Math-Net.Ru

Общероссийский математический портал

Г. И. Ивченко, Ю. И. Медведев, Случайные многочлены над конечным полем,
Дискрет. матем., 2008, том 20, выпуск 1, 3–24

DOI: <https://doi.org/10.4213/dm985>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и
согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.197.130.99

26 апреля 2023 г., 07:11:35

Случайные многочлены над конечным полем

© 2008 г. Г. И. Ивченко, Ю. И. Медведев

Рассматриваются нормированные (со старшим коэффициентом 1) многочлены фиксированной степени n над произвольным конечным полем $GF(q)$, где $q \geq 2$ — простое число или степень простого числа. Предполагается, что на множестве $\mathcal{F}_n = \{f_n\}$ всех q^n таких многочленов задана равномерная мера, приписывающая каждому многочлену вероятность q^{-n} . Для произвольного многочлена $f_n \in \mathcal{F}_n$ определяется его локальная структура $\mathcal{H}_n = \mathcal{H}(f_n)$ как совокупность кратностей всех неприводимых сомножителей в каноническом разложении f_n , и изучаются различные структурные характеристики многочлена (их точные и асимптотические при $n \rightarrow \infty$ распределения), представляющие собой функционалы от $\mathcal{H}_n$. Формулируются направления возможных дальнейших исследований.

1. Введение

Для произвольного многочлена

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

его каноническое разложение в произведение неприводимых над полем $GF(q)$ сомножителей может быть записано в виде

$$f_n = \prod_{i=1}^n \prod_{j=1}^{\psi_i} \varphi_{ij}^{k_{ij}}, \quad (1)$$

где $\varphi_{i1}, \dots, \varphi_{i\psi_i}$ — занумерованные в произвольном порядке все нормированные неприводимые многочлены степени i , $\psi_i = \psi_i(q)$ — число таких многочленов (вид и свойства этих чисел известны и приводятся в приложении) и $k_{ij} \geq 0$ — кратность вхождения многочлена φ_{ij} в каноническое разложение (1).

Кратности k_{ij} подчиняются очевидному условию

$$\sum_{i=1}^n i \sum_{j=1}^{\psi_i} k_{ij} = n, \quad (2)$$

их совокупность обозначается

$$\mathcal{H}_n = \mathcal{H}(f_n) = \{k_{ij}, i = 1, \dots, n, j = 1, \dots, \psi_i\}$$

и называется локальной структурой (ЛС) многочлена f_n , а любой функционал от $\mathcal{H}_n$ — его структурной характеристикой.

Простейшими структурными характеристиками многочлена f_n являются его локальные кратности k_{ij} . Приведем список наиболее важных структурных характеристик интегрального типа, которые будут далее предметом нашего внимания:

$k_i = \sum_{j=1}^{\psi_i} k_{ij}$ — число множителей (с учетом их кратностей) степени i в каноническом разложении (1), или i -я интегральная кратность, $i = 1, \dots, n$;

$k = \sum_{i=1}^n k_i = \sum_{i,j} k_{ij}$ — общее число множителей (с учетом их кратностей) в (1);

$k_i^+ = \max_j k_{ij}$ — максимальная кратность множителей степени i ;

$r_i = \sum_{j=1}^{\psi_i} I(k_{ij} \geq 1)$ — число различных множителей степени i (здесь и далее $I(A)$ — индикатор события A);

$r = \sum_{i=1}^n r_i$ — общее число различных множителей в (1);

$i_{\max}$ (соответственно $i_{\min}$) — максимальная (соответственно минимальная) степень неприводимого множителя в (1), и вообще,

$i_{\min} = i_1 < i_2 < \dots < i_{\max}$ — вариационный ряд различных степеней неприводимых множителей канонического разложения многочлена f_n ;

$k_{\max}$ (соответственно $k_{\min}$) — число множителей с максимальной (соответственно минимальной) степенью;

$l_1 = \sum_{i=1}^n I(k_i \geq 1)$ — число различных степеней, присутствующих в (1), и более общо,

$l_r = \sum_{i=1}^n I(k_i \geq r)$ — число степеней, представленных по крайней мере r сомножителями φ_{ij} каждая;

$m_r = l_r - l_{r+1} = \sum_{i=1}^n I(k_i = r)$ — число степеней, представленных ровно r сомножителями каждая, $r = 1, 2, \dots$;

$k_{(1)} \leq k_{(2)} \leq \dots \leq k_{(n)}$ — вариационный ряд интегральных кратностей, получаемый расположением чисел $k_1, \dots, k_n$ в порядке их возрастания;

$d = \sum_{i,j} I(k_{ij} \geq 2)$ — число кратных множителей в (1).

Отметим, что характеристика k_1 — число линейных множителей — определяет число корней многочлена f_n в поле $GF(q)$, а r_1 — число различных из них.

Для наглядности ЛС $\mathcal{H}_n$ можно представить в виде следующей n -строчной таблицы, имеющей трапецевидную форму (длины ее строк, то есть числа ψ_i , с ростом i возрастают приближенно как q^i/i):

i	j	1	2	...	ψ_n	k_i	r_i
1		k_{11}	k_{12}	...	$k_{1\psi_1}$	k_1	r_1
2		k_{21}	k_{22}	...	$k_{2\psi_2}$	k_2	r_2
				...			
n		k_{n1}	k_{n2}	...	$k_{n\psi_n}$	k_n	r_n
Σ						k	r

Отметим следующие свойства этой таблицы, являющиеся очевидными следствиями условия (2):

$\sum_{i>n/2} k_i \leq 1$, то есть во всей нижней половине таблицы может присутствовать самое

большее одна единица (в разложение (1) может входить лишь один сомножитель степени, большей $n/2$);

$\sum_{n/3 < i \leq n/2} k_i \leq 2$, то есть в строках с номерами $i \in (n/3, n/2]$ может присутствовать лишь

одна двойка либо самое большее лишь две единицы, и в этой зоне число ненулевых строк не может быть больше двух;

в общем случае, если рассматривать зону таблицы, включающую строки с номерами $i \in (n/(s+1), n/s]$ для $s = 1, 2, \dots$, то здесь могут встретиться локальные кратности k_{ij} лишь со значениями, не большими s , причем число ненулевых строк не может быть больше s (в разложение (1) может входить самое большее s сомножителей степени, большей $n/(s+1)$, но не большей n/s).

Таким образом, нижняя часть таблицы $\mathcal{H}_n$ в описанном смысле весьма сильно структурирована, и по мере подъема вверх по зонам $(n/(s+1), n/s]$, $s = 1, 2, \dots$, возможные заполнения ее строк становятся все разнообразнее.

Эти и другие общие особенности ЛС $\mathcal{H}_n$ могут быть выражены в соответствующих вероятностных утверждениях, если предположить, что многочлен f_n является случайным, выбираемым с равной вероятностью из множества $\mathcal{F}_n$ всех q^n нормированных многочленов степени n . Как хорошо известно, подобная модель является эффективным инструментом решения различных перечисленных задач, в которых требуется подсчитать (или хотя бы оценить) число многочленов в $\mathcal{F}_n$, обладающих заданными структурными свойствами. Напомним кратко общую схему решения таких задач.

Пусть S есть заданный комплекс условий на значения тех или иных структурных характеристик многочлена $f_n \in \mathcal{F}_n$ и $A_n(S) \subset \mathcal{F}_n$ — множество всех многочленов из $\mathcal{F}_n$, обладающих свойством S . Тогда для числа $N_n(S) = |A_n(S)|$ таких многочленов справедливо соотношение $N_n(S)/q^n = \mathbf{P}(f_n \in A_n(S))$, сводящее задачу вычисления $N_n(S)$ к определению вероятности соответствующего случайного события. Для решения же последней задачи можно использовать хорошо развитый аппарат современной теории вероятностей, включая предельные (при $n \rightarrow \infty$) теоремы, позволяющие получать приближенные оценки для чисел $N_n(S)$ при больших значениях n .

Для случайного многочлена f_n все его структурные характеристики становятся случайными величинами, которые в дальнейшем обозначаются соответствующими заглавными буквами, снабженными аргументом n . Например, локальные кратности будут обозначаться $K_{ij}(n)$, случайная величина $K(n)$ будет обозначать общее число сомножителей канонического разложения случайного многочлена, $R_i(n)$ — это число различных сомножителей степени i и т. д.

Наряду с таблицей $\mathcal{K}_n = \{K_{ij}(n)\}$ случайного многочлена f_n мы будем рассматривать аналогичную таблицу $\mathcal{K}'_n = \{K_{ij}, i = 1, \dots, n, j = 1, \dots, \psi_i\}$, составленную из независимых в совокупности геометрически распределенных случайных величин, где K_{ij} имеет геометрическое распределение $Ge(q^{-i})$ при всех $j = 1, \dots, \psi_i$:

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

Введем соответствующую бесконечную таблицу $\mathcal{K}' = \{K_{ij}, i = 1, 2, \dots, j = 1, \dots, \psi_i\}$ из независимых геометрически распределенных случайных величин.

