ISSN 2079-3316 ПРОГРАММНЫЕ СИСТЕМЫ: ТЕОРИЯ И ПРИЛОЖЕНИЯ т. 9, № 3(38), с. 3–9

ББК 32.811.3
УДК 519.65

С. В. Парамонов

Идентификация псевдослучайных последовательностей по моментам вероятностных распределений

Аннотация. В работе рассматривается обоснование метода определения детерминированного характера псевдослучайного процесса, формируемого нелинейным отображением $[0,1] \to [0,1]$, путем сопоставления двумерных смешанных моментов распределений значений, генерируемых этим отображением. Рассматривается возможность аппроксимации отображения, генерирующего псевдослучайную последовательность, по совокупности двумерных смешанных моментов распределения.

Ключевые слова и фразы: одномерное отображение, моменты распределения, аппроксимация.

Введение

При изучении динамических систем последнее время особый интерес вызывают системы (как правило, нелинейные), при определенных параметрах генерирующие сложные незатухающие апериодические траектории, по многим характеристикам сходными со случайными недетерминированными «шумовыми» процессами. Подобные системы и формируемые ими процессы, как известно, называют *хаотическими*. В прикладном аспекте методы определения детерминированного характера наблюдаемого процесса, имеющего признаки чисто случайного, имеют применение, в частности, в области идентификации систем, построения нелинейных регрессионных моделей, машинного обучения и пр [1].

Работа выполнена в рамках НИР «Исследование и разработка методов машинного обучения для обнаружения аномалий», номер гос. регистрации 0077-2016-0002.

10.25209/2079-3316-2018-9-3-3-9

В данной статье рассматривается возможность идентификации детерминированных систем с дискретным временем, задаваемых рекуррентным уравнением вида

$$x_{n+1} = f(x_n), \tag{1}$$

известным также как отображение отрезка в себя. Известно, что существует класс отображений вида (1), которые при определенных параметрах являются хаотическими [2].

Пусть рассматриваемая система формирует хаотическую траекторию $\{\dots, x_{n-1}, x_n, x_{n+1}, \dots\}$, где $x_n = f^{(n)}(x_0) = \underbrace{f(f\dots(f(x_0)))}_{n}$, а x_0 — начальная точка траектории. При этом значения последовательности $\{\dots, x_{n-1}, x_n, x_{n+1}, \dots\}$ будут формировать асимптотическое распределение с плотностью, описываемой гладкой функцией

$$W^*(x) = \lim_{\Delta x \to\ 0} \lim_{N \to \infty} \frac{1}{\Delta x} \frac{1}{N} \sum_{n=0}^{N-1} \chi_{\Delta x}(f^{(n)}(x_0))$$

(здесь Δx — интервал разбиения области значений $\{x_n\}$ — отрезка $[0, 1]$, а χ — индикаторная функция на Δx).

Если преобразование (1) хаотическое, то для него выполняется условие эргодичности, то есть $W^*(x)$ должна быть инвариантна относительно преобразования f [3]

$$W^*(x) = \frac{d}{dx} \int_{f_{-1}([0,1])} W^*(x')\, dx' \equiv W_1(x).$$

Здесь $W_1(x)$ — обозначение для одномерной плотности распределения вероятностей (ПРВ) значений $\{x_n\}$.

При этом двумерная совместная плотность распределения вероятностей определяется как

$$W_2(x, y) = W_1(x)\delta(y - f(x)). \tag{2}$$

Для данного преобразования и связанной с ним функции ПРВ существуют одномерные моменты

$$m_p = \int\limits_0^1 x^p W_1(x)\, dx \tag{3}$$

и двумерные смешанные моменты

$$m_{k,l} = \int_0^1 \int_0^1 x^k y^l W_2(x,y)\,dxdy = \int_0^1 x^k (f(x))^l W_1(x)\,dx. \tag{4}$$

Выполнение условия эргодичности для хаотического процесса позволяет рассматривать при численном анализе одномерных и многомерных моментов их оценки, полученные в результате усреднения значений x_n, взятых из одной траектории $\{\ldots, x_{n-1}, x_n, x_{n+1}, \ldots\}$.

