УДК 519.214 DOI 10.17223/2226308X/12/4

О ЧИСЛЕ f-РЕКУРРЕНТНЫХ СЕРИЙ И ЦЕПОЧЕК В КОНЕЧНОЙ ЦЕПИ МАРКОВА

Н. М. Меженная

Будем называть f-рекуррентной цепочкой отрезок дискретной последовательности, знаки которого получаются последовательным применением функции f к l предыдущим знакам, а цепочку, которую нельзя продлить ни в одну сторону с сохранением свойства f-рекуррентности, — f-рекуррентной серией. При помощи метода Чена — Стейна получена оценка расстояния по вариации между распределением числа ξ f-рекуррентных серий длины не меньше s в отрезке длины n конечной эргодической стационарной цепи Маркова и сопровождающим законом распределения Пуассона, т. е. распределением Пуассона с параметром $\lambda_s = \mathsf{E}\xi$, порядка $\mathrm{O}\big(s\lambda_s/n + \mathrm{e}^{us}\sqrt{\lambda_s}\big)$ при некотором $u > 0$. Из этой оценки стандартными методами выведены пуассоновская и нормальная предельные теоремы для случайной величины ξ (при стремлении длины n отрезка цепи Маркова и параметра s к бесконечности). Также полученная оценка позволяет показать, что вероятность наличия f-рекуррентных цепочек длины не меньше s стремится к $1 - \mathrm{e}^{\lambda}$, если $n, s \to \infty$ так, что $s/n \to 0$, $\lambda_s/n \to 0$ и $\lambda_s \to \lambda$. Свойства распределений частот f-рекуррентных серий или цепочек с определёнными свойствами могут быть использованы при разработке статистических критериев для проверки качества псевдослучайных последовательностей.

Ключевые слова: *цепь Маркова, f-рекуррентная серия, f-рекуррентная цепочка, предельная теорема Пуассона, нормальная предельная теорема, метод Чена — Стейна.*

Пусть $\{X_j, j = 1, \ldots, n\}$ — эргодическая стационарная цепь Маркова с множеством состояний $\mathscr{A}_N = \{1, \ldots, N\}$, $N \geqslant 2$, матрицей переходных вероятностей $P = ||p_{a,b}||_{a,b\in\mathscr{A}_N}$ и распределением вероятностей $\{\pi_a, a \in \mathscr{A}_N\}$. Элементы матрицы P^n обозначим $p^{(n)}_{a,b}$, $p^{(1)}_{a,b} = p_{a,b}$.

Известно [1, ч. 2, § 2, с. 100], что существуют константы $C, \gamma > 0$, при которых

$$|p^{(n)}_{a,b} - \pi_b| \leqslant C\pi_b \mathrm{e}^{-\gamma n},\ n \geqslant 1. \tag{1}$$

Пусть $f : \mathscr{A}^l_N \to \mathscr{A}_N$ — числовая функция, $s \geqslant 2$. Приведём определение f-рекуррентной цепочки и серии [2].

Определение 1. Случайные величины $X_{j+1}, \ldots, X_{j+l+s}$ образуют *f-рекуррентную цепочку* длины не меньше s, если

$$X_{j+l+1} = f(X_j, \ldots, X_{j+l-1}),\ \ldots,\ X_{j+l+s} = f(X_{j+s}, \ldots, X_{j+l+s-1}). \tag{2}$$

Определение 2. Случайные величины $X_j, \ldots, X_{j+l+s}$ образуют *f-рекуррентную серию* длины не меньше s, если

$$\begin{gathered} X_{j+l} \neq f(X_j, \ldots, X_{j+l-1}), \\ X_{j+l+1} = f(X_{j+1}, \ldots, X_{j+l}),\ \ldots,\ X_{j+l+s} = f(X_{j+s}, \ldots, X_{j+l+s-1}). \end{gathered} \tag{3}$$

Обозначим A_j и B_j индикаторы событий (2) и (3) соответственно.

Определение f-рекуррентной серии обобщает известное определение серии из одинаковых знаков [3, с. 62]. Действительно, если $l = 1$, функция $f \equiv a$, $a \in \mathscr{A}_N$, то

$$B_j = \{X_{j+1} \neq a, X_{j+2} = a, \ldots, X_{j+s+1} = a\}$$

и f-рекуррентная серия длины не меньше s совпадает с обычной серий знаков a длины не меньше s.

Точные распределения чисел серий в двоичных марковских цепях изучены в [4, 5], а их предельные распределения в цепях Маркова с любым числом состояний получены в [6]. Распределение длины наибольшей серии одинаковых знаков рассмотрено в [7 – 9] для последовательности независимых случайных величин, в [10 – 12] — для цепи Маркова.

Распределение числа f-рекуррентных серий в последовательности независимых случайных величин изучено в [2, 13]. В [14] получены аналогичные результаты для f-рекуррентных серий с возможными пропусками знаков.

