Math-Net.Ru

Общероссийский математический портал

Г. И. Ивченко, Ю. И. Медведев, Случайные многочлены над конечным полем, *Теория вероятн. и ее примен.*, 1996, том 41, выпуск 1, 204–210

DOI: <https://doi.org/10.4213/tvp2795>

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: 18.208.226.222

26 апреля 2023 г., 10:56:40

© 1996 г.

ИВЧЕНКО Г. И.*, МЕДВЕДЕВ Ю. И.*

СЛУЧАЙНЫЕ МНОГОЧЛЕНЫ НАД КОНЕЧНЫМ ПОЛЕМ

Рассматриваются многочлены фиксированной степени n над произвольным конечным полем $GF(p)$, коэффициенты которых являются независимыми случайными величинами с равномерным распределением на множестве $\{0, 1, \dots, p-1\}$. Вводится понятие структуры $\xi(n) = (\xi_1(n), \dots, \xi_n(n))$ случайного многочлена, где $\xi_i(n)$ означает число сомножителей (с учетом их кратностей) степени i в каноническом разложении многочлена на неприводимые сомножители, и исследуются точные и асимптотические (при $n \rightarrow \infty$) свойства распределений различных характеристик случайной структуры $\xi(n)$.

Ключевые слова и фразы: конечные поля, неприводимые многочлены над ними, случайные многочлены и их структура, производящие функции, моменты и предельные распределения структурных характеристик.

1. Рассматриваются нормированные (т.е. со старшим коэффициентом, равным 1) многочлены фиксированной положительной степени n над произвольным конечным полем $GF(p)$ ($p \geq 2$ есть простое число; все соответствующие алгебраические и теоретико-числовые сведения можно найти, например, в [1]):

$$f(x) = x^n + a_1 x^{n-1} + \dots + a_n, \quad a_i \in GF(p). \quad (1)$$

Известно, что каждый такой многочлен может быть однозначным образом представлен в виде произведения

$$f = f_1^{e_1} \dots f_m^{e_m}, \quad (2)$$

где $f_1, \dots, f_m$ — различные нормированные неприводимые (над полем $GF(p)$) многочлены, а $e_1, \dots, e_m$ — натуральные числа. Пусть k_i обозначает число сомножителей (с учетом их кратностей) степени i в каноническом разложении (2), $i = 1, 2, \dots, n$. Тогда $\sum_i i k_i = n$, и набор $k = (k_1, k_2, \dots, k_n)$ мы будем называть *структурой* многочлена f .

Далее мы будем рассматривать многочлены со случайными коэффициентами, считая, что в (1) $a_1, \dots, a_n$ являются независимыми случайными величинами (с.в.) с равномерным распределением на множестве $\{0, 1, \dots, p-1\}$. В таком случае f становится случайным многочленом, выбираемым с равной вероятностью из множества p^n всех многочленов степени n , а его структура становится случайным вектором, который мы будем обозначать $\xi(n) = (\xi_1(n), \xi_2(n), \dots, \xi_n(n))$.

Нас будут интересовать различные характеристики случайной структуры $\xi(n)$, такие как $\nu(n) = \sum_i \xi_i(n)$ — общее число сомножителей (с учетом их кратностей) в каноническом разложении (2) случайного многочлена, $\mu_{\max}(n)$ (соответственно $\mu_{\min}(n) = \max(\min)\{i: \xi_i(n) \neq 0\}$ — максимальная (минимальная) степень неприводимого сомножителя в разложении (2) случайного многочлена, $\xi_{\max}(n)$ (соответственно $\xi_{\min}(n)$) — число сомножителей максимальной (минимальной) степени в (2), и т.д.

Интерес к исследованию подобных комбинаторных объектов инспирирован (помимо чисто математических стимулов) рядом практических проблем, в частности,

*Московский государственный институт электроники и математики, Б. Трехсвятительский пер., 3/12, 109028 Москва, Россия.