Оказывается (это раскрывается ниже), что асимптотически (при $n \rightarrow \infty$) ЛС $\mathcal{K}_n$ случайного многочлена $f_n \in \mathcal{F}_n$ во многом (но не во всем) устроена так же, как таблица $\mathcal{K}'_n$, и даже (в некоторых аспектах) как бесконечная таблица $\mathcal{K}'$.

В дальнейшем распределение случайной величины ξ обозначается символом $\mathcal{L}(\xi)$, так что, например, $\mathcal{L}(K_{ij}) = Ge(q^{-i})$, $\mathcal{L}\left(K_i = \sum_{j=1}^{\psi_i} K_{ij}\right) = \overline{Bi}(\psi_i, q^{-i})$ — отрицательное биномиальное распределение с параметрами ψ_i и q^{-i} , задаваемое вероятностями

$$\mathbf{P}(K_i = r) = \binom{\psi_i + r - 1}{r} q^{-ir}(1 - q^{-i})^{\psi_i}, \quad r = 0, 1, \dots$$

Литература по случайным многочленам над конечными полями достаточно обширна, хотя история вопроса насчитывает лишь два с небольшим десятилетия. Интерес к ним инспирирован рядом практических проблем, связанных, в частности, с задачами защиты информации. Первые фундаментальные результаты в этой проблематике были получены В. Е. Степановым (1983 г.), который для случая поля $GF(2)$ разработал аналитический аппарат исследования асимптотического (при $n \rightarrow \infty$) поведения распределений ряда структурных характеристик случайного многочлена. Случай произвольного поля $GF(q)$, $q \geq 2$, был рассмотрен в последующем В. Н. Сачковым (1986 г.), который получил ряд общих результатов при различных ограничениях на структуру канонического разложения многочлена. Различным частным и общим задачам исследования структурных свойств случайных многочленов посвящены также работы [1–9], результаты которых отражены в настоящем обзоре.

2. Исходные соотношения

Для совместного распределения локальных кратностей $\{K_{ij}(n), (i, j) \in S\}$, где S — произвольное заданное подмножество пар индексов в таблице (ЛС) $\mathcal{K}_n$, имеет место общее соотношение (см. [4, 12])

$$\mathbf{P}(K_{ij}(n) \geq r_{ij}, (i, j) \in S) = q^{-r} I(r \leq n), \quad r = \sum_{(i,j) \in S} ir_{ij}. \quad (3)$$

Следствием (3) является формула

$$\mathbf{P}(K_{ij}(n) \geq s) = q^{-is} I(is \leq n), \quad (4)$$

означающая, что случайная величина $K_{ij}(n)$ имеет усеченное сверху в точке $[n/i]$ геометрическое распределение $Ge(q^{-i})$ (здесь и далее $[a]$ означает целую часть числа a); при $i > n/2$ это распределение является бернуллиевским с параметром q^{-i} .

Из (4) также следует, что вероятность вхождения данного неприводимого многочлена φ_{ij} степени $i \leq n$ в каноническое разложение (1) случайного многочлена f_n есть

$$\mathbf{P}(K_{ij}(n) \geq 1) = q^{-i},$$

а средняя кратность его вхождения есть

$$\mathbf{E}K_{ij}(n) = \frac{1 - q^{-i[n/i]}}{q^i - 1},$$

что при больших n и i эквивалентно q^{-i} .

Далее, из (4) для расстояния по вариации между распределениями случайных величин $K_{ij}(n)$ и K_{ij} следует соотношение

$$\sigma(K_{ij}(n), K_{ij}) = \frac{1}{2} \sum_s |\mathbf{P}(K_{ij}(n) = s) - \mathbf{P}(K_{ij} = s)| = q^{-i([n/i]+1)},$$

показывающее близость распределений этих случайных величин при больших значениях n во всем диапазоне изменения пар индексов (i, j) . Отсюда также следует, что при больших n появление в ЛС $\mathcal{K}_n$ отличных от нуля кратностей $K_{ij}(n)$ с большими значениями индекса i (то есть присутствие в каноническом разложении (1) случайного многочлена сомножителей высоких степеней) будут редкими событиями.

Более того, для событий

$$A_{is}(n) = \bigcup_{j=1}^{\psi_i} \{K_{ij}(n) \geq s\}, \quad A_s^b(n) = \bigcup_{b < i \leq n} A_{is}(n), \quad s = 1, 2,$$

оказывается, что

$$\mathbf{P}(A_{i1}(n)) < \frac{1}{i}, \quad \mathbf{P}(A_{i2}(n)) < \frac{1}{iq^i},$$

а

$$\mathbf{P}(A_2^b(n)) < \sum_{b < i \leq [n/2]} \frac{1}{i} q^{-i}, \quad b < \frac{n}{2}.$$

Следовательно, если $n \rightarrow \infty$, то $\mathbf{P}(A_{i1}(n)) \rightarrow 0$ с ростом i (вероятность присутствия в i -й строке таблицы $\mathcal{K}_n$ хотя бы одного ненулевого элемента мала для больших i), а также $\mathbf{P}(A_2^b(n)) \rightarrow 0$ при $b = b(n) \rightarrow \infty$ сколь угодно медленно (вероятность присутствия в нижней части таблицы $\mathcal{K}_n$, включающей строки с номерами $i > b$, хотя бы одного элемента, не меньшего 2, будет мала при больших b). Особенно важно последнее свойство ЛС $\mathcal{K}_n$ (ввиду его интегрального характера), которое, в свою очередь, может быть значительно усилено до следующего утверждения [12].

Введем случайную величину

$$D(n) = \sum_{i=1}^n \sum_{j=1}^{\psi_i} I(K_{ij}(n) \geq 2),$$

представляющую собой число элементов в $\mathcal{K}_n$, принявших значение, не меньшее 2, и аналогичную случайную величину

$$D = \sum_{i=1}^{\infty} \sum_{j=1}^{\psi_i} I(K_{ij} \geq 2)$$

для бесконечной совокупности $\mathcal{K}'$ независимых геометрически распределенных случайных величин.

Тогда справедливо следующее утверждение.

Теорема 1. Если $n \rightarrow \infty$, то $\mathcal{L}(D(n)) \rightarrow \mathcal{L}(D)$.

Поскольку случайная величина D является собственной (ряд для D сходится с вероятностью 1), то эта теорема означает, что число элементов, не меньших 2, во всей таблице $\mathcal{K}_n$ остается в асимптотике конечным. Другими словами, за исключением лишь конечного числа членов в верхней части таблицы $\mathcal{K}_n$, все остальные ее члены в асимптотике (при $n \rightarrow \infty$) с вероятностью, близкой к 1, принимают лишь значения 0 и 1, то есть являются асимптотически бернуллиевскими.

Теорема 1 позволяет, в частности, оценить вероятность того, что многочлен f_n будет свободен от квадратов, то есть будет раскладываться в произведение различных неприводимых множителей. Именно, при $n \rightarrow \infty$

$$\begin{aligned} \mathbf{P}(f_n \text{ свободен от квадратов}) &= \mathbf{P}(D(n) = 0) \rightarrow \mathbf{P}(D = 0) \\ &= \prod_{i=1}^{\infty} \prod_{j=1}^{\psi_i} \mathbf{P}(K_{ij} \leq 1) = \prod_{i=1}^{\infty} (1 - q^{-2i})^{\psi_i} = 1 - q^{-1}. \end{aligned} \quad (5)$$

Приведенные результаты во многом проясняют асимптотическую (при $n \rightarrow \infty$) картину в нижней части $\mathcal{K}_n^b = \{K_{ij}(n), i > b, j = 1, \dots, \psi_i\}$, то есть при $b = b(n) \rightarrow \infty$ (сколько угодно медленно), таблицы $\mathcal{K}_n$. Дополнительную информацию об этом дает рассмотрение хвостовых случайных величин таких, как

$$\text{сумма } K^b(n) = \sum_{i>b} \sum_{j=1}^{\psi_i} K_{ij}(n) = \sum_{i>b} K_i(n) \text{ всех локальных (или интегральных) кратностей в } \mathcal{K}_n^b,$$

$$\text{число } R^b(n) = \sum_{i>b} \sum_{j=1}^{\psi_i} I(K_{ij}(n) \geq 1) \text{ ненулевых элементов в } \mathcal{K}_n^b,$$

$$\text{число } R_1^b(n) = \sum_{i>b} \sum_{j=1}^{\psi_i} I(K_{ij}(n) = 1) \text{ единиц в } \mathcal{K}_n^b,$$

$$\text{число } L_1^b(n) = \sum_{i>b} I(K_i(n) \geq 1) \text{ ненулевых интегральных кратностей в } \mathcal{K}_n^b,$$

число $M_1^b(n) = \sum_{i>b}^n I(K_i(n) = 1)$ единичных интегральных кратностей в $\mathcal{K}_n^b$.