1. Сравнение двумерных смешанных моментов для одномерного хаотического отображения

Рассмотрим класс G одномерных хаотических отображений вида (1), задаваемых аналитическими функциями, представимыми в виде разложения

$$f(x) = \sum_{m=0}^{\infty} a_m x^m. \tag{5}$$

Для данного класса отображений справедливо следующее утверждение:

Утверждение 1. *Если одномерное отображение, заданное аналитической функцией f, является хаотическим, то для совокупности двумерных смешанных моментов вида (4) распределения значений последовательности, сформированной данным отображением, найдется хотя бы одно значение k такое, что*

$$m_{k,k+1} \neq m_{k+1,k}. \tag{6}$$

Условие аналитичности в данном случае вызвано необходимостью исключить из рассмотрения кусочно-гладкие и кусочно-непрерывные отображения, имеющие особые точки на интервале [0,1], рассмотрение которых является особым случаем.

Доказательство. Представим $m_{k,k+1}$ в виде

$$\begin{aligned} m_{k,k+1} &= \int_0^1 (xf(x))^k (\sum_{m=0}^{\infty} a_m\, x^m)\, W_1(x)\,dx = \\ &= \sum_{m=0}^{\infty} a_m \int_0^1 x^{k+m} f(x)^k W_1(x)\,dx = \sum_{m=0}^{\infty} a_m m_{k+m,k}. \end{aligned} \tag{7}$$

Рассмотрим для начала случай, когда ряд (5) ограничен и состоит из $M+1$ начальных членов (то есть $f(x)$ — полином конечной степени). Для $(M+1)$ коэффициентов ряда можно составить систему из $(M+1)$ уравнений вида $\mathbf{DA} = \mathbf{B}$

$$(8)\quad \begin{pmatrix} m_{0,0} & m_{1,0}\dots & m_{M,0} \\ m_{1,1} & m_{2,1}\dots & m_{M+1,1} \\ \dots & \dots & \dots \\ m_{M,M} & m_{M+1,M}\dots & m_{2M,M} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \dots \\ a_M \end{pmatrix} = \begin{pmatrix} m_{0,1} \\ m_{1,2} \\ \dots \\ m_{M,M+1} \end{pmatrix}.$$

Определитель для матрицы $\mathbf{D}$ не равен 0, так как решение системы (8) является единственным ввиду единственности разложения (5). Предположим, что $m_{k,k+1} = m_{k+1,k}$ для любого значения k. С учетом этого равенства, перепишем (8) в виде

$$(9)\quad \begin{pmatrix} m_{0,0} & m_{1,0}\dots & m_{M,0} \\ m_{1,1} & m_{2,1}\dots & m_{M+1,1} \\ \dots & \dots & \dots \\ m_{M,M} & m_{M+1,M}\dots & m_{2M,M} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \dots \\ a_M \end{pmatrix} = \begin{pmatrix} m_{1,0} \\ m_{2,1} \\ \dots \\ m_{M+1,M} \end{pmatrix}.$$

В этом случае единственным решением будет $a_0 = 0$, $a_1 = 1$, $a_2 = .. = a_M = 0$, то есть f — тождественное преобразование, и оно не входит в G. Любые другие решения допустимы лишь при $m_{k,k+1} \neq m_{k+1,k}$, следовательно, утверждение 1 верно. □

Очевидно, что оно выполняется для любого количества членов ряда в разложении (5).

