Math-Net.Ru

Общероссийский математический портал

И. А. Круглов, Случайные последовательности вида $X_{t+1} = a_t X_t + b_t \pmod{n}$ с зависимыми коэффициентами a_t, b_t , *Дискрет. матем.*, 2005, том 17, выпуск 2, 49–55

DOI: <https://doi.org/10.4213/dm97>

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: 52.87.193.239

26 апреля 2023 г., 18:09:25

Случайные последовательности вида $X_{t+1} = a_t X_t + b_t \pmod{n}$ с зависимыми коэффициентами a_t, b_t

© 2005 г. И. А. Круглов

В статье доказаны неравенства для среднеквадратического отклонения $\delta_{N,n}$ матрицы переходных вероятностей за N шагов от равновероятной матрицы для некоторого случайного аффинного блуждания в кольце вычетов по модулю n с зависимыми линейной компонентой и компонентой сдвига блуждания.

Показано, что соотношение $\lim_{n \rightarrow \infty} \delta_{N,n} = 0$ выполняется тогда и только тогда, когда $N/n^2 \rightarrow \infty$ при $n \rightarrow \infty$, при этом при $n \rightarrow \infty$

$$\delta_{N,n}^2 \sim \varepsilon_n \exp\{-\pi^2 N/l_n^2\},$$

где $\varepsilon_n = 2$, если n четно, $\varepsilon_n = 1$, если n нечетно, $l_n = n/2$, если n четно, $l_n = n$, если n нечетно.

Работа выполнена при поддержке программой Президента Российской Федерации поддержки ведущих научных школ, грант НШ-2358.2003.9.

1. Постановка задачи и основные результаты

Функционирование некоторых датчиков псевдослучайных последовательностей, используемых в вычислительной технике, может быть описано соотношением

$$X_{t+1} = aX_t + b \pmod{n}, \quad t = 0, 1, \dots, \quad (1)$$

где a, b — фиксированные числа, n — натуральное число, $X_0 \in \{0, 1, \dots, n-1\}$ — начальное состояние датчика (см. [6]). Для анализа статистических свойств последовательностей вида (1) можно ввести аналогичную вероятностную модель, заменив a и b случайными последовательностями a_t и b_t , $t = 0, 1, \dots$, соответственно,

$$X_{t+1} = a_t X_t + b_t \pmod{n}, \quad t = 0, 1, \dots \quad (2)$$

Свойства случайных последовательностей вида (2) при условии, что случайные величины X_0, a_t, b_t , $t = 0, 1, \dots$, независимы в совокупности, исследовались ранее в [2–5]. Предметом исследования являлись неравенства для оценки снизу и сверху для величины

$$\sum_{k=0}^{n-1} |\mathbf{P}(X_t = k) - 1/n|.$$

В отличие от указанных выше работ, мы рассматриваем один из случаев последовательности вида (2), в котором для каждого t знаки a_t и b_t зависимы между собой. Кроме того, для некоторого фиксированного N мы рассматриваем последовательность X_{Nt} , $t = 0, 1, 2, \dots$ (регулярную выборку с шагом N из последовательности (2)). Нас будет интересовать, при каких условиях на N и n данная регулярная выборка мало отличается от случайной равновероятной последовательности вычетов по модулю n .

Уточним постановку задачи. Пусть в соотношении (2) случайные пары (a_t, b_t) , $t = 0, 1, \dots$, одинаково распределены, независимы между собой и от X_0 , причем

$$\mathbf{P}(a_1 = 1, b_1 = 1) = \mathbf{P}(a_1 = n - 1, b_1 = k) = \frac{1}{2},$$

где $k \in \{0, 1, \dots, n-1\}$ и возможно зависит от n . Последовательность X_t , $t = 0, 1, \dots$, есть простая однородная цепь Маркова с множеством состояний $\{0, 1, \dots, n-1\}$, обозначим ее матрицу переходных вероятностей через P_n . Для любого целого положительного N , возможно зависящего от n , последовательность X_{Nt} , $t = 0, 1, \dots$, также образует простую однородную цепь Маркова с матрицей переходных вероятностей

$$P_n^N = \|P_n^{(N)}(i, j)\|_{i,j=0}^{n-1}.$$

В качестве меры близости матрицы P_n^N к матрицу переходных вероятностей равновероятной последовательности вычетов по модулю n будем рассматривать величину

$$\delta_{N,n} = \sum_{i,j=0}^{n-1} (P_n^{(N)}(i, j) - 1/n)^2.$$

Сформулируем основные результаты работы.