Математические ожидания всех этих случайных величин ведут себя асимптотически (при $n, b \rightarrow \infty$) одинаково, именно, как $\ln(n/b)$, то есть при $b = o(n)$ эти случайные величины в среднем неограниченно возрастают (в $\mathcal{K}_n^b$ в среднем присутствует много единичных элементов, но разбросанных по разным строкам), а при $b \sim \alpha n$, $0 < \alpha < 1$, эти средние в пределе равны $\ln(1/\alpha)$. Более того, в последнем случае указанные случайные величины имеют собственное предельное распределение, указанное в следующей теореме [12].

Теорема 2. . При $n \rightarrow \infty$ и $b = b(n) \sim \alpha n$, $0 < \alpha < 1$, случайные величины $K^b(n)$, $R^b(n)$, $R_1^b(n)$, $L_1^b(n)$ и $M_1^b(n)$ имеют одно и то же предельное распределение, задаваемое производящей функцией

$$P_\alpha(t) = 1 + \sum_{1 \leq k < 1/\alpha} \frac{(t-1)^k}{k!} \mathcal{J}_k(\alpha), \quad (6)$$

где

$$\mathcal{J}_k(\alpha) = \int \frac{dx_1 \dots dx_k}{x_1 \dots x_k}, \quad k = 1, 2, \dots$$

и интегрирование проводится по области $\{x_1 + \dots + x_k \leq 1, \quad x_1 \geq \alpha, \dots, x_k \geq \alpha\}$.

Добавим к этому, что функция $P_\alpha(t)$ в (6) является многочленом степени $[1/\alpha]$, тем самым предельное распределение сосредоточено в точках $0, 1, \dots, [1/\alpha]$, а при $\alpha > 1/2$ оно является бернуллиевским; среднее значение предельного распределения есть

$$P'_\alpha(1) = \mathcal{J}_1(\alpha) = \ln \frac{1}{\alpha},$$

и оно совпадает с предельным значением $\mathbf{E}K^b(n)$.

Для сравнения отметим, что аналогичные характеристики $K'^b(n)$, $R'^b(n)$, $R_1'^b(n)$, $L_1'^b(n)$ и $M_1'^b(n)$ для совокупности $\mathcal{K}_n^b = \{K_{ij}, b < i \leq n, j = 1, \dots, \psi_i\}$ независимых геометрически распределенных случайных величин, также асимптотически совпадающие при $n, b \rightarrow \infty$, имеют при $b \sim \alpha n$, $0 < \alpha < 1$, в качестве предельного распределения распределение Пуассона с параметром $\ln(1/\alpha)$. Таким образом, для таких значений границы b зависимостью в $\mathcal{K}_n^b$ в асимптотике пренебрегать нельзя.

Обратимся теперь к верхней части $\mathcal{K}_{n,b} = \{K_{ij}(n), i \leq b, j = 1, \dots, \psi_i\}$ таблицы $\mathcal{K}_n$. Ее асимптотическое строение определяется следующим утверждением [12].

Теорема 3. Если $n \rightarrow \infty$, то для любого $b \leq b^* = [n/\ln n]$ распределение совокупности $\mathcal{K}_{n,b}$ асимптотически совпадает с распределением соответствующей совокупности $\mathcal{K}'_b = \{K_{ij}, i \leq b, j = 1, \dots, \psi_i\}$, независимых геометрически распределенных случайных величин. Другими словами, при $i \leq b^*$ случайные величины $K_{ij}(n)$ в совокупности асимптотически независимы и $\mathcal{L}(K_{ij}(n)) \rightarrow \text{Ge}(q^{-i})$ для всех j .

Суммируя изложенное, можно нарисовать следующую общую картину. Пусть $n \rightarrow \infty$ и $b^* = [n/\ln n]$. Тогда верхняя часть $\mathcal{K}_{n,b^*} = \{K_{ij}(n), i \leq b^*\}$ таблицы $\mathcal{K}_n$ — локальной

структуры случайного многочлена f_n — асимптотически устроена так же, как соответствующая совокупность $\mathcal{K}'_{b^*} = \{K_{ij}, i \leq b^*\}$ независимых геометрически распределенных случайных величин. В нижней же части $\mathcal{K}_n^{b^*} = \{K_{ij}(n), b^* < i \leq n\}$ таблицы $\mathcal{K}_n$ с вероятностью, близкой к 1, все локальные кратности $K_{ij}(n)$ принимают лишь значения 0 и 1 (для значений $i > n/2$ они в точности бернуллиевские), при этом число ненулевых кратностей в среднем ведет себя как $\ln \ln n$, и эти редкие единичные значения разбросаны по разным строкам. Еще ниже, то есть в зоне $\mathcal{K}_n^b$ при $b \sim \alpha n$, $0 < \alpha < 1$, число единиц асимптотически конечно, но зависимость между локальными кратностями здесь в асимптотике сохраняется. Общее же число элементов таблицы $\mathcal{K}_n$ со значениями, не меньшими 2, асимптотически конечно, и такие значения присутствуют лишь в верхней части таблицы; при этом с вероятностью, указанной в (5), таблица $\mathcal{K}_n$ будет состоять вообще лишь из 0 и 1. Более подробная детализация асимптотического строения ЛС $\mathcal{K}_n$ дается в последующих разделах.

3. Производящие функции

Основным аналитическим инструментом исследования структуры $\mathcal{K}_n$ случайного многочлена является аппарат производящих функций в сочетании с использованием теории вычетов и метода перевала. Основная производящая функция, то есть совместная производящая функция для всей ЛС $\mathcal{K}_n$, имеет вид [6]

$$\begin{aligned} A_n(t_{ij}, i = 1, \dots, n, j = 1, \dots, \psi_i) &= \mathbf{E} \prod_{i,j} t_{ij}^{K_{ij}(n)} = [z^n] \prod_{i \geq 1} \prod_{j=1}^{\psi_i} (1 - t_{ij}(z/q)^i)^{-1} \\ &= [z^n] \frac{1}{1-z} \prod_{i \geq 1} \prod_{j=1}^{\psi_i} \frac{1 - (z/q)^i}{1 - t_{ij}(z/q)^i}, \end{aligned} \quad (7)$$

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

Отсюда, придавая переменным t_{ij} соответствующие конкретные значения, можно получать производящие функции для конкретных структурных характеристик. Приведем некоторые примеры.

Полагая в (7) все $t_{ij} = 1$ при $i > r$, получим совместную производящую функцию для совокупности $\mathcal{K}_{n,r} = \{K_{ij}(n), i = 1, \dots, r, j = 1, \dots, \psi_i\}$

$$\mathbf{E} \prod_{i=1}^r \prod_{j=1}^{\psi_i} t_{ij}^{K_{ij}(n)} = [z^n] \frac{1}{1-z} \prod_{i=1}^r \prod_{j=1}^{\psi_i} \frac{1 - (z/q)^i}{1 - t_{ij}(z/q)^i}. \quad (8)$$

Если положить в (7) $t_{ij} = t_i$ при всех i, j , то для интегральных кратностей

$$K_i(n) = \sum_{j=1}^{\psi_i} K_{ij}(n), \quad i = 1, \dots, n,$$

получим совместную производящую функцию

$$A_n(t_1, \dots, t_n) = \mathbf{E} \prod_{i=1}^n t_i^{K_i(n)} = [z^n] \frac{1}{1-z} \prod_{i \geq 1} \left(\frac{1 - (z/q)^i}{1 - t_i(z/q)^i} \right)^{\psi_i}. \quad (9)$$

В свою очередь, из (8) и (9) легко следуют произвольные маргинальные производящие функции для отдельных кратностей и их наборов, с помощью которых можно получать точные распределения и моменты конкретных характеристик. Проиллюстрируем это несколькими конкретными результатами.