Данное утверждение даёт возможность продемонстрировать отличие хаотической последовательности, формируемой одномерным отображением класса G, от чисто случайной последовательности, значения которого между собой независимы (случайного процесса типа «белый шум»). Действительно, рассмотрим наряду с хаотической последовательностью, удовлетворяющей условиям утверждения 1, такую чисто случайную последовательность $\{..\xi_{s-1}, \xi_s, \xi_{s+1}, ..\}$, одномерная ПРВ значений которой тождественна ПРВ значений хаотической последовательности. Из взаимной независимости значений $\{\xi_n\}$ следует, в частности, что для двумерных смешанных моментов их распределения $m_{\xi k,k+1}$ справедливо равенство

$$m_{\xi k,k+1} = m_{\xi k+1} m_{\xi k} = m_{\xi k+1,k},$$

которое, в силу утверждения 1, не выполняется для хаотической последовательности, формируемой одномерным отображением в виде аналитической функции.

2. Аппроксимация функции одномерного отображения

Пусть в нашем распоряжении есть последовательность значений $\{..x_{n-1}, x_n, x_{n+1}, ..\}$, произведенная некоторым одномерным отображением. На базе данной последовательности можно получить оценки моментов 1-го и 2-го порядка $\hat{m}_p$ $\hat{m}_{k,l}$ и получить аппроксимацию функции $\hat{f}$ в виде суммы $\hat{f}(x) = \sum\limits_{m=0}^{M} \hat{a}_m \cdot x^m$ на $[0,1]$, где $\hat{a}_m$ являются решениями системы (8).

Аппроксимированная функция $\hat{f}$ будет представлена как полином конечной степени M.

В прикладных задачах для восстановление функции отображения потребуется применение вычислительных процедур, реализуемых на ЭВМ. В связи с этим, возникает известная проблема точности аппроксимации на ЭВМ, связанная с ограничением разрядной сетки [4]. Это приводит к тому, что в случае сходимости ряда (5) при аппроксимации можно ограничить предельную величину m некоторым конечным значением M_z, превышать которое не имеет смысла.

3. Выводы

Выше было показано, что сравнение двумерных случайных моментов для последовательности с дискретным временем дает основание предполагать наличие функциональной связи между соседними отсчетами, исходя из предположения, что данная функциональная зависимость — одношаговая (x_{n+1} зависит от x_n). Между тем, существуют также отображения вида $x_n = f(x_{n-1}, x_{n-2}....)$, включающие в себя зависимость от большего числа шагов, также способные формировать траектории типа «хаотический аттрактор» [5]. Открытым остается вопрос о том, как соотносятся смешанные моменты для таких отображений.

Отдельной задачей является обоснование эргодического характера исследуемого процесса. Эргодичность отображения приводит к наличию инвариантного вероятностного распределения, плотность которого равна ПРВ для отдельной траектории $\{..x_{n-1}, x_n, x_{n+1}, ..\}$, что позволяет при анализе процесса использовать средние по времени (по траектории) оценки моментов распределения. При практическом применении эргодичность процесса можно оценить по скорости затухания его корреляционной функции [6].

Одновременно с этим, детерминированный характер процесса не означает автоматически, что формирующее его отображение является хаотическим. Наличие хаотического аттрактора связано с неустойчивостью траекторий динамического процесса и может быть обосновано, например, расчетом показателей Ляпунова [7].

Список литературы

[1] Ф. Мун. *Хаотические колебания*, Мир, М., 1990, 312 с. ↑3

[2] Charalampos (Haris) Skokos, Georg A. Gottwald, Jacques Laskar (eds.). *Chaos Detection and Predictability*, Springer-Verlag, Berlin–Heidelberg, 2016, 269 p. ↑4

[3] S. Grossmann, S. Thomae. "Invariant Distributions and Stationary Correlation Functions of One-Dimensional Discrete Processes", *Zeitschrift Naturforschung Teil A*, **32** (Dec. 1977), pp. 1353–1363. ↑4

[4] Дж. Форсайт, М. Малькольм, К. Моулер. *Машинные методы математических вычислений*, Мир, М., 1980, 280 с. ↑7

