b_i - b_{i+1}) = \frac{a^{s+1}}{s(a-1)} + \frac{a}{a-1} \sum_{i=1}^{s-1} \frac{a^i}{i(i+1)} - \frac{a}{a-1},$$

если положить

$$A_i = a + a^2 + \ldots + a^i = \frac{a^{i+1} - a}{a-1}, \qquad b_i = \frac{1}{i}.$$

Повторное применение этого преобразования к сумме

$$\sum_{i=1}^{s-1} \frac{a^i}{i(i+1)}$$

приводит к формуле

$$u_s(a) = \frac{a^{s+1}}{s(a-1)} \left(1 + \frac{1}{(s-1)(a-1)}\right) +$$
$$+ \frac{2a^2}{(a-1)^2} \sum_{i=1}^{s-2} \frac{a^i}{i(i+1)(i+2)} - \frac{a}{a-1} \left(1 + \frac{a}{2(a-1)}\right).$$

Применив этот алгоритм k раз, получим общую формулу

$$u_s(a) = \frac{a^{s+1}}{s(a-1)} \sum_{j=0}^{k-1} \binom{s-1}{j}^{-1} (a-1)^{-j} +$$
$$+ k! \left(\frac{a}{a-1}\right)^k \sum_{i=1}^{s-k} \frac{a^i}{i(i+1)\ldots(i+k)} - \sum_{j=1}^{k} \frac{1}{j} \left(\frac{a}{a-1}\right)^j, \tag{П.9}$$

из которой следует асимптотическое представление

$$u_s(a) = \frac{a^{s+1}}{s(a-1)} \left(\sum_{j=0}^{k-1} \binom{s-1}{j}^{-1} (a-1)^{-j} + O\left(\frac{1}{s^k}\right) \right). \qquad (\text{П}.10)$$

Применение (П.10) к числам τ_s дает, в частности, оценку

$$\tau_s = \frac{q^{s+1}}{s(q-1)} \left(1 + O\left(\frac{1}{s}\right)\right). \qquad (\text{П}.11)$$

2. Для вычисления точных значений вероятностей $P_n(s)$ (см. (43)) при $s < n$ ($P_n(s) = 1$ при $s \geq n \geq 0$) можно использовать рекуррентные соотношения, которые легко выводятся из формулы свертки и из первого представления в (35). Именно, если воспользоваться равенством

$$\left(1 - \left(\frac{z}{q}\right)^s\right)^{-\psi_s} = \sum_{r=0}^{\infty} \binom{\psi_s + r - 1}{r} \left(\frac{z}{q}\right)^{sr}, \qquad |z| < q,$$

то получим прямую рекурренту

$$P_n(s) = \sum_{r=0}^{[n/s]} \binom{\psi_s + r - 1}{r} q^{-sr} P_{n-sr}(s-1), \qquad s = 2, 3, \ldots, n-1, \qquad (\text{П}.12)$$

с начальным условием

$$P_n(1) = \binom{\psi_1 + n - 1}{n} q^{-n}.$$

Однако более удобна для использования обратная рекуррента

$$P_n(s-1) = \sum_{r=0}^{[n/s] \wedge \psi_s} (-1)^r \binom{\psi_s}{r} q^{-sr} P_{n-sr}(s), \qquad (\text{П}.13)$$

которая следует из представления

$$\prod_{i=1}^{s-1} \left(1 - \left(\frac{z}{q}\right)^i\right)^{-\psi_i} = \left(1 - \left(\frac{z}{q}\right)^s\right)^{\psi_s} \prod_{i=1}^{s} \left(1 - \left(\frac{z}{q}\right)^i\right)^{-\psi_i}.$$

Так, в частности, как следует из (П.13), при $n/2 < s \leq n$

$$P_n(s-1) = P_n(s) - \frac{\psi_s}{q^s},$$

откуда получаем формулу

$$P_n(s-1) = 1 - \sum_{r=s}^{n} \frac{\psi_r}{q^r}, \qquad \frac{n}{2} < s \leq n. \qquad (\text{П}.14)$$

Отметим, что из (П.14) с учетом (П.4) также следует асимптотическая формула (56).