Из производящей функции (8) следует, что при $r = 1$

$$\begin{aligned} \mathbf{E} \prod_{j=1}^q t_j^{K_{1j}(n)} &= \sum_{m_1, \dots, m_q} t_1^{m_1} \dots t_q^{m_q} [z^{n-m}] \frac{(1-z/q)^q}{1-z} \\ &= \sum_{m_1, \dots, m_q} q^{-m} \sum_{j=0}^{n-m} (-1)^j \binom{q}{j} q^{-j} t_1^{m_1} \dots t_q^{m_q}, \end{aligned}$$

где $m = m_1 + \dots + m_q$. Отсюда следует, что совместное распределение кратностей $K_{1j}(n)$, $j = 1, \dots, q$, имеет вид

$$\mathbf{P}(K_{1j}(n) = m_j, j = 1, \dots, q) = q^{-m} \sum_{j=0}^{n-m} (-1)^j \binom{q}{j} q^{-j},$$

где $m = m_1 + \dots + m_q$. Маргинальные же распределения этих случайных величин (они одинаково распределены) и их моменты находятся из производящей функции

$$Q(t) = \mathbf{E} t^{K_{11}(n)} = [z^n] \frac{1-z/q}{(1-z)(1-tz/q)} = \sum_{j=0}^{n-1} (1-q^{-1}) q^{-j} t^j + q^{-n} t^n$$

и ее производных в точке $t = 1$

$$\mathbf{E}(K_{11}(n))_r = Q^{(r)}(1) = \frac{r!}{q^r} [z^{n-r}] \frac{1}{(1-z)(1-z/q)^r} = \frac{r!}{q^r} \sum_{j=0}^{n-r} \binom{r+j-1}{j} q^{-j},$$

где $(a)_r = a(a-1)\dots(a-r+1)$. Используя эти результаты, можно получить также распределение числа $R_1(n) = \sum_{j=1}^q I(K_{1j}(n) \geq 1)$ различных линейных множителей канонического разложения случайного многочлена f_n или числа различных корней f_n в поле $GF(q)$

$$\mathbf{P}(R_1(n) = r) = \binom{q}{r} q^{-r} \sum_{j=0}^{n-r} \binom{q-r}{j} \left(-\frac{1}{q}\right)^j, \quad r = 0, 1, \dots, q.$$

Факториальные моменты этой случайной величины равны

$$\mathbf{E}(R_1(n))_m = \begin{cases} (q)_m q^{-m}, & m \leq \min(n, q), \\ 0, & m > \min(n, q). \end{cases}$$

В частности, $\mathbf{E} R_1(n) = 1$, то есть при любых n и q в среднем лишь один элемент поля $GF(q)$ является корнем случайного многочлена n -й степени.

Используя производящую функцию (9), получаем следующие представления для распределения случайной величины $K_i(n)$ и ее моментов: при $m = 0, 1, \dots, [n/i]$

$$\mathbf{P}(K_i(n) = m) = \binom{\psi_i + m - 1}{m} q^{-im} \sum_{j=0}^{[n/i]-m} \binom{\psi_i}{j} \left(-\frac{1}{q^i}\right)^j,$$

$$\mathbf{E}(K_i(n))_r = (\psi_i + r - 1)_r q^{-ir} \sum_{j=0}^{[n/i]-r} \binom{r + j - 1}{j} q^{-ij}.$$

Отсюда, в частности, следует, что при $n \rightarrow \infty$ и фиксированном i

$$\mathbf{E}K_i(n) = \frac{\psi_i}{q^i - 1} + O(q^{-n}), \quad \mathbf{D}K_i(n) = \frac{q^i \psi_i}{(q^i - 1)^2} + O(nq^{-n}).$$

4. Предельные теоремы для аддитивных структурных характеристик

В этом разделе излагаются результаты об асимптотическом поведении интегральных кратностей $K_i(n) = \sum_{j=1}^{\psi_i} K_{ij}(n)$, чисел $R_i(n) = \sum_{j=1}^{\psi_i} I(K_{ij}(n) \geq 1)$ различных множителей степени i канонического разложения случайного многочлена f_n и некоторых других, непосредственно связанных с ними, структурных характеристик аддитивного типа.

Непосредственным следствием теоремы 3 являются следующие утверждения [6].

Теорема 4. Если $n \rightarrow \infty$, то случайные величины $K_i(n)$ при $i \leq b^* = [n/\ln n]$ асимптотически независимы и при этом

$$\mathcal{L}(K_i(n)) \sim \mathcal{L}\left(K_i = \sum_{j=1}^{\psi_i} K_{ij}\right) = \bar{Bi}(\psi_i, q^{-i}),$$

где $\bar{Bi}(s, \theta)$ обозначает отрицательное биномиальное распределение с параметрами s и θ . Имеет место также и сходимость моментов, в частности,

$$\mathbf{E}K_i(n) = \frac{\psi_i}{q^i - 1} (1 - q^{-i[n/i]}) \sim \frac{\psi_i}{q^i - 1} = \mathbf{E}K_i.$$

Теорема 5. Если $n \rightarrow \infty$, то случайные величины $R_i(n)$ при $i \leq b^*$ асимптотически независимы и при этом

$$\mathcal{L}(R_i(n)) \sim \mathcal{L}\left(R_i = \sum_{j=1}^{\psi_i} I(K_{ij} \geq 1)\right) = Bi(\psi_i, q^{-i}),$$

где $Bi(s, \theta)$ обозначает биномиальное распределение с параметрами s и θ . Отметим также, что $\mathbf{E}R_i(n) = \psi_i q^{-i} = \mathbf{E}R_i$.

Выделим простейший, но важный частный случай этих теорем для $i = 1$. Как отмечалось во введении, $K_1(n)$ есть число всех корней случайного многочлена f_n в поле $GF(q)$, а $R_1(n)$ — число различных из них. Из сказанного выше следует, что асимптотическое распределение случайной величины $K_1(n)$ является отрицательным биномиальным

$\bar{B}i(q, q^{-1})$ (поскольку $\psi_1 = q$), в то время как для $R_1(n)$ оно оказывается биномиальным $Bi(q, q^{-1})$.

Для любого $i \geq 1$ при $n \rightarrow \infty$

$$\mathbf{E}K_i(n) - \mathbf{E}R_i(n) \sim \frac{\psi_i}{q^i(q^i - 1)},$$

что убывает как q^{-i}/i с ростом i . Это говорит о том, что уже для небольших значений i характеристики $K_i(n)$ и $R_i(n)$ в среднем асимптотически мало отличаются.

Для более глубокого сравнения этих характеристик вводятся в рассмотрение избыточности в строках таблицы $\mathcal{H}_n$, определяемые как разности

$$Z_i(n) = K_i(n) - R_i(n) = \sum_{j=1}^{\psi_i} (K_{ij}(n) - I(K_{ij}(n) \geq 1)) = \sum_{j=1}^{\psi_i} (K_{ij}(n) - 1)^+, \quad (10)$$

где $i = 1, \dots, n$. Здесь и далее $a^+ = \max(0, a)$.

Параллельно с этими характеристиками рассматриваются также избыточности интегральных кратностей

$$\tilde{Z}_i(n) = K_i(n) - I(K_i(n) \geq 1) = (K_i(n) - 1)^+, \quad i = 1, \dots, n. \quad (11)$$

Случайная величина $Z(n) = \sum_{i=1}^n Z_i(n)$ измеряет избыточность всей ЛС $\mathcal{H}_n$, а $\tilde{Z}(n) = \sum_{i=1}^n \tilde{Z}_i(n)$ — избыточность всей совокупности интегральных кратностей $\{K_i(n), i = 1, \dots, n\}$.

Теорема 6. Если $n \rightarrow \infty$, то случайные величины $Z(n)$, $\tilde{Z}(n)$ сходятся по распределению к собственным пределам, соответственно,

$$Z = \sum_{i=1}^{\infty} \sum_{j=1}^{\psi_i} (K_{ij} - 1)^+, \quad \tilde{Z} = \sum_{i=1}^{\infty} (K_i - 1)^+.$$

В то же время $Z(n) = K(n) - R(n)$, где $K(n) = \sum_{i=1}^n K_i(n)$ есть общее число множителей (с учетом их кратностей) канонического разложения случайного многочлена, а $R(n) = \sum_{i=1}^n R_i(n)$ — число различных из них, поэтому теорема 6 означает, что асимптотически числа $K(n)$ и $R(n)$ различаются лишь на конечную величину Z .

Аналогично, $\tilde{Z}(n) = K(n) - L_1(n)$, где $L_1(n) = \sum_{i=1}^n I(K_i(n) \geq 1)$ есть число отличных от нуля интегральных кратностей, другими словами, $L_1(n)$ — это число различных степеней, присутствующих в каноническом разложении случайного многочлена f_n . Теорема 6 говорит о том, что числа $K(n)$ и $L_1(n)$ различаются асимптотически также лишь на конечную величину $\tilde{Z}$.

Рассмотрим теперь характеристики

$$R_i^1(n) = \sum_{j=1}^{\psi_i} I(K_{ij}(n) = 1), \quad i = 1, \dots, n,$$

то есть числа локальных кратностей в строках таблицы $\mathcal{H}_n$, принявших значение 1, в частности, $R_1^1(n)$ есть число простых корней многочлена $f(n)$. Для этих чисел справедлив следующий аналог теоремы 5.

Теорема 7. Если $n \rightarrow \infty$, то случайные величины $R_i^1(n)$ при $i \leq b^*$ асимптотически независимы и при этом

$$\mathcal{L}(R_i^1(n)) \sim \mathcal{L}\left(R_i^1 = \sum_{j=1}^{\psi_i} I(K_{ij} = 1)\right) = Bi(\psi_i, q^{-i}(1 - q^{-i})).$$

Далее, общее число элементов таблицы $\mathcal{K}_n$, принявших значение 1, есть

$$R^1(n) = \sum_{i=1}^n R_i^1(n) = R(n) - D(n), \quad (12)$$

где случайная величина $D(n)$ — число элементов $\mathcal{K}_n$ со значениями, не меньшими 2, — рассмотрена в теореме 1. Из этой теоремы следует, что асимптотически числа $R(n)$ и $R^1(n)$ различаются (так же, как и числа $R(n)$ и $K(n)$) лишь на конечную величину, именно, на величину D .