случайные многочлены представляют интерес в связи с некоторыми задачами защиты информации. Первые результаты в этой проблематике получены В. Е. Степановым (теоремы 1, 2–4, 7 для случая $p = 2$). Ряд результатов по анализу с.в. $\mu_{\max}(n)$ установлен в [4].

Отметим также сходство рассматриваемой проблематики с интенсивно обсуждавшимися в литературе задачами исследования структуры случайных подстановок (см. [2], а также книгу [3] и библиографию в ней). Эта аналогия отчетливо проявляется в ряде приводимых ниже результатов, а также и в методах их получения.

2. В дальнейшем $\psi_m = \psi_m(p)$ обозначает число нормированных неприводимых (над полем $\text{GF}(p)$) многочленов степени m . Эти числа играют в рассматриваемой проблематике ключевую роль. Из известных их свойств упомянем следующие [1]:

$$\sum_{d|m} d\psi_d(p) = p^m$$

(сумма берется по всем положительным делителям d числа m) и

$$\psi_m(p) = \frac{1}{m} \sum_{d|m} \mu(d) p^{m/d},$$

где $\mu(d)$ — известная в теории чисел функция Мёбиуса.

Через эти числа распределение структуры $\xi(n)$ выражается следующим образом:

$$P\{\xi(n) = k\} = p^{-n} \prod_{i=1}^n \binom{\psi_i + k_i - 1}{k_i}, \quad \sum_i i k_i = n.$$

Как известно, эффективным средством исследования многих комбинаторных объектов сложной структуры является восходящий к работе В. Л. Гончарова [2] аппарат производящих функций вместе с использованием теории вычетов и методов перевала и разложения дробно-рациональных функций на простейшие дроби. Дополнительным подтверждением этого является и настоящая работа, все основные результаты которой получены именно на этом пути.

Введем основную производящую функцию (пр.ф.)

$$A_n(t_1, \dots, t_n) = E \prod_i t_i^{\xi_i(n)},$$

тогда для нее имеют место представления

$$\begin{aligned} A_n(t_1, \dots, t_n) &= \text{coef}_{z^n} \frac{1}{1-z} \prod_{i=1}^n \left(\frac{1 - (z/p)^i}{1 - t_i(z/p)^i} \right)^{\psi_i} \\ &= \text{coef}_{z^n} \frac{1}{1-z} \exp \left\{ \sum_{m=1}^{\infty} \left(\frac{z}{p} \right)^m \frac{1}{m} \sum_{i|m} i \psi_i (t_i^{m/i} - 1) \right\}. \end{aligned} \quad (3)$$

Придавая переменным $t_1, \dots, t_n$ различные частные значения, из (3) можно получать представления для пр.ф. или функций распределения конкретных структурных характеристик случайного многочлена. Так, при $t_r = t$, $t_i = 1$, $i \neq r$, имеем маргинальную пр.ф.

$$E t^{\xi_r(n)} = \text{coef}_{z^n} \frac{1}{1-z} \left(\frac{1 - (z/p)^r}{1 - t(z/p)^r} \right)^{\psi_r};$$

аналогично, при $t_1 = \dots = t_n = t$ получаем пр.ф. с.в. $\nu(n)$:

$$Et^{\nu(n)} = \text{coef}_z^n \frac{1}{1-z} \exp \left\{ \sum_{m=1}^{\infty} \left(\frac{z}{p} \right)^m \frac{1}{m} \sum_{i|m} i \psi_i (t^{m/i} - 1) \right\};$$

полагая в (3) $t_i = 1$ при $i \leq s$ и $t_i = 0$ при $i > s$, находим

$$P\{\mu_{\max}(n) \leq s\} = P\{\xi_i(n) = 0, i > s\} = \text{coef}_z^n \prod_{i=1}^s \left(1 - \left(\frac{z}{p} \right)^i \right)^{-\psi_i},$$