Теорема 1. Пусть $N \geq 2$, $n \geq 5$ и если n четно, то k нечетно. Тогда справедливы неравенства

$$\begin{aligned} \varepsilon_n \exp \left\{ -\frac{\pi^2(N-1)}{l_n^2} \left(1 + \frac{\pi^2}{l_n^2(2 - \pi^2/l_n^2)} \right) \right\} \\ \leq \delta_{N,n} \leq \varepsilon_n \left(\exp \left\{ -\frac{\pi^2(N-1)}{l_n^2} \left(1 - \frac{\pi^2}{12l_n^2} \right) \right\} + \exp \left\{ -\frac{4\pi^2(N-1)}{l_n^2} \left(1 - \frac{\pi^2}{192} \right) \right\} \right. \\ \left. \times \left(1 + \frac{l_n^2}{4(N-1)\pi^2(1 - \pi^2/192)} \right) + (l_n + 1) \left(\frac{1}{2} \right)^{N+1} \right), \end{aligned}$$

где

$$l_n = \begin{cases} n/2, & \text{если } n \text{ четно,} \\ n, & \text{если } n \text{ нечетно,} \end{cases} \quad \varepsilon_n = \begin{cases} 2, & \text{если } n \text{ четно,} \\ 1, & \text{если } n \text{ нечетно.} \end{cases}$$

Следствие 1. Пусть выполнены условия теоремы 1 и $N = N(n)$. Соотношение

$$\lim_{n \rightarrow \infty} \delta_{N,n} = 0$$

справедливо тогда и только тогда, когда при $n \rightarrow \infty$ выполняется условие

$$\frac{N(n)}{n^2} \rightarrow \infty.$$

При выполнении этого условия при $n \rightarrow \infty$

$$\delta_{N,n} \sim \varepsilon_n \exp\{-N\pi^2/l_n^2\}.$$

Результат следствия 1 позволяет говорить о наличии своего рода порогового эффекта в поведении величины $\delta_{N,n}$ (см. также [2, 4, 5]).

2. Доказательство теоремы 1

Фиксируем параметры N, n, k , удовлетворяющие условиям теоремы 1. Введем подстановки степени n

$$\bar{A} = \begin{pmatrix} & i \\ i+1 & \end{pmatrix} \pmod{n}, \quad \bar{B}_k = \begin{pmatrix} & i \\ k-i & \end{pmatrix} \pmod{n},$$

и пусть A, B_k — соответствующие подстановочные $n \times n$ матрицы. Тогда

$$P_n = \frac{1}{2}(A + B_k).$$

Нетрудно видеть, что подстановки $\bar{A}$ и $\bar{B}_k$ порождают группу диэдра D_n степени n , рассматриваемую как группа подстановок. Пусть $(G, *)$ — изоморфная ей абстрактная группа, $q: G \rightarrow D_n$ — изоморфизм и

$$a = q^{-1}(\bar{A}), \quad b_k = q^{-1}(\bar{B}_k), \quad a, b_k \in G.$$

Пусть ξ — случайная величина с значениями в группе G , для которой

$$\mathbf{P}(\xi = a) = \mathbf{P}(\xi = b_k) = \frac{1}{2}.$$

Тогда матрица P_n совпадает с матрицей переходных вероятностей $\Pi_\xi^{(q)}$ случайной величины ξ в схеме (G, q, ξ) , описанной в статье [1]. Из результатов первого параграфа этой статьи следует, что существует унитарная матрица J над полем комплексных чисел, для которой выполнено соотношение

$$J^{-1} \Pi_\xi^{(q)} J = \text{Diag}(\dots, (k_V, \Phi_\xi^{(q)}(V)), \dots). \quad (3)$$

В правой части равенства (3) стоит блочно-диагональная матрица, у которой на диагонали k_V раз встречается блок

$$\Phi_\xi^{(q)}(V) = \frac{1}{2} (V(a) + V(b_k)),$$

V — неприводимое унитарное матричное представление группы G , k_V — кратность представления V в матричном представлении Q группы G подстановочными матрицами, соответствующем представлению q .