Введем, наконец, еще одну глобальную структурную характеристику аддитивного типа — число $M_1(n)$ интегральных кратностей, принявших значение 1. Для этой величины справедливо равенство

$$M_1(n) = \sum_{i=1}^n I(K_i(n) = 1) = L_1(n) - L_2(n), \quad (13)$$

где случайная величина $L_1(n)$ введена ранее, а $L_2(n) = \sum_{i=1}^n I(K_i(n) \geq 2)$.

Для $L_2(n)$ справедлив аналог теоремы 1: при $n \rightarrow \infty$ случайная величина $L_2(n)$ сходится по распределению к собственной случайной величине $L_2 = \sum_{i=1}^{\infty} I(K_i \geq 2)$ (случайные величины K_i определены в теореме 4). Тем самым асимптотически числа $L_1(n)$ и $M_1(n)$ различаются (так же, как и числа $L_1(n)$ и $K(n)$) лишь на конечную величину, именно, на величину L_2 .

Таким образом, все пять глобальных аддитивных характеристик ЛС $\mathcal{K}_n$: общее число $K(n)$ множителей канонического разложения случайного многочлена f_n , число $R(n)$ различных множителей, число $R^1(n)$ множителей кратности 1, число $L_1(n)$ ненулевых интегральных кратностей и, наконец, число $M_1(n)$ единичных интегральных кратностей асимптотически отличаются друг от друга лишь на конечные величины (в том смысле, что разности между ними сходятся по распределению при $n \rightarrow \infty$ к собственным случайным величинам).

Такое же заключение справедливо и для более общих характеристик

$$\begin{aligned} K(t; n) &= \sum_{i \leq n^t} K_i(n), & R(t; n) &= \sum_{i \leq n^t} R_i(n), & R_1(t; n) &= \sum_{i \leq n^t} R_i^1(n), \\ L_1(t; n) &= \sum_{i \leq n^t} I(K_i(n) \geq 1), & M_1(t; n) &= \sum_{i \leq n^t} I(K_i(n) = 1) \end{aligned}$$

при любом $t \in [0, 1]$, то есть для соответствующих случайных процессов от параметра t .

Что же касается распределения самих этих характеристик, то имеет место следующее общее утверждение (см. [3, 12]).

Теорема 8. Все пять нормированных процессов

$$\begin{aligned} K^*(t; n) &= (R(t; n) - t \ln n) / \sqrt{\ln n}, & R^*(t; n) &= (R(t; n) - t \ln n) / \sqrt{\ln n}, \\ R_1^*(t; n) &= (R_1(t; n) - t \ln n) / \sqrt{\ln n}, & L_1^*(t; n) &= (L_1(t; n) - t \ln n) / \sqrt{\ln n}, \\ M_1^*(t; n) &= (M_1(t; n) - t \ln n) / \sqrt{\ln n} \end{aligned}$$

слабо сходятся при $n \rightarrow \infty$ к стандартному броуновскому движению $W(t)$ на $[0, 1]$.

Исследована также и скорость сходимости этих процессов к предельному процессу, она имеет порядок $O(\ln \ln n / \sqrt{\ln n})$ (см. [4]).

Подчеркнем также, что эта теорема при $t = 1$ дает асимптотическую нормальность $\mathcal{N}(\ln n, \ln n)$ всех пяти характеристик $K(n)$, $R(n)$, $R^1(n)$, $L_1(n)$ и $M_1(n)$.

Теорема 8 дает следующую картину асимптотического поведения интегральных кратностей: последовательности $\{K_i(n), i = 1, \dots, n\}$, $\{I(K_i(n) \geq 1), i = 1, \dots, n\}$ и $\{I(K_i(n) = 1), i = 1, \dots, n\}$ асимптотически мало различаются, именно, для любого $t > 0$ суммы первых n^t членов этих последовательностей асимптотически имеют один и тот же порядок $t \ln n$. Другими словами, в подавляющем большинстве случаев интегральные кратности с вероятностью, стремящейся к единице при $n \rightarrow \infty$, принимают лишь значения 0 и 1. Правда, для начальных значений индекса i они с положительной вероятностью могут принимать любые конечные значения (как случайные величины, имеющие отрицательное биномиальное распределение), но таковых относительно немного и с ростом i они быстро затухают.

Итак, имеются два типа глобальных структурных характеристик аддитивного вида для ЛС $\mathcal{H}_n$. К первому относятся характеристики, указанные в теореме 8, общим для них является то, что они суммируют события, связанные с единичными значениями кратностей (локальных либо интегральных), таковых же событий реализуется достаточно много и этим обуславливается неограниченный рост соответствующих характеристик. Примерами характеристик второго типа являются избыточности $Z(n)$ и $\tilde{Z}(n)$ (теорема 6), а также $D(n)$ (теорема 1) и $L_2(n)$, они зависят лишь от кратностей со значениями, не меньшими 2, и имеют собственные пределы (без нормировок). К ним можно добавить также характеристики

$$\begin{aligned} K(n) - R^1(n) &= Z(n) + D(n) = \sum_{i,j} K_{ij}(n) I(K_{ij}(n) \geq 2), \\ K(n) - M^1(n) &= \tilde{Z}(n) + L_2(n) = \sum_i K_i(n) I(K_i(n) \geq 2), \\ L_r(n) &= \sum_i I(K_i(n) \geq r), \quad M_r(n) = \sum_i I(K_i(n) = r), \quad r \geq 2. \end{aligned} \quad (14)$$

Для них при $n \rightarrow \infty$ имеют место асимптотические соотношения [12]

$$\begin{aligned} \mathcal{L}(K(n) - R^1(n)) &\rightarrow \mathcal{L}\left(Z + D = \sum_{i=1}^{\infty} \sum_{j=1}^{\psi_i} K_{ij} I(K_{ij} \geq 2)\right), \\ \mathcal{L}(K(n) - M^1(n)) &\rightarrow \mathcal{L}\left(\tilde{Z} + L_2 = \sum_{i=1}^{\infty} K_i I(K_i \geq 2)\right), \\ \mathcal{L}(L_r(n)) &\rightarrow \mathcal{L}\left(L_r = \sum_{i=1}^{\infty} I(K_i \geq r)\right), \quad r \geq 2, \\ \mathcal{L}(M_r(n)) &\rightarrow \mathcal{L}\left(M_r = \sum_{i=1}^{\infty} I(K_i = r)\right), \quad r \geq 2, \end{aligned} \quad (15)$$

где все предельные случайные величины являются собственными.

Прокомментируем, например, первое из этих соотношений. Оно говорит о том, что не только общее число элементов таблицы $\mathcal{H}_n$, принявших значения, не меньшие 2, остается асимптотически конечным (как это утверждается теоремой 1), но также остается в асимптотике конечным и сумма всех таких элементов.

Отметим некоторые важные следствия этих соотношений. Обобщением (5) является следующее утверждение (см. [12]): для любого $r \geq 2$

$$\begin{aligned} \mathbf{P}(f_n \text{ свободен от } r\text{-х кратностей}) &= \mathbf{P}(K_{ij}(n) < r \ \forall (i, j)) = \mathbf{P}\left(\sum_{i,j} I(K_{ij}(n) \geq r) = 0\right) \\ &\rightarrow \mathbf{P}\left(\sum_{i,j} I(K_{ij} \geq r) = 0\right) = \prod_{i=1}^{\infty} \prod_{j=1}^{\psi_i} \mathbf{P}(K_{ij} < r) = \prod_{i=1}^{\infty} (1 - q^{-ir})^{\psi_i} = 1 - q^{-r+1}. \end{aligned} \quad (16)$$

Пусть событие $B(n)$ означает, что случайный многочлен f_n раскладывается в произведение различных неприводимых множителей различных же степеней. Тогда

$$\begin{aligned} \mathbf{P}(B(n)) &= \mathbf{P}(K_i(n) \leq 1 \ \forall i) = \mathbf{P}(L_2(n) = 0) \rightarrow \mathbf{P}(L_2 = 0) \\ &= \mathbf{P}(K_i \leq 1 \ \forall i) = \prod_{i=1}^{\infty} \mathbf{P}(K_i \leq 1) = \prod_{i=1}^{\infty} (1 - q^{-i})^{\psi_i} (1 + \psi_i q^{-i}) = b(q), \end{aligned} \quad (17)$$

в частности, $b(2) = 0,4039 \dots$, $b(3) = 0,48349 \dots$

Рассмотрим, наконец, события $A_r(n) = \{\max_i K_i(n) < r\}$, $r \geq 2$. Для вероятности такого события справедливо соотношение

$$\begin{aligned} \mathbf{P}(A_r(n)) &= \mathbf{P}(K_i(n) < r \ \forall i) = \mathbf{P}(L_r(n) = 0) \rightarrow \mathbf{P}(L_r = 0) \\ &= \prod_{i=1}^{\infty} \mathbf{P}(K_i < r) = \prod_{i=1}^{\infty} \sum_{j < r} \binom{\psi_i + j - 1}{j} q^{-ij} (1 - q^{-i})^{\psi_i}. \end{aligned} \quad (18)$$

5. Предельные теоремы для экстремальных характеристик

5.1. В модели случайного многочлена f_n имеются два типа экстремальных характеристик, связанных с его каноническим разложением (1): экстремальные (то есть минимальное и максимальное) значения степеней неприводимых множителей, присутствующих в разложении (1), и экстремальные значения кратностей этих множителей. Что касается максимальных кратностей (локальных либо интегральных), то из описанных выше общих свойств таблицы $\mathcal{H}_n$ ясно, что асимптотически (при $n \rightarrow \infty$) они с высокой вероятностью будут связаны с начальными строками, то есть максимумами независимых случайных величин. Более того, некоторые из изложенных в разделе 4 результатов могут быть непосредственно интерпретированы в терминах поведения соответствующих экстремальных характеристик.