а если $t_i = 0, i \leq s$, и $t_i = 1, i > s$, то

$$P\{\mu_{\min}(n) > s\} = P\{\xi_i(n) = 0, i \leq s\} = \text{coef}_z^n \frac{1}{1-z} \prod_{i=1}^s \left(1 - \left(\frac{z}{p} \right)^i \right)^{\psi_i}.$$

В качестве примера использования указанных пр.ф. приведем некоторые формулы для моментов:

$$\begin{aligned} E\xi_r(n) &= \text{coef}_z^n \frac{\psi_r}{1-z} \frac{(z/p)^r}{1-(z/p)^r} = \frac{\psi_r}{p^r-1} \left(1 - p^{-r[n/r]} \right), \\ E\xi_r(n)(\xi_r(n)-1) &= \psi_r(\psi_r+1) \text{coef}_z^n \frac{1}{1-z} \frac{(z/p)^{2r}}{(1-(z/p)^r)^2} \\ &= \frac{\psi_r(\psi_r+1)}{(p^r-1)^2} \left(1 - \left[\frac{n}{r} \right] p^{-r[n/r]+r} + \left(\left[\frac{n}{r} \right] - 1 \right) p^{-r[n/r]} \right) \end{aligned}$$

(здесь $[a]$ — целая часть числа a). Отсюда, в частности, следует, что при фиксированном r и $n \rightarrow \infty$

$$E\xi_r(n) = \frac{\psi_r}{p^r-1} + O(p^{-n}), \quad D\xi_r(n) = \frac{\psi_r p^r}{(p^r-1)^2} + O(n p^{-n});$$

кроме того, используя свойства чисел ψ_r , можно заключить, что уже при небольших r справедливы приближения

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

Также можно показать, что

$$\left| \text{cov}(\xi_r(n), \xi_s(n)) \right| < \psi_r \psi_s \frac{n^2}{rs} p^{-n} \xrightarrow{n \rightarrow \infty} 0, \quad r \neq s$$

(асимптотическая некоррелированность), а для числа $\nu(n)$ сомножителей в (2) справедливы асимптотические соотношения

$$E\nu(n) \sim D\nu(n) \sim \ln n, \quad n \rightarrow \infty$$

(как и для числа циклов в случайной подстановке степени n).

3. Основным интерес, как это обычно бывает в подобных задачах, представляет асимптотическое поведение структурных характеристик при $n \rightarrow \infty$. Имеют место следующие асимптотические результаты.

Теорема 1. Если $n \rightarrow \infty$, то для любого фиксированного r с.в. $\xi_i(n)$, $i = 1, 2, \dots, r$, асимптотически независимы и $\xi_i(n)$ имеет в пределе отрицательное биномиальное распределение $\overline{\text{Bi}}(\psi_i, p^{-i})$:

$$P\{\xi_i(n) = k\} \rightarrow \binom{\psi_i + k - 1}{k} p^{-ik} (1 - p^{-i})^{\psi_i}, \quad k = 0, 1, \dots;$$

более того, если $r = r(n) \rightarrow \infty$ так, что $(r \ln r)/n \rightarrow 0$, то с.в. $\xi_1(n), \dots, \xi_r(n)$ продолжают оставаться асимптотически независимыми, а распределение $\xi_i(n)$ при больших i аппроксимируется распределением Пуассона $\Pi(1/i)$.

Следующие утверждения о распределении минимальной степени $\mu_{\min}(n)$ и о числе сомножителей минимальной степени являются прямыми следствиями этой теоремы.

Следствие 1. Для любого натурального r при $n \rightarrow \infty$

$$P\{\mu_{\min}(n) \leq r\} = 1 - \prod_{i=1}^r (1 - p^{-i})^{\psi_i} + o(1),$$

при этом при достаточно больших r

$$P\{\mu_{\min}(n) > r\} \approx \frac{1}{r}.$$

Следствие 2. Для любых натуральных r и k при $n \rightarrow \infty$

$$P\{\mu_{\min}(n) = r, \xi_r(n) = k\} = \binom{\psi_r + k - 1}{k} p^{-rk} \prod_{i=1}^r (1 - p^{-i})^{\psi_i} + o(1),$$

а также $\mathcal{L}(\xi_{\min}(n) \mid \mu_{\min}(n) = r) \rightarrow \mathcal{L}(\xi_r \mid \xi_r > 0)$, где $\mathcal{L}(\xi_r) = \overline{\text{Bi}}(\psi_r, p^{-r})$.

