Детерминированный хаос

Изв. вузов «ПНД», т.12, № 3, 2004 УДК 531.19

МОДИФИКАЦИИ ОТОБРАЖЕНИЯ ПЕКАРЯ: ОСОБЕННОСТИ АСИМПТОТИЧЕСКОГО ПОВЕДЕНИЯ

А.Ф. Голубенцев, *В.М. Аникин, С.А. Ноянова*

Двумерное недиссипативное отображение пекаря может быть обобщено посредством задания закона изменения «растягивающей» координаты x в форме G-ичного сдвига Бернулли (G - произвольное целое число) или «зеркального» сдвига Бернулли, ветви которого имеют отрицательный угловой коэффициент. Как в случае классического отображения пекаря, так и для его модификаций закон изменения «сжимающей» y-компоненты отображения пекаря может быть представлен в форме линейной авторегрессионной модели первого порядка. Роль «возмущения» играет дискретная случайная величина, с равной вероятностью принимающая значения 0,1,..., G-1 и порождаемая разложением в G-ичную дробь произвольно выбираемого стартового значения x_0 «растягивающей» координаты x. В асимптотике изменение «сжимающей» координаты y теряет зависимость от начального значения условия y_0. Линейный фильтр, описывающий преобразование пекаря, является каузальным, устойчивым и обратимым. Учет асимптотических особенностей отображения пекаря особенно важен в схемах хаотической криптографии, использующих это отображение.

Введение

Среди двумерных отображений, сохраняющих площадь, особая роль принадлежит так называемому «отображению пекаря» (baker transformation). Введенное впервые в 1934 году Е. Хопфом [1], это отображение стало классическим образцом эргодического (обладающего инвариантной плотностью) и перемешивающего (имеющего инвариантную плотность пределом нестационарных распределений - решений оператора Перрона - Фробениуса) отображения [2-12][1].

Интересны приложения отображения пекаря к конкретным задачам моделирования, возникающим в естественных науках. С помощью цепочки связанных отображений пекаря моделировались такие физико-химические процессы, как изомеризация (три связанных отображения пекаря), диффузия и хаотическое рассеяние (бесконечная цепочка отображений пекаря) [13]. Наиболее «прозрачное» и эффективное применение отображение пекаря нашло в последнее

[1] Своим названием рассматриваемое отображение тоже обязано Е. Хопфу, который в работе [1] для придания образности отображению отметил, что «повторное проведение <его> напоминает приготовление слоеного теста».

время при решении криптографических задач[2]. Связано это с тем, что благодаря свойству перемешиваемости отображение пекаря в процессе итераций быстро нивелирует особенности полезного дискретного и квантованного сигнала, который выступает в качестве начального значения для «сжимающей» координаты этого преобразования. Двумерное распределение при этом в силу ярко выраженных хаотических свойств «растягивающей» компоненты отображения «релаксирует» к равномерному. Поэтому аналитическое исследование процесса релаксации имеет для данного круга задач, пожалуй, первостепенное значение.

Классическое отображение пекаря, в основе которого лежит двоичный сдвиг Бернулли, может быть обобщено посредством задания закона изменения «растягивающей» координаты x в форме G-ичного сдвига Бернулли (G - произвольное целое число) или «зеркального» сдвига Бернулли, ветви которого имеют отрицательный угловой коэффициент. Целью настоящего рассмотрения является построение данных модификаций отображения пекаря, выявлений отличий в их характеристиках и исследование их асимптотического поведения, то есть выявление особенностей (закономерностей) преобразования с ростом числа итераций.

1. Классическое отображение пекаря как авторегрессионная система

Преобразование пекаря как дискретный процесс на единичном квадрате ($0 \le x \le 1$, $0 \le y \le 1$) определяется системой двух разностных уравнений первого порядка [1-12]

$$\begin{aligned} x_{n+1} &= 2x_n, \quad y_{n+1} = y_n/2, \quad 0 \le x_n < 1/2, \\ x_{n+1} &= 2x_n - 1, \quad y_{n+1} = (y_n+1)/2, \quad 1/2 \le x_n \le 1. \end{aligned} \tag{1}$$

В процессе итераций (1) происходит преобразование начальных условий (x_0,y_0), и решение системы (1) может быть однозначно представлено через названные начальные условия и номер итерации n

$$x_n = x_n(x_0,y_0,n), \quad y_n = y_n(x_0,y_0,n), \quad n = 1,2,\ldots . \tag{2}$$

Как мы далее покажем, в случае преобразования пекаря задача Коши (задача однозначного нахождения решения по заданным начальным условиям) носит своеобразный (вырожденный) характер, а именно: с ростом числа итераций влияние начального условия y_0 на решения (2) утрачивается.