Так, результат (16) есть одновременно и утверждение об асимптотическом поведении функции распределения случайной величины $K^+(n) = \max_{i,j} K_{ij}(n)$, максимума всех локальных кратностей в таблице $\mathcal{H}_n$ (см. [7]):

$$\mathbf{P}(K^+(n) < r) \rightarrow 1 - q^{-r+1}, \quad r \geq 2. \quad (19)$$

В частности, при $r = 2$ справедливо соотношение

$$\mathbf{P}(K^+(n) = 1) \rightarrow 1 - q^{-1},$$

что является другой формой записи результата (5).

Аналогично, (17)–(18) дают предельную функцию распределения максимума интегральных кратностей.

Добавим следующий простой результат. Пусть $K_i^+(n) = \max_{1 \leq j \leq \psi_i} K_{ij}(n)$ и $K_i^+ = \max_{1 \leq j \leq \psi_i} K_{ij}$, $i = 1, 2, \dots$, тогда

$$\mathbf{P}(K_i^+(n) < r) \rightarrow \mathbf{P}(K_i^+ < r) = (1 - q^{-ir})^{\psi_i}, \quad r = 1, 2, \dots \quad (20)$$

Из (20), в частности, следует, что с ростом i случайная величина $K_i^+(n)$ вырождается в 0: $\mathbf{P}(K_i^+(n) = 0) \approx 1 - 1/i$.

5.2. Рассмотрим более детально вариационный ряд интегральных кратностей $K_i(n)$, $i = 1, \dots, n$ (см. [7]):

$$K_{(1)}(n) \leq K_{(2)}(n) \leq \dots \leq K_{(n-m+1)}(n) \leq \dots \leq K_{(n)}(n). \quad (21)$$

Члены этого ряда связаны с введенными и исследованными в разделе 4 (см. (14)) случайными величинами $L_r(n)$ соотношением

$$\mathbf{P}(K_{(n-m+1)}(n) < r) = \mathbf{P}(L_r(n) < m),$$

с помощью которого можно полностью описать асимптотическое строение вариационного ряда (21). Сначала в (21) долго будут идти нули: $\mathbf{P}(K_{(n-m+1)}(n) = 0) \rightarrow 1$ пока m удовлетворяет условию $(m - \ln n)/\sqrt{\ln n} \rightarrow \infty$ при $n \rightarrow \infty$. При значениях m вида $m = \ln n + x\sqrt{\ln n}$, $|x| \leq c < \infty$,

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

то есть с вероятностью $1 - \Phi(x)$ случайная величина $K_{(n-m+1)}(n)$ будет уже принимать (асимптотически) положительные значения, а при $(m - \ln n)/\sqrt{\ln n} \rightarrow -\infty$ члены ряда (21) с номерами $n - m + 1$ устойчиво становятся положительными. Итак, зону положительных значений в (21) можно описать условием $(m - \ln n)/\sqrt{\ln n} \rightarrow -\infty$; в этой зоне, за исключением некоторого числа крайних правых членов, все остальные члены будут устойчиво равны 1: $\mathbf{P}(K_{(n-m+1)}(n) = 1) \rightarrow 1$, если $m = m(n) \rightarrow \infty$ как угодно медленно; наконец, для любого фиксированного m

$$\mathbf{P}(K_{(n-m+1)}(n) < r) \rightarrow \mathbf{P}(L_r < m), \quad r \geq 2,$$

где случайная величина L_r определена в (15).

Таким образом, значения, большие 1, асимптотически с положительной вероятностью могут присутствовать лишь на самом краю ряда (21). В частности, для максимальной кратности $K_{(n)}(n)$ выполняется соотношение

$$\mathbf{P}(K_{(n)}(n) < r) \rightarrow \mathbf{P}(L_r = 0),$$

где предельная вероятность указана в (18), а вероятность того, что весь ряд (21) будет состоять лишь из 0 и 1, есть

$$\mathbf{P}(K_{(n)}(n) = 1) \rightarrow \mathbf{P}(L_2 = 0),$$

где предельная вероятность дана в (17).

Завершая описание асимптотического строения вариационного ряда (21), добавим к сказанному, что число его членов на правом краю, принявших значения $r = 2, 3, \dots$, есть случайная величина $M_r(n)$ (см. (14)); результат же, указанный в (15), дает ответ на вопрос об асимптотическом поведении этих чисел.

5.3. Обратимся теперь к экстремальным характеристикам, связанным со степенями неприводимых множителей, присутствующих в каноническом разложении (1) случайного многочлена f_n . Общее число различных степеней в (1) есть введенная и описанная в разделе 4 случайная величина $L_1(n) = \sum_{i=1}^n I(K_i(n) \geq 1)$. Обозначим последовательные (в порядке возрастания) значения этих степеней $\mathcal{J}_j(n)$, $j = 1, \dots, L_1(n)$, они образуют возрастающую последовательность натуральных чисел (см. [7])

$$1 \leq \mathcal{J}_1(n) < \mathcal{J}_2(n) < \dots < \mathcal{J}_{L_1(n)}(n) \leq n. \quad (22)$$

Другими словами, числа в ряду (22) — это последовательные номера отличных от нуля интегральных кратностей $K_1(n), \dots, K_n(n)$, так что

$$\mathcal{J}_1(n) = \mathcal{J}_{\min}(n) = \min\{i: K_i(n) \neq 0\}, \quad \mathcal{J}_{L_1(n)}(n) = \mathcal{J}_{\max}(n) = \max\{i: K_i(n) \neq 0\}$$

и, вообще,

$$\mathcal{J}_m(n) = \min\{i > \mathcal{J}_{m-1}(n): K_i(n) \neq 0\}, \quad m = 2, 3, \dots$$

Из определения этих случайных величин следует, что для любых целых $m \geq 1$ и $1 \leq r_1 < \dots < r_m \leq n$

$$\begin{aligned} \mathbf{P}(\mathcal{J}_j(n) = r_j, \quad j = 1, \dots, m) \\ = \mathbf{P}(K_j(n) > 0, \quad j = r_1, \dots, r_m, \quad K_i(n) = 0, \quad 1 \leq i \leq r_m, \quad i \neq r_1, \dots, r_m). \end{aligned}$$

Отсюда по теореме 4 следует, что при $n \rightarrow \infty$

$$\mathbf{P}(\mathcal{J}_j(n) = r_j, \quad j = 1, \dots, m) \rightarrow \prod_i (1 - q^{-i})^{\psi_i} \prod_{j=1}^m (1 - (1 - q^{-r_j})^{\psi_{r_j}}), \quad (23)$$

где первое произведение берется по всем $i = 1, \dots, r_m$, $i \neq r_1, \dots, r_m$.

Отметим также следующий результат: для любых натуральных m и r

$$\mathbf{P}(\mathcal{J}_m(n) \leq r) = \mathbf{P}\left(\sum_{i=1}^r I(K_i(n) \geq 1) \geq m\right),$$

откуда следует, что при $n \rightarrow \infty$

$$\mathbf{P}(\mathcal{J}_m(n) \leq r) = \mathbf{P}\left(\sum_{i=1}^r I(K_i \geq 1) \geq m\right) + o(1). \quad (24)$$

В частности, для минимальной степени $\mathcal{F}_{\min}(n)$ имеет место предельное соотношение

$$\mathbf{P}(\mathcal{F}_{\min}(n) \leq r) = 1 - \prod_{i=1}^r (1 - q^{-i})^{\psi_i} + o(1), \quad (25)$$

в то же время $\mathbf{E}\mathcal{F}_{\min}(n) \rightarrow \infty$ при $n \rightarrow \infty$.

Соотношениями (23)–(25) описывается асимптотическое поведение начальных членов ряда (22). Рассмотрим теперь средние члены этого ряда, которые соответствуют номерам $m \sim t \ln n$ при $0 < t < 1$ (ведь общее число членов ряда (22) имеет порядок $\ln n$, см. теорему 8). Для них справедлива теорема о логарифмической нормальности [7].