Из соотношения (3) следует, что

$$J^{-1} P_n^N J = \text{Diag}(\dots, (k_V, \Phi_\xi^{(q)}(V)^N), \dots). \quad (4)$$

Для комплексной матрицы S положим $S^* = \bar{S}'$, где штрих — знак транспонирования, а $\bar{S}'$ — матрица с элементами, сопряженными к элементам матрицы S' . Нетрудно видеть, что

$$\delta_{N,n} + 1 = \sum_{i,j=0}^{n-1} (P_n^{(N)}(i, j))^2 = \text{Tr}(P^N (P^*)^N), \quad (5)$$

где $\text{Tr}(S)$ — след матрицы S . Так как $J^* = J^{-1}$, из соотношений (4) и (5) следует, что

$$\delta_{N,n} = \sum_V k_V \text{Tr}(\Phi_\xi^{(q)}(V)^N (\Phi_\xi^{(q)}(V)^*)^N) - 1. \quad (6)$$

В правой части соотношения (6) сумма берется по всем неэквивалентным неприводимым представлениям группы G .

Пусть $n = 2r + 1$, где r — целое число, $r \geq 2$. Представление Q раскладывается с нулевой кратностью в сумму неприводимых представлений (см. [8]), именно, единичного представления

$$V_0(a) = V_0(b_k) = 1, \quad k_{V_0} = 1, \quad \Phi_\xi^{(q)}(V_0) = 1,$$

и двумерных представлений

$$U_m(a) = \begin{pmatrix} e^{2\pi m i/n} & 0 \\ 0 & e^{-2\pi m i/n} \end{pmatrix},$$

$$U_m(b_0) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad k_{U_m} = 1, \quad m = 1, 2, \dots, r.$$

Очевидно, что $b_k = b_0 * a^k$. Таким образом,

$$\Phi_\xi^{(q)}(U_m) = \frac{1}{2} \begin{pmatrix} e^{2\pi m i/n} & e^{-2\pi m k i/n} \\ e^{2\pi m k i/n} & e^{-2\pi m i/n} \end{pmatrix}, \quad m = 1, \dots, r.$$

Фиксируем произвольное $m \in \{1, \dots, r\}$. Пусть

$$S = \begin{pmatrix} e^{-2\pi m k i/n} & e^{2\pi m i/n} \\ -e^{2\pi m i/n} & e^{-2\pi m k i/n} \end{pmatrix}, \quad m = 1, \dots, r.$$

Как легко видеть, S обратима и

$$\Phi_\xi^{(q)}(U_m) = S \begin{pmatrix} 0 & 0 \\ 0 & \cos(2\pi m/n) \end{pmatrix} S^{-1},$$

$$(\Phi_\xi^{(q)}(U_m))^N (\Phi_\xi^{(q)}(U_m)^*)^N = \frac{2}{|\det S|^2} \cos^{2N} \left(\frac{2\pi m}{n} \right) \begin{pmatrix} 1 & e^{2\pi m(k-1)i/n} \\ e^{2\pi m(k-1)i/n} & 1 \end{pmatrix},$$

$$|\det S|^2 = 4 \cos^2(2\pi m/n). \quad (7)$$

Из соотношений (6) и (7) следует, что

$$\delta_{N,n} = \sum_{m=1}^r \cos^{2(N-1)} \left(\frac{2\pi m}{n} \right). \quad (8)$$