Большинство современных криптографических систем предполагает использование псевдослучайных последовательностей, обладающих свойствами, близкими к свойствам случайных равновероятных последовательностей. Для оценки их качества используются различные статистические критерии, в том числе основанные на статистиках от частот значений функций от s-цепочек: тест частот встречаемости s-грамм, покер-тест, тест линейной сложности, тест ранга случайной матрицы, тест интервалов и др. [15]. Для построения таких критериев могут быть использованы и частоты появлений f-рекуррентных цепочек и серий при подходящем выборе функции f.

Будем считать, что задана функция f от $l \geqslant 1$ переменных. Пусть $\Gamma = \{1, \ldots, n-s-l\}$; $\{\alpha_j = I_{A_j} : j \in \Gamma\}$ и $\{\beta_j = I_{B_j} : j \in \Gamma\}$ — наборы случайных индикаторов, соответствующих событиям $\{A_j : j \in \Gamma\}$ и $\{B_j : j \in \Gamma\}$; $Q_s = \mathsf{P}\{B_j\}$ — вероятность любого события из набора $\{B_j : j \in \Gamma\}$.

Определим случайную величину $\xi = \sum\limits_{j=1}^{n-s} \beta_j$, равную числу f-рекуррентных серий в $\{X_j, j = 1, \ldots, n\}$, и её математическое ожидание $\lambda_s = \mathsf{E}\xi = (n-s-l)Q_s$, а также случайную величину $\xi^* = \sum\limits_{j=1}^{n-s} \alpha_j$, равную числу f-рекуррентных цепочек в $\{X_j, j = 1, \ldots, n\}$.

Будем использовать следующие обозначения: $\mathcal{L}(\xi)$ — для закона распределения случайной величины ξ; $\mathrm{Pois}(\lambda)$ — для распределения Пуассона с параметром λ; $\mathcal{N}(0,1)$ — для стандартного нормального распределения; $\rho\left(\mathcal{L}(\xi), \mathcal{L}(\eta)\right)$ — для расстояния по вариации между $\mathcal{L}(\xi)$ и $\mathcal{L}(\eta)$. Для неотрицательных целочисленных случайных величин η_1 и η_2 оно задаётся формулой

$$\rho\left(\mathcal{L}(\eta_1), \mathcal{L}(\eta_2)\right) = \frac{1}{2} \sum_{u=0}^{\infty} \left|\mathsf{P}\{\eta_1 = u\} - \mathsf{P}\{\eta_2 = u\}\right|.$$

Теорема 1. Пусть $s, l, m \geqslant 1$ и $\lambda_s \geqslant 1$. Тогда

$$\rho\left(\mathcal{L}(\xi), \mathrm{Pois}(\lambda_s)\right) \leqslant \left(2(s+l+2m) + 1 + \frac{2C}{\mathrm{e}^{\gamma} - 1}\right) Q_s + \\ + C\mathrm{e}^{-\gamma(m+1)} \sqrt{\lambda_s} \left(2 + C\mathrm{e}^{-\gamma(m+1)} + \mathrm{e}^{-\gamma(s+l+m+1)}\right),$$

где константы C и γ определены в (1).

Следствие 1. Пусть число $l \geqslant 1$ фиксировано, $s, n \to \infty$, так что

$$\frac{s}{n} \to 0, \quad Q_s \to 0, \quad \lambda_s \to \lambda \in (0, \infty).$$

Тогда

1) $\mathcal{L}(\xi) \to \mathrm{Pois}(\lambda)$;
2) $\mathsf{P}\{\xi^* \geqslant 1\} \to 1 - e^{-\lambda}$.

Следствие 2. Пусть число $l \geqslant 1$ фиксировано, $s, n \to \infty$, так что

$$\lambda_s \to \infty, \quad \frac{s}{n}\lambda_s \to 0,$$

и существует константа $u > 0$, для которой $\lambda_s = \mathrm{o}(e^{us})$. Тогда

$$\mathcal{L}\left(\frac{\xi - \lambda_s}{\sqrt{\lambda_s}}\right) \to \mathcal{N}(0,1).$$

Замечание 1. Для доказательства теоремы 1 использованы метод Чена — Стейна (см. теорему 1.A из [16, с. 9]) и схема рассуждений, предложенная в [17, 18].