Теорема 9. При $n \rightarrow \infty$ и $m = t \ln n + o(\sqrt{\ln n})$, $0 < t < 1$, случайная величина $\ln \mathcal{F}_m(n)$ асимптотически нормальна с параметрами (m, m) .

Наконец, асимптотическое поведение крайних правых членов ряда (22) описывается следующим утверждением [7].

Теорема 10. При $n \rightarrow \infty$ и фиксированном $m \geq 1$

$$\mathbf{P}\left(\frac{1}{n} \mathcal{F}_{L_1(n)-m+1}(n) \leq \alpha\right) \rightarrow \begin{cases} F_m(\alpha), & 0 < \alpha < 1/m, \\ 1, & \alpha \geq 1/m, \end{cases}$$

где функция $F_m(\alpha)$ имеет вид

$$F_m(\alpha) = 1 - \sum_{m \leq k < 1/\alpha} \frac{(-1)^{k-m}}{k(m-1)!(k-m)!} \mathcal{F}_k(\alpha)$$

и $\mathcal{F}_k(\alpha)$ указаны в (6). В частности, для максимальной степени $\mathcal{F}_{\max}(n)$ справедливо соотношение

$$\mathbf{P}\left(\frac{1}{n} \mathcal{F}_{\max}(n) \leq \alpha\right) \rightarrow F_1(\alpha), \quad 0 < \alpha < 1, \quad (26)$$

при этом $\mathbf{E}\mathcal{F}_{\max}(n)/n \rightarrow 0,6243 \dots$

Справедлива также и соответствующая локальная предельная теорема, многомерный вариант которой формулируется следующим образом [7].

Теорема 11. Пусть $r \geq 1$, $0 < \alpha_r < \alpha_{r-1} < \dots < \alpha_1 < 1$ таковы, что $0 < \alpha_1 + \dots + \alpha_r < 1$. Тогда

$$\lim_{n \rightarrow \infty} n^r \mathbf{P}(\mathcal{F}_{L_1(n)-j+1}(n) = [n\alpha_j], j = 1, \dots, r) = \frac{1}{\alpha_1 \dots \alpha_r} F_1\left(\frac{\alpha_r}{1 - \alpha_1 - \dots - \alpha_r}\right).$$

Добавим к этому, что для числа $K_{\max}(n)$ множителей канонического разложения, имеющих максимальную степень $\mathcal{F}_{\max}(n)$, при $n \rightarrow \infty$ выполняется соотношение

$$\mathbf{P}(K_{\max}(n) = 1) \rightarrow 1. \quad (27)$$

Для числа же $K_{\min}(n)$ множителей с минимальной степенью $\mathcal{F}_{\min}(n)$ при $n \rightarrow \infty$ справедливо соотношение

$$\mathbf{P}(K_{\min}(n) = k) = \sum_{i \geq 1} \binom{\psi_i + k - 1}{k} q^{-ik} \prod_{j=1}^i (1 - q^{-j})^{\psi_j} + o(1). \quad (28)$$

Здесь предельное распределение имеет конечное среднее

$$m(q) = \sum_{i \geq 1} \frac{\psi_i}{q^i - 1} \prod_{j=1}^{i-1} (1 - q^{-j})^{\psi_j}, \quad (29)$$

в частности, $m(2) = 0,128 \dots$, $m(3) = 0,061 \dots$

В заключение этой темы отметим, что наряду с рядом (22) можно построить также вариационный ряд степеней всех $K(n)$ множителей канонического разложения, то есть учитывая каждую степень столько раз, какова ее интегральная кратность. Это был бы ряд

$$\mathcal{F}'_1(n) \leq \mathcal{F}'_2(n) \leq \dots \leq \mathcal{F}'_{K(n)}(n), \quad (30)$$

в котором соседние члены могут совпадать. Но такие совпадения с положительной (при $n \rightarrow \infty$) вероятностью могут появляться лишь на левом краю этого ряда, что отразится соответствующим образом на виде предельных распределений его минимальных членов. Так, для m -го минимального члена $\mathcal{F}'_m(n)$ справедливо соотношение

$$\mathbf{P}(\mathcal{F}'_m(n) \leq r) = \mathbf{P}\left(\sum_{i=1}^r K_i \geq m\right) + o(1), \quad (31)$$

являющееся аналогом соотношения (24) для ряда (22). В то же время результат (25) для минимальной степени остается справедливым и для случайной величины $\mathcal{F}'_{\min}(n) = \mathcal{F}'_1(n)$. Также и асимптотические результаты для средних и максимальных членов рядов (30) и (22) идентичны.

Наконец, отметим, что результаты для средних и максимальных членов ряда (22) (теоремы 9 и 10) идентичны аналогичным результатам для вариационного ряда длин циклов случайной n -подстановки (см., например, [10]), в то время как для минимальных членов соответствующие результаты существенно различаются.

6. Другие результаты

В этом разделе приводятся некоторые дополнительные результаты о структурных характеристиках случайного многочлена.

6.1. Максимальная степень $\mathcal{F}_{\max}(n)$ неприводимого сомножителя в каноническом разложении случайного многочлена f_n представляет собой одну из наиболее интересных и важных для приложений его структурных характеристик. Указанный в (26) результат позволяет оценивать вероятности $P_n(s) = \mathbf{P}(\mathcal{F}_{\max}(n) \leq s)$ при $n, s \rightarrow \infty$ так, что $s/n \rightarrow \alpha$, $0 < \alpha < 1$. Однако для приложений представляет также интерес поведение $P_n(s)$ и в зоне $s/n \rightarrow 0$ (в этой зоне $P_n(s) \rightarrow 0$ и речь, следовательно, идет о скорости убывания этих вероятностей). Информацию об этом дают следующие результаты (см. [5]): если $n \rightarrow \infty$, то при фиксированном $s \geq 1$

$$P_n(s) = a_s \frac{n^{\tau_s - 1}}{(\tau_s - 1)!} q^{-n} (1 + O(1/n)), \quad (32)$$

где $\tau_s = \sum_{i=1}^s \psi_i$ и $a_s = \prod_{i=1}^s i^{-\psi_i}$; если же $s = s(n) \rightarrow \infty$ так, что $(\ln s)/\ln n \in [\varepsilon, 1 - \varepsilon]$, где $\varepsilon > 0$ — произвольно малая постоянная, то (см. [6])

$$P_n(s) \sim \frac{1}{\sqrt{2\pi ns}} e^{-H_{s,n}}, \quad (33)$$

где

$$H_{s,n} = \frac{n}{s} \left(\ln \frac{n}{s} + \ln \ln \frac{n}{s} - 1 + O \left(\frac{\ln \ln(n/s)}{\ln(n/s)} \right) \right).$$

Для вычисления точных значений вероятностей $P_n(s)$ при конечных n и $s < n$ ($P_n(s) = 1$ при $s \geq n \geq 0$) можно использовать рекуррентное соотношение

$$P_n(s-1) = \sum_{0 \leq r \leq n/s \wedge \psi_s} (-1)^r \binom{\psi_s}{r} q^{-sr} P_{n-sr}(s),$$

в частности, при $n/2 < s \leq n$

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

при $n/3 < s \leq n/2$

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

6.2. Представляют также интерес условные распределения различных структурных характеристик при условии, что все множители разложения (1) имеют степени, ограниченные сверху некоторым числом s , в различных зонах изменения s . Приведем несколько результатов такого типа (см. [5]).

Теорема 12. Для любого фиксированного $s > 1$ при $n \rightarrow \infty$

$$\mathcal{L} \left(\frac{i}{n} K_i(n), i = 1, \dots, s \mid \mathcal{F}_{\max}(n) \leq s \right) \rightarrow \mathcal{D}(\psi_1, \dots, \psi_s),$$

где $\mathcal{D}$ — распределение Дирихле, в частности,

$$\mathcal{L} \left(\frac{s}{n} K_s(n) \mid \mathcal{F}_{\max}(n) \leq s \right) \rightarrow Be(\psi_s, \tau_{s-1}),$$

где Be — бета-распределение и числа τ_s указаны в (32).

Этот результат говорит о том, что при условии, что $\mathcal{F}_{\max}(n) \leq s$, число сомножителей каждой степени $i = 1, 2, \dots, s$ в разложении (1) имеет порядок $O(n/i)$.