Функция $y = \cos^2 x$ четна и имеет период π , поэтому

$$\cos^2(2\pi m/n) = \cos^2(2\pi(n-m)/n), \quad m \in \{1, \dots, r\}.$$

Из соотношения (8) следует, что

$$2\delta_{N,n} = \sum_{m=1}^{2r} \cos^{2(N-1)}\left(\frac{2\pi m}{n}\right).$$

Так как n нечетно, множество наименьших неотрицательных вычетов чисел $2m$, $m = 1, \dots, n-1$, по модулю n совпадает с множеством всех ненулевых вычетов по модулю n . Таким образом,

$$2\delta_{N,n} = \sum_{m=1}^{2r} \cos^{2(N-1)}\left(\frac{\pi m}{n}\right) = 2 \sum_{m=1}^r \cos^{2(N-1)}\left(\frac{\pi m}{n}\right),$$

и окончательно

$$\delta_{N,n} = \sum_{m=1}^r \cos^{2(N-1)}\left(\frac{\pi m}{n}\right) = \varepsilon_n \sum_{m=1}^r \cos^{2(N-1)}\left(\frac{\pi m}{l_n}\right), \quad (9)$$

Легко проверить, что при $0 \leq x \leq \pi/4$

$$\cos x \leq 1 - \frac{x^2}{2} = \frac{x^4}{24} \leq 1 - \frac{x^2}{2} \left(1 - \frac{\pi^2}{192}\right).$$

Так как $1 - a \leq e^{-a}$ для всех $a > 0$, справедливы неравенства

$$\begin{aligned} \cos(\pi/n) &\leq \exp\left\{-\frac{\pi^2}{2n^2}\left(1 - \frac{\pi^2}{12n^2}\right)\right\}, \\ \cos(\pi m/n) &\leq \exp\left\{-\frac{\pi^2 m^2}{2n^2}\left(1 - \frac{\pi^2}{192}\right)\right\}, \quad m = 2, \dots, [n/4]. \end{aligned} \quad (10)$$

Кроме того,

$$\cos x \leq \frac{\sqrt{2}}{2}, \quad \frac{\pi}{4} < x \leq \frac{\pi}{2}. \quad (11)$$

Из соотношений (9), (10), (11) получаем неравенства

$$\begin{aligned} \delta_{N,n} &\leq \exp\left\{-\frac{\pi^2(N-1)}{n^2}\left(1 - \frac{\pi^2}{12n^2}\right)\right\} + \exp\left\{-\frac{4\pi^2(N-1)}{n^2}\left(1 - \frac{\pi^2}{192}\right)\right\} \\ &\quad + \sum_{m=3}^{[n/4]} \exp\left\{-\frac{\pi^2(N-1)m^2}{n^2}\left(1 - \frac{\pi^2}{192}\right)\right\} + \sum_{m=[n/4]+1}^r \cos^{2(N-1)}\left(\frac{\pi m}{n}\right) \\ &\leq \exp\left\{-\frac{\pi^2(N-1)}{n^2}\left(1 - \frac{\pi^2}{12n^2}\right)\right\} + \exp\left\{-\frac{4\pi^2(N-1)}{n^2}\left(1 - \frac{\pi^2}{192}\right)\right\} \\ &\quad + \int_2^\infty e^{-Zt^2} dt + (n+1) \left(\frac{1}{2}\right)^{N+1}, \end{aligned} \quad (12)$$

где

$$Z = \frac{\pi^2(N-1)}{n^2} \left(1 - \frac{\pi^2}{192}\right).$$

В силу леммы 2 на стр. 192 в [7]

$$\int_2^\infty e^{-Zt^2} dt \leq \frac{1}{4Z} e^{-4Z}. \quad (13)$$

Из соотношений (12) и (13) следует верхняя оценка $\delta_{N,n}$, указанная в теореме 1.