Отсюда, в частности, можно заключить, что в среднем минимальная степень растет неограниченно с ростом n , но число сомножителей в (2) с минимальной степенью в среднем остается конечным.

Что касается общего числа сомножителей $\nu(n)$ в разложении (2) случайного многочлена, то его асимптотическое распределение аналогично распределению числа циклов в случайной подстановке степени n и описывается следующей теоремой.

Теорема 2. При $n \rightarrow \infty$

$$\mathcal{L}(\nu(n)) \sim \mathcal{N}(\ln n, \ln n).$$

Подобная аналогия со случайными подстановками имеет место и для экстремальной характеристики $\mu_{\max}(n)$. Именно, если $\tilde{\mu}_{\max}(n)$ обозначает длину максимального цикла в случайной подстановке степени n , то справедлив следующий результат.

Теорема 3. Распределения нормированных случайных величин $\mu_{\max}(n)/n$ и $\tilde{\mu}_{\max}(n)/n$ сходятся при $n \rightarrow \infty$ к одному и тому же предельному распределению.

Вид этого предельного распределения хорошо известен и потому нами не приводится (его можно найти, например, в [3], где имеется и соответствующая библиография с комментариями), отметим лишь, что $E\mu_{\max}(n)/n \rightarrow 0,6243 \dots$.

Теорема 3 позволяет оценивать вероятности

$$P_n(s) = P\{\mu_{\max}(n) \leq s\}$$

при $s = s(n) \rightarrow \infty$ так, что $s/n \rightarrow x$, $0 < x < 1$. Однако для приложений нужны оценки этих вероятностей и в зоне $s/n \rightarrow 0$ (тогда $P_n(s) \rightarrow 0$). Такие оценки даются следующими утверждениями.

Теорема 4. Пусть при $n \rightarrow \infty$ $s = s(n)$ изменяется так, что $\ln s / \ln n \in [\varepsilon, 1 - \varepsilon]$, где $\varepsilon > 0$ произвольно мало. Тогда

$$P_n(s) = \exp \left\{ -\frac{n}{s} \ln \frac{n}{s} - \frac{n}{s} \ln \ln \frac{n}{s} + \frac{n}{s} + O\left(\frac{n}{s} \frac{\ln \ln(n/s)}{\ln(n/s)}\right) \right\}.$$

Теорема 5. Если $n \rightarrow \infty$, $a_s \geq 1$ фиксированно, то

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

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

Представляют также интерес условные распределения различных структурных характеристик случайного многочлена (1) при условии, что все множители разложения (2) имеют степени, ограниченные сверху некоторым числом s , в различных зонах изменения s . Приведем несколько результатов такого типа.

Теорема 6. Для любого фиксированного $s > 1$ при $n \rightarrow \infty$

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

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

$$\mathcal{L}\left(\frac{s}{n} \xi_{\max}(n) \mid \mu_{\max}(n) \leq s\right) \rightarrow \text{Be}(\psi_s, t_{s-1}),$$

где $\text{Be}(\cdot)$ есть бета-распределение и числа t_i указаны в теореме 5.