Аналогично, при $n/3 < s \le n/2$ в (П.13) "работают" лишь три первых члена, и при этом

$$P_{n-2s}(s) = 1,$$

т.е. здесь

$$P_n(s-1) = P_n(s) - \psi_s q^{-s} P_{n-s}(s) + \binom{\psi_s}{2} q^{-2s},$$

или

$$P_n(s-1) = P_n\left(\left[\frac{n}{2}\right]\right) - \sum_{r=s}^{[n/2]} \psi_r q^{-r} P_{n-r}(r) + \sum_{r=s}^{[n/2]} \binom{\psi_r}{2} q^{-2r}.$$

Для вероятностей $P_n([n/2])$ и $P_{n-r}(r)$ здесь можно использовать представление (П.14) и получить формулу

$$P_n(s-1) = 1 - \sum_{r=s}^{n} \psi_r q^{-r} + \sum_{r=s}^{[n/2]} \psi_r q^{-r} \sum_{j=r+1}^{n-r} \psi_j q^{-j} + \sum_{r=s}^{[n/2]} \binom{\psi_r}{2} q^{-2r}, \qquad (\text{П.15})$$

$$\frac{n}{3} < s \le \frac{n}{2}.$$

Из этой формулы и (П.4) следует также, что при $n \to \infty$

$$P_n(s-1) = 1 - \sum_{r=s}^{n} \psi_r q^{-r} + \frac{1}{2} \sum_{\substack{r+j \le n \\ r,j \ge s}} \frac{\psi_r \psi_j}{q^r q^j} + O\left(n^{-2}\right),$$

что, как нетрудно видеть, эквивалентно (57).

Подобный анализ, в принципе, можно продолжить и дальше, последовательно опускаясь по зонам $n/(r+1) < s \le n/r$, хотя с ростом r аналитические сложности быстро нарастают.

Наконец, отметим, что если ввести числа

$$N(n,s) = q^n P_n(s),$$

представляющие собой числа многочленов степени n над полем $\mathrm{GF}(q)$, все неприводимые сомножители которых имеют степени не выше s, то для них из (П.12) и (П.13) следуют аналогичные рекуррентные формулы: прямая

$$N(n,s) = \sum_{r=0}^{[n/s]} \binom{\psi_s + r - 1}{r} N(n - sr,\, s-1),$$

и обратная

$$N(n, s-1) = \sum_{r=0}^{[n/s] \wedge \psi_s} (-1)^r \binom{\psi_s}{r} N(n - sr,\, s).$$

СПИСОК ЛИТЕРАТУРЫ

1. *Лидл Р., Нидеррайтер Г.* Конечные поля. Т. 1, 2. — М.: Мир, 1988.
2. *Гончаров В. Л.* Из области комбинаторики. — Известия АН СССР, 1944, т. 8, №1, с. 3–48.
3. *Колчин В. Ф.* Случайные отображения. — М.: Наука, 1984.
4. *Odlyzko A. M.* Discrete logarithms in finite fields and their cryptographic significance. — In: Lect. Notes Comput. Sci., 1985, v. 209, p. 224–314.
5. *Федорюк М. В.* Метод перевала. — М.: Наука, 1977.
6. *Степанов В. Е.* Предельные распределения некоторых характеристик случайных отображений. — Теория вероятн. и ее примен., 1969, т. 14, в. 4, с. 639–653.
7. *Arratia R., Barbour A. D., Tavaré S.* On random polynomials over finite fields. — Math. Proc. Cambridge Phil. Soc., 1993, v. 114, №2, p. 347–368.
8. *Hansen J. C.* Factorization in $F_q[x]$ and Brownian motion combinatorics. — Comb., Probab. and Comp., 1993, v. 2, p. 285–299.
9. *Ивченко Г. И., Медведев Ю. И.* Случайные многочлены над конечным полем. — Теория вероятн. и ее примен., 1996, т. 41, в. 1, с. 204–210.