Для наших целей (1) удобнее переписать в несколько другом виде. При итерационном процессе (1) координаты (x,y) переходят в координаты $(2x,y/2)$, если $0 \le x < 1/2$, или в координаты $(2x-1,(y+1)/2)$, если $1/2 \le x \le 1$. Таким образом, изменение координаты x при итерациях совершенно не зависит от изменения координаты y. Закон же изменения y, хотя и не включает явной зависимости от x, тем не менее, «управляется» этой координатой посредством выбора правила преобразования в зависимости от подынтервала нахождения x - $[0, 1/2)$ или $[1/2, 1]$.

Учтем последнее обстоятельство явным образом, записав преобразования (1) отдельно по каждой координате. Именно в такой форме записывают диссипативное (не сохраняющее площадь) отображение пекаря [14] (оно

---

[2] Последние публикации в этом направлении: R.M. Machado, M.S. Baptista, C.Grebogi. Cryptography with chaos at physical level (Chaos, Solitons and Fractals. 2004. V. 21. Iss. 5. Pp. 1265-1269); G. Tang, X. Liao, Y. Chen. A novel method for designing S-boxes based on chaotic maps (Chaos, Solitons and Fractals. 2004. V. 21).

отличается от «простого» заменой коэффициента $^1/_2$ при координате y на множитель $a<1$).

Введем характеристическую функцию $\theta_{[a,b]}(x)$ отрезка $[a,b]$. По определению, эта функции равна единице внутри этого отрезка и нулю за его пределами. Объединив законы преобразования координаты x для обеих частей единичного отрезка [0,1], легко увидеть, что эта координата изменяется согласно диадическому преобразованию (сдвигу Бернулли с коэффициентом 2)

$$x_{n+1} = 2x_n\theta_{0,1/2}(x_n) + (2x_n\text{-}1)\theta_{1/2,1}(x_n) = 2x_n - \theta_{1/2,1}(x_n) = \\ = 2x_n - \lfloor 2x_n \rfloor = 2x_n \bmod 1 = \{2x_n\}, \quad 0 \le x_n \ge 1. \tag{3}$$

Здесь символ $\{x\}$ означает дробную часть числа x, а $\lfloor x \rfloor$ - соответственно целую часть этого числа («пол», согласно обозначению Д. Кнута [15]). Соответственно закон преобразования второй координаты будет иметь вид

$$y_{n+1} = (y_n+\theta_{1/2,1}(x_n))/2, \quad 0 \le x_n \le 1, \quad 0 \le y_n \le 1. \tag{4}$$

Интересно, что характеристическая функция отрезка $[\,^1/_2, 1]$ определяет не что иное, как целую часть числа $2x_n$ для любого значения $x_n \in (0,1)$. Следовательно, выражение (4) может быть переписано в форме [16-17]:

$$y_{n+1} = {}^1/_2\, y_n + {}^1/_2 \lfloor 2x_n \rfloor. \tag{5}$$

Выясним действие преобразований (3)-(5) на двоичные представления начальных условий (x_0,y_0). Пусть стартовые значения задаются как

$$x_0 = 0.\beta_1\,\beta_2 \ldots \beta_n \ldots = \Sigma_{p=1}^{\infty}\, \beta_p/2^p \tag{6}$$

и

$$y_0 = 0.\gamma_1\gamma_2\ldots\gamma_n\ldots = \Sigma_{p=1}^{\infty}\, \gamma_p/2^p, \tag{7}$$

где β_p и γ_p - двоичные разряды. Как известно, для иррациональных чисел x_0 и y_0 односторонние последовательности β_p и γ_p являются бесконечными и неповторяющимися последовательностями нулей и единиц. В случае рациональных чисел их двоичные представления могут быть либо конечными, либо периодически повторяющимися последовательностями нулей и единиц.

Используя представление (6), решение нелинейного разностного уравнения (3) можно представить как

$$x_n = \{2^n x_0\} = \Sigma_{p=1}^{\infty}\, \beta_{n+p}/2^p. \tag{8}$$

Тогда преобразование (4) перепишется в виде

$$y_{n+1} = {}^1/_2\,(y_n + \beta_{n+1}), \tag{9}$$

где β_{n+1} суть $(n+1)$-я цифра в двоичном представлении начального значения x_0.

Пусть начальное условие x_0 представляет случайную величину, равномерно распределенную на интервале (0,1). Как установил еще в 1909 году Э. Борель, в этом случае двоичные разряды β_