Теорема 7. В условиях теоремы 4

$$\mathcal{L}\left(\ln \frac{n}{s} \cdot \left(\frac{n}{s}\right)^{-1/2} \left(\nu(n) - \sum_{i=1}^s \frac{r^i}{i}\right) \mid \mu_{\max}(n) \leq s\right) \rightarrow \mathcal{N}(0, 1),$$

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

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

Из теоремы 7 следует, что при условии $\mu_{\max}(n) \leq s$ с вероятностью, близкой к 1 при больших n , число сомножителей в каноническом разложении (2) будет $(n/s)(1+o(1))$. С другой стороны, при указанном условии число сомножителей $\geq n/s$, причем этот минимум достигается только лишь когда все сомножители разложения имеют степень s . Сравнивая это, получаем, что в условиях теоремы 7 почти все сомножители канонического разложения случайного многочлена должны иметь степень, близкую к максимально возможной степени s .

Отметим также, что в условиях теоремы 7 равномерно по $i \leq s$

$$E\left(\xi_i(n) \mid \mu_{\max}(n) \leq s\right) = \psi_i \left(\frac{r}{p}\right)^i \frac{1+o(1)}{1-(r/p)^i},$$

а если $i = i(n) \rightarrow \infty$, то $E(\xi_i(n) \mid \mu_{\max}(n) \leq s) = (r^i/i)(1+o(1))$. Таким образом, среднее число сомножителей степени i с ростом i сначала уменьшается, достигая

минимума при $i \sim s/\ln(n/s)$, а затем начинает увеличиваться. Среднее же число сомножителей максимально возможной степени в этом случае удовлетворяет асимптотическим соотношениям

$$E(\xi_{\max}(n) \mid \mu_{\max}(n) \leq s) \sim \frac{r^s}{s} \sim \frac{n}{s^2} \ln \frac{n}{s}.$$

Последняя величина конечна, если s имеет порядок $\sqrt{n \ln n}$, неограниченно растет, если $s = o(\sqrt{n \ln n})$, и стремится к нулю, если $s/\sqrt{n \ln n} \rightarrow \infty$.

Наконец, отметим, что средняя кратность, с которой данный неприводимый многочлен степени i входит в каноническое разложение случайного многочлена равна

$$\left(\frac{r}{p}\right)^i \frac{1 + o(1)}{1 - (r/p)^i}$$

при конечных i и $(r/p)^i(1 + o(1))$ при $i \rightarrow \infty$ вместе с n . Последняя величина монотонно убывает к 0 с ростом i , и она асимптотически совпадает с вероятностью того, что данный многочлен степени i будет входить в состав канонического разложения случайного многочлена.

4. После того, как данная статья была подготовлена к печати, нам стала известна недавняя публикация на рассматриваемую тему [5], в которой разработан оригинальный метод, позволяющий получать аппроксимации для совместных распределений структурных характеристик случайных многочленов над конечными полями посредством установления верхних границ d_{TV} для расстояний по вариации до более простых дискретных распределений. Например (в наших обозначениях), для $d_{TV}(\mathcal{L}(\xi_1(n), \dots, \xi_r(n)), \mathcal{L}(\xi_1, \dots, \xi_r))$, где $\xi_1, \dots, \xi_r$ — независимые с.в. и $\mathcal{L}(\xi_i) = \text{Bi}(\psi_i, p^{-i})$, получена равномерная по $r \geq 1$ оценка вида $O(r \exp\{-(n/(2r)) \times \ln(4/3)\})$ (ср. с теоремой 1), а для с.в. $\nu(n)$ аналогичный результат имеет вид

$$d_{TV}(\mathcal{L}(\nu(n)), \Pi(L_n)) = O((\ln n)^{-1/2}),$$

где $L_n = \sum_{j=1}^n j^{-1}$ (ср. с теоремой 2).

Характерной особенностью этой работы является систематически проводимая параллель между проблемами факторизации случайных многочленов (в произведении неприводимых сомножителей) и цикловой структурой случайных подстановок, что существенно отражается и на форме получаемых в ней результатов. Кратко эти результаты можно суммировать следующим образом: структурные свойства многочленов, выражаемых через большие степени (неприводимых сомножителей), асимптотически (при $n \rightarrow \infty$) эквивалентны аналогичным свойствам случайных равновероятных подстановок степени n , выражаемых через их длинные циклы; для малых же степеней и коротких циклов соответствующие свойства асимптотически различаются.