Теорема 13. Пусть $n \rightarrow \infty$, $a = s(n)$ таково, что $(\ln s)/\ln n \in [\varepsilon, 1-\varepsilon]$, где ε — произвольно малое фиксированное положительное число. Тогда условное распределение числа $K(n)$ неприводимых множителей разложения (1) при условии, что все множители этого разложения имеют степени не большие, чем s , асимптотически нормально, именно,

$$\mathcal{L} \left(\frac{\ln(n/s)}{\sqrt{n/s}} \left(K(n) - \sum_{i=1}^s \frac{r^i}{i} \right) \mid \mathcal{F}_{\max}(n) \leq s \right) \rightarrow \mathcal{N}(0, 1),$$

где r — положительный корень уравнения $z + z^2 + \dots + z^s = n$, при этом центрирующая и нормирующая величины здесь являются асимптотическими значениями соответствующих условных моментов и

$$\sum_{i=1}^s \frac{r^i}{i} = \frac{n}{s} \left(1 - \frac{\ln \ln(n/s)}{\ln(n/s)} + \frac{1}{\ln(n/s)} + \frac{2}{\ln^2(n/s)} + O \left(\left(\frac{\ln \ln(n/s)}{\ln(n/s)} \right)^3 \right) \right).$$

Из этой теоремы, в частности, следует, что почти все множители канонического разложения должны иметь степень, близкую к максимально возможной степени s . Далее, в условиях теоремы 13 справедливо соотношение

$$\mathbf{E}(K_i(n) \mid \mathcal{F}_{\max}(n) \leq s) = \psi_i(r/q)^i \frac{1 + o(1)}{1 - (r/q)^i}, \quad i \leq s,$$

если же $i = i(n) \rightarrow \infty$, то правая часть этого соотношения есть $r^i/i(1 + o(1))$. Таким образом, это условное среднее с ростом i сначала уменьшается, достигая минимума при $i \sim s/\ln(n/s)$, а затем увеличивается.

Для среднего числа сомножителей максимальной степени справедливо соотношение

$$\mathbf{E}(K_{\max}(n) \mid \mathcal{F}_{\max}(n) \leq s) \sim \frac{r^s}{s} \sim \frac{n}{s^2} \ln \frac{n}{s}.$$

Последняя величина конечна, если s имеет порядок $\sqrt{n \ln n}$, неограниченно возрастает, если $s/\sqrt{n \ln n} \rightarrow 0$, и стремится к 0, если $s/\sqrt{n \ln n} \rightarrow \infty$.

6.3. Изложенные выше результаты относятся к равновероятной модели случайных многочленов. Представляет интерес рассмотрение и других моделей, допускающих те или иные отклонения от равновероятности. Весьма общей такой моделью является следующая параметрическая модель [8, 9]: на множестве $\mathcal{F}_n$ задается вероятностная мера, зависящая от параметра $\theta = (\theta_1, \dots, \theta_n)$, $\theta_1, \dots, \theta_n \geq 0$, в соответствии с которой произвольный многочлен $f_n \in \mathcal{F}_n$ с интегральными кратностями $K_i(n) = a_i$, $i = 1, \dots, n$, наблюдается с вероятностью, пропорциональной $\prod_i \theta_i^{a_i}$. Именно,

$$\mathbf{P}_\theta(f_n) = I \left(\sum_{i=1}^n i a_i = n \right) \prod_{i=1}^n \theta_i^{a_i} / H_n(\theta), \quad (34)$$

где

$$H_n(\theta) = \sum_{a: \sum_i i a_i = n} \prod_{i=1}^n \binom{\psi_i + a_i - 1}{a_i} \prod_{i=1}^n \theta_i^{a_i} = [z^n] \prod_{i=1}^n (1 - z^i \theta_i)^{-\psi_i}. \quad (35)$$

В модели (34) производящая функция интегральных кратностей $K_i(n)$, $i = 1, \dots, n$, имеет вид

$$A_{n,\theta}(t_1, \dots, t_n) = \mathbf{E}_\theta \prod_{i=1}^n t_i^{K_i(n)} = H_n(t \cdot \theta) / H_n(\theta), \quad (36)$$

где $t \cdot \theta = (t_1 \theta_1, t_2 \theta_2, \dots, t_n \theta_n)$.

Представление (36) сводится к (9), если $\theta_i = 1$, $i = 1, \dots, n$.

Выбирая соответствующим образом значения параметра $\theta = (\theta_1, \theta_2, \dots, \theta_n)$, можно задавать на множестве $\mathcal{F}_n$ различные распределения и тем самым получать возможность исследовать различные неравновероятные модели случайных многочленов, решать для них не только перечисленные задачи, но и проводить их более глубокий вероятностный и статистический анализ.

В заключение отметим одно важное свойство интегральных кратностей в модели (34), которое может быть полезным для анализа (см. [9]): распределение случайных величин

$K_i(n)$, $i = 1, \dots, n$, может быть представлено как условное распределение независимых случайных величин $Z_1, \dots, Z_n$ с отрицательным биномиальным распределением

$$\mathcal{L}_\theta(K_i(n), i = 1, \dots, n) = \mathcal{L}_\theta \left(Z_1, \dots, Z_n \mid \sum_{i=1}^n i Z_i = n \right),$$

где $\mathcal{L}_\theta(Z_i) = \overline{Bi}(\psi_i, \theta_i)$, $\theta_i \in (0, 1)$.

Кроме того, если степень многочлена n специальным образом рандомизировать, то есть рассматривать ее как случайную величину η с распределением

$$\mathbf{P}_\theta(\eta = n) = \frac{H_n(\theta)x^n}{f_\theta(x)}, \quad n = 0, 1, 2, \dots, \quad f_\theta(x) = \prod_{i=1}^{\infty} (1 - x^i \theta_i)^{-\psi_i},$$

то случайные величины $K_i(\eta)$, $i = 1, \dots, n$, оказываются независимыми с распределением $\mathcal{L}_\theta(K_i(\eta)) = \overline{Bi}(\psi_i, x^i \theta_i)$.

Приложение

Приведем основные сведения о числах $\psi_i = \psi_i(q)$ (см., например, гл. 3 в [11]). Эти числа удовлетворяют соотношению

$$\sum_{i|m} i \psi_i = q^m$$

(сумма берется по всем положительным делителям числа m). Точная формула для них имеет вид

$$\psi_i(q) = \frac{1}{i} \sum_{j|i} \mu(i/j) q^j,$$

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

Числа $\psi_i(q)$ удовлетворяют неравенствам

$$\frac{q^i}{i} \left(1 - \frac{q}{q-1} q^{-i/2} \right) < \frac{q^i}{i} - \frac{q}{i(q-1)} (q^{i/2} - 1) \leq \psi_i(q) \leq \frac{q}{i} (q^{i-1} - 1) < \frac{q^i}{i},$$

откуда следует, что равномерно по i

$$i \psi_i(q) = q^i + O(q^{i/2}).$$

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

$$\sum_{i|m, i \leq r} i \psi_i \leq \sum_{i|m, i < m} i \psi_i = \sum_{i|m} i \psi_i - m \psi_m \leq \frac{q}{q-1} (q^{m/2} - 1) < 2q^{m/2}.$$

Далее, для их сумм $\tau_s = \sum_{i=1}^s \psi_i$ имеют место оценки

$$\sum_{i=1}^s \frac{q^i}{i} - \frac{q}{q-1} \sum_{i=1}^s \frac{q^{i/2} - 1}{i} \leq \tau_s \leq \sum_{i=1}^s \frac{q^i}{i} - q \sum_{i=1}^s \frac{1}{i},$$

откуда следует, что равномерно по s

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

Список литературы

1. Odlyzko A. M., Discrete logarithms in finite fields and their cryptographic significance. *Lect. Notes Computer Sci.* (1985) **209**, 224–314.
2. Flajolet P., Soria M., Gaussian limiting distributions for the number of components in combinatorial structures. *J. Comb. Theory, Ser. A* (1990) **53**, №2, 165–182.
3. Hansen J. C., Factorization in $F_q[x]$ and Brownian motion. *Comb. Probab. Comput.* (1993) **2**, №2, 285–299.
4. Arratia R., Barbour A. D., Tavaré S., On random polynomials over finite fields. *Math. Proc. Cambridge Phil. Soc.* (1993) **114**, №2, 347–368.
5. Ивченко Г. И., Медведев Ю. И., Случайные многочлены над конечным полем. *Теория вероятностей и ее применения* (1996) **41**, №1, 204–210.
6. Ивченко Г. И., Медведев Ю. И., О структуре случайных многочленов над конечными полями. *Труды по дискретной математике* (2000) **3**, 111–138.
7. Ивченко Г. И., Медведев Ю. И., Экстремальные характеристики случайного многочлена над конечным полем. *Труды по дискретной математике* (2001) **4**, 71–82.
8. Ивченко Г. И., Медведев Ю. И., Неравновероятные меры на множествах разложимых комбинаторных объектов. *Обзорные прикладной и промышленной математики* (2003) **10**, №2, 348–349.
9. Ивченко Г. И., Медведев Ю. И., Случайные комбинаторные объекты. *Докл. РАН* (2004) **396**, №2, 151–154.
10. Колчин В. Ф., *Случайные отображения*. Наука, Москва, 1984.
11. Лидл Р., Нидеррайтер Г., *Конечные поля*, **1**. Мир, Москва, 1988.
12. Ivchenko G. I., Medvedev Yu. I., Local structure of random polynomials over finite fields. In: *Probab. Methods in Discrete Math.* VSP, Utrecht, 2001, pp. 27–46.

Статья поступила 22.02.2007.