ЛИТЕРАТУРА

1. *Розанов Ю. А.* Случайные процессы. Краткий курс. М.: Наука, 1979. 184 с.
2. *Михайлов В. Г.* Об асимптотических свойствах числа серий событий // Тр. по дискр. матем. 2006. Т. 9. С. 152–163.
3. *Феллер В.* Введение в теорию вероятностей и ее приложения. В 2-х т. Т. 1. М.: Мир, 1984. 528 с.
4. *Савельев Л. Я., Балакин С. В., Хромов Б. В.* Накрывающие серии в двоичных марковских последовательностях // Дискрет. матем. 2003. Т. 15. № 1. С. 50–76.
5. *Савельев Л. Я., Балакин С. В.* Некоторые применения стохастической теории серий // Сиб. журн. индустр. матем. 2012. Т. 15. № 3. С. 111–123.
6. *Тихомирова М. И.* Предельные распределения числа непоявившихся цепочек одинаковых исходов // Дискрет. матем. 2008. Т. 20. № 3. С. 293–300.
7. *Erdos P. and Revesz P.* On the length of the longest head-run // Topics in Inform. Theory. Colloquia Math. Soc. J. Bolyai 16 Keszthely. 1975. P. 219–228.
8. *Fu J. C.* Distribution theorem of runs and patterns associated with a sequence of multi-state trials // Statist. Sinica. 1996. V. 6. P. 957–974.
9. *Lou W. Y. W.* On runs and longest runs tests: a method of finite Markov chain imbedding // J. Amer. Statist. Assoc. 1996. V. 91. P. 1595–1601.
10. *Vaggelatou E.* On the length of the longest run in a multi-state Markov chain // Statist. Probab. Let. 2003. V. 62. P. 211–221.
11. *Chryssaphinou O., Papastavridis S., and Vaggelatou E.* Poisson approximation for the number of non-overlapping appearances of several words in Markov chain // Combinatorics Probab. 2001. V. 10. P. 293–308.
12. *Zhang Y. Z. and Wu X. Y.* Some results associated with the longest run in a strongly ergodic Markov chain // Acta Mathematica Sinica. 2013. V. 29. No. 10. P. 1939–1948.
13. *Михайлов В. Г.* О предельной теореме Б. А. Севастьянова для сумм зависимых случайных индикаторов // Обозрение прикладной и промышленной математики. 2003. Т. 10. № 3. С. 571–578.
14. *Меженная Н. М.* Предельные теоремы для числа плотных F-рекуррентных серий и цепочек в последовательности независимых случайных величин // Вестник Московского государственного технического университета им. Н. Э. Баумана. Сер. Естественные науки. 2014. № 3. С. 11–25.
15. *Шойтов А. М.* Вероятностные модели псевдослучайных последовательностей в криптографии // Материалы Второй Междунар. науч. конф. по проблемам безопасности и противодействия терроризму. МГУ им. М. В. Ломоносова. М.: МЦНМО, 2006. С. 116–134.

16. *Barbour A. D., Holst L., and Janson S.* Poisson Approximation. Oxford: Oxford Univ. Press, 1992. 277 p.
17. *Михайлов В. Г., Шойтов А. М.* О длинных повторениях цепочек в цепи Маркова // Дискрет. матем. 2014. Т. 26. № 3. С. 79–89.
18. *Minakov A. A.* Poisson approximation for the number of non-decreasing runs in Markov chains // Матем. вопр. криптогр. 2018. Т. 9. № 2. С. 103–116.

УДК 512.772 DOI 10.17223/2226308X/12/5

ХАРАКТЕРИСТИЧЕСКИЕ МНОГОЧЛЕНЫ НЕКОТОРЫХ ГИПЕРЭЛЛИПТИЧЕСКИХ КРИВЫХ РОДОВ 2,3 И p-РАНГА 1[1]

Е. М. Мельничук, С. А. Новоселов

Исследуются характеристические многочлены некоторых классов гиперэллиптических кривых рода $2, 3$ p-ранга 1 над конечным полем. p-Ранг является важным инвариантом кривой, который накладывает ограничения на характеристический многочлен кривой и, следовательно, на число точек в её якобиане. Получены сравнения (по модулю характеристики) и ограничения на коэффициенты для характеристических многочленов кривых p-ранга 1 с автоморфизмами.

Ключевые слова: *гиперэллиптические кривые, p-ранг, характеристические многочлены, группа автоморфизмов.*

Введение

Гиперэллиптическая кривая C рода g над конечным полем $\mathbb{F}_q$ задаётся уравнением

$$y^2 + h(x)y = f(x),$$

где $h(x), f(x) \in \mathbb{F}_q[x]$ и $\deg h(x) \leqslant g+1$, $\deg f(x) = 2g+1$ или $\deg f(x) = 2g+2$ и многочлен $f(x)$ является унитарным.

В настоящее время гиперэллиптические кривые изучаются как альтернатива эллиптическим кривым. Гиперэллиптические кривые требуют меньший размер ключа при сравнимом уровне безопасности. Одними из перспективных направлений в криптографии на (гипер)эллиптических кривых являются классическая криптография на дискретном логарифме, криптография на билинейных спариваниях, постквантовая криптография на изогениях.

Для криптографии на дискретном логарифме необходимы кривые рода 2 и 3 с большим простым числом точек в якобиане. Для кривых больших родов имеются атаки методом исчисления индексов. Для криптографии на билинейных спариваниях, помимо требований для стойкости дискретного логарифма, необходимы кривые с малой степенью вложения. Ярким примером применения криптосистем на билинейных спариваниях является механизм Zk-Snark, применяемый в криптовалюте Zcash. В основе Zk-Snark лежит редуцированное эйт-спаривание. Криптография на изогениях гиперэллиптических кривых в настоящее время только начинает развиваться. Основной проблемой является отсутствие эффективных формул для вычисления изогений.

Множество точек гиперэллиптических кривых рода 2 и 3 не образует группу, в отличие от эллиптических кривых, поэтому для использования таких кривых в криптографии строится ассоциированная с кривой группа — якобиан кривой.

[1]Исследование выполнено при финансовой поддержке РФФИ, проект № 18-31-00244.