Оценим $\delta_{N,n}$ снизу. Очевидно, что

$$\delta_{N,n} \geq (\cos^2(\pi/n))^{N-1}. \quad (14)$$

При $|x| < \sqrt{2}$

$$\begin{aligned} \ln(\cos x) &\geq \ln(1 - x^2/2) = - \sum_{k=1}^{\infty} \frac{1}{k} \left(\frac{x^2}{2}\right)^k \\ &\geq - \left(\frac{x^2}{2} + \frac{x^4}{4} \left(1 + \frac{x^2}{2} + \dots + \left(\frac{x^2}{2}\right)^k + \dots\right) \right) = - \frac{x^2}{2} \left(1 + \frac{x^2}{2-x^2}\right). \end{aligned}$$

При $x = \pi/n$, $n \geq 5$, получаем, что

$$\ln(\cos x) \geq - \frac{\pi^2}{2n^2} \left(1 + \frac{\pi^2}{2n^2 - \pi^2}\right). \quad (15)$$

Из соотношений (14) и (15) получаем нижнюю оценку $\delta_{N,n}$, указанную в теореме.

Пусть теперь $n = 2r$, где r — целое число, $r \geq 3$. Представление Q раскладывается с нулевой кратностью в сумму неприводимых представлений группы G , а именно, представления

$$V_0: k_{V_0} = 1, \quad \Phi_{\xi}^{(q)}(V_0) = 1,$$

представления

$$V_1(a) = -1, \quad V_1(b_0) = 1, \quad k_{V_1} = 1, \quad \Phi_{\xi}^{(q)}(V_1) = \frac{1}{2}(1 + (-1)^k) = 0$$

(так как по условию k нечетно), и представлений

$$U_m, \quad k_{U_m} = 1, \quad \Phi_{\xi}^{(q)}(U_m) = \frac{1}{2} \begin{pmatrix} e^{2\pi mi/n} & e^{-2\pi mki/n} \\ e^{2\pi mki/n} & e^{-2\pi mi/n} \end{pmatrix}, \quad m = 1, \dots, r-q.$$

Проводя вычисления $\text{Tr}((\Phi_{\xi}^{(q)}(U_m))^N (\Phi_{\xi}^{(q)}(U_m)^*)^N)$ аналогично случаю нечетного n , получаем, что

$$\delta_{N,n} = \sum_{m=1}^{r-1} \cos^{2(N-1)}(2\pi m/n).$$

Поскольку n четно, множество $\{2m, m = 1, \dots, r-1\}$ есть множество четных ненулевых вычетов по модулю n . Учитывая периодичность функции $y = \cos^2 x$, получаем, что

$$\delta_{N,n} = 2 \sum_{m=1}^{[(r-1)/2]} \cos^{2(N-1)}(2\pi m/n) = \varepsilon_n \sum_{m=1}^{[(r-1)/2]} \cos^{2(N-1)}(\pi m/l_n). \quad (16)$$

Дальнейшие оценки суммы в правой части соотношения (16) проводятся совершенно аналогично оценке правой части соотношения (9).

Теорема доказана.

Список литературы

1. Горчинский Ю. Н., Круглов И. А., Капитонов В. М., Вопросы теории распределений на конечных группах. *Труды по дискретной математике* (1997) **1**, 85–112.
2. Chung F., Diaconis P., Graham R. L., A random walk problem arising in random number generation. *Ann. Probab.* (1987) **15**, 1148–1165.
3. Chassing P., An optimal random number generator on Z_p . *Statist. Probab. Lett.* (1989) **7**, 307–309.
4. Hildebrand M., Random processes of the form $X_{n+1} = a_n X_n = b_n \pmod{p}$. *Ann. Probab.* (1993) **21**, 710–720.
5. Hildebrand M., Random processes of the form $X_{n+1} = a_n X_n = b_n \pmod{p}$, where b_n takes on a single value. In: *Random Discrete Structures. IMA Vol. Math. Appl.* (1996) **76**, 153–174.
6. Кнут Д., *Искусство программирования для ЭВМ*, т. 2: *Получисленные алгоритмы*. Мир, Москва, 1984.
7. Феллер В., *Введение в теорию вероятностей и ее приложения*, т. 1. Мир, Москва, 1984.
8. Серр Ж.-П., *Линейные представления групп*. Мир, Москва, 1970.

Статья поступила 15.12.2004.