Эти же выводы следуют и из наших результатов, однако мы, в основном, преследовали другую цель, а именно, — возможные приложения случайных многочленов и, как средство для этого, получение результатов в форме, наиболее удобной для использования в конкретных задачах и вычислениях. Следует также подчеркнуть, что круг вопросов, рассмотренных в этих двух работах, имея неизбежные пересечения, существенно разнится. В частности, нами уделено значительное внимание моментам, экстремальным характеристикам и условным распределениям, чего нет в [5].

В свете сказанного, эти две работы, в которых по существу один и тот же объект рассматривается под разными углами зрения, исследуется разными методами, приводящими к разным формам (в ряде случаев одних и тех же) результатов, можно рассматривать, по-нашему мнению, как дополняющие друг друга в различных аспектах.

СПИСОК ЛИТЕРАТУРЫ

1. Лидл Р., Нидеррайтер Г. Конечные поля. Т. 1. М.: Мир, 1988, 430 с.
2. Гончаров В. Л. Из области комбинаторики. — Изв. АН СССР, сер. матем., 1944, т. 8, № 1, с. 3–48.
3. Колчин В. Ф. Случайные отображения. М.: Наука, 1984, 206 с.
4. Odizko A. M. Discrete logarithms in finite fields and there cryptographic significance. — Proceedings of EUROCRYPT 1984. Berlin: Springer-Verlag, 1984, p. 225–314.
5. Arratia R., Barbour A., Tavaré S. On random polynomials over finite fields. — Math. Proc. Cambridge Philos. Soc., 1993, v. 114, p. 347–368.

Поступила в редакцию
7.XII.1995

© 1996 г.

МИЛЬШТЕЙН Г. Н.*

**ПРИМЕНЕНИЕ ЧИСЛЕННОГО ИНТЕГРИРОВАНИЯ
СТОХАСТИЧЕСКИХ УРАВНЕНИЙ
ДЛЯ РЕШЕНИЯ КРАЕВЫХ ЗАДАЧ
С ГРАНИЧНЫМИ УСЛОВИЯМИ НЕЙМАНА**

В статье приводится ряд методов построения марковской цепи с отражением такой, что математическое ожидание определенного функционала от траекторий цепи близко к решению задачи Неймана для уравнений параболического типа. Эта марковская цепь слабо аппроксимирует решение системы стохастических дифференциальных уравнений, являющейся характеристической для задачи Неймана. Для рассмотренных методов получены теоремы сходимости с указанием порядка точности относительно шага аппроксимации.

Ключевые слова и фразы: численное интегрирование стохастических дифференциальных уравнений, слабая аппроксимация решений стохастических дифференциальных уравнений, одношаговый порядок точности метода, порядок сходимости метода, методы Монте-Карло решения задач математической физики.

1. Пусть G — ограниченная область в $\mathbf{R}^n$, $Q = G \times [T_0, T_1]$ — цилиндр в $\mathbf{R}^{n+1}$. Рассмотрим уравнение параболического типа

$$\begin{aligned} \frac{\partial u}{\partial t} + \frac{1}{2} \sum_{i,j=1}^n a^{ij}(t, x) \frac{\partial^2 u}{\partial x^i \partial x^j} + \sum_{i=1}^n b^i(t, x) \frac{\partial u}{\partial x^i} \\ + c(t, x) u + g(t, x) = 0, \quad (t, x) \in Q, \end{aligned} \quad (1.1)$$

с начальным условием

$$u(t_1, x) = \varphi(x) \quad (1.2)$$

и граничным условием Неймана

$$\frac{\partial u}{\partial \nu} + \bar{c}(t, x) u = \bar{g}(t, x), \quad T_0 \leq t \leq T_1, \quad x \in \partial G, \quad (1.3)$$

*Уральский государственный ун-т, пр. Ленина, 51, 620081 Екатеринбург, Россия.