[5] А. Б.. Каток, Б. Хасселблат. *Введение в теорию динамических систем с обзором последних достижений*, Пер. с англ., Факториал, М., 1999, 767 с. ↑7

[6] A. Lasota, M. C. Mackey. *Probabilistic properties of deterministic systems*, Cambridge Univ. Press, New York, 1986, 358 p. ↑7

[7] G. Boeing. "Visual Analysis of Nonlinear Dynamical Systems: Chaos, Fractals, Self-Similarity and the Limits of Prediction", *Systems*, **4**:4 (2016), pp. 37–55 `http://www.mdpi.com/2079-8954/4/4/37`. ↑8

Рекомендовал к публикации *д.т.н. Е. П. Куршев*

Пример ссылки на эту публикацию:

С. В. Парамонов. «Идентификация псевдослучайных последовательностей по моментам вероятностных распределений». *Программные системы: теория и приложения*, 2018, **9**:3(38), с. 3–9.

10.25209/2079-3316-2018-9-3-3-9

`http://psta.psiras.ru//read/psta2018_3_3-9.pdf`

Об авторе:

Семён Владимирович Парамонов

Научные интересы: алгоритмы и методы обработки изображений и сигналов со сложной природой происхождения

0000-0001-8219-9401

e-mail: psvpox@gmail.com

UDC 519.65

Semion Paramonov. *Pseudo-random sequences identification by probability distribution moments.*

ABSTRACT. The paper discusses the method for determining the deterministic nature of a pseudo-random process, formed by a nonlinear mapping $[0,1]$ to $[0,1]$. The method is based on comparing two-dimensional mixed moments of distributions of values generated by this mapping. The possibility of approximation for the mapping that generates pseudo-random process based on aggregation of two-dimensional mixed distribution moment is considered. (*In Russian*).

Key words and phrases: one-dimensional mapping, moments of distribution, approximations.

2010 *Mathematics Subject Classification*: 97P20; 97N40, 97N50

References

[1] F. C. Moon. *Chaotic Vibration*, Wiley, New York, 1987.↑3

[2] Charalampos (Haris) Skokos, Georg A. Gottwald, Jacques Laskar (eds.). *Chaos Detection and Predictability*, Springer-Verlag, Berlin–Heidelberg, 2016, 269 p. ↑4

[3] S. Grossmann, S. Thomae. "Invariant Distributions and Stationary Correlation Functions of One-Dimensional Discrete Processes", *Zeitschrift Naturforschung Teil A*, **32** (Dec. 1977), pp. 1353–1363. ↑4

[4] G. E. Forsythe, M. A. Malcolm, C. B. Moler, *Computer Methods for Mathematical Computations*, Prentice-Hall Series in Automatic Computation, Prentice Hall, Englewood Cliffs, N.J., 1977, 270 p.↑7

[5] A. B.. Katok, B. Hasselblatt, *Introduction to the Modern Theory of Dynamical Systems*, Encyclopedia of Mathematics and its Applications, vol. **54**, Cambridge Univ. Press, 1995, xviii+802 p.↑7

[6] A. Lasota, M. C. Mackey. *Probabilistic properties of deterministic systems*, Cambridge Univ. Press, New York, 1986, 358 p. ↑7

[7] G. Boeing. "Visual Analysis of Nonlinear Dynamical Systems: Chaos, Fractals, Self-Similarity and the Limits of Prediction", *Systems*, **4**:4 (2016), pp. 37–55 http://www.mdpi.com/2079-8954/4/4/37.↑8

Sample citation of this publication:

Semion Paramonov. "Pseudo-random sequences identification by probability distribution moments". *Program Systems: Theory and Applications*, 2018, **9**:3(38), pp. 3–9. (*In Russian*). 10.25209/2079-3316-2018-9-3-3-9

URL http://psta.psiras.ru//read/psta2018_3_3-9.pdf

10.25209/2079-3316-2018-9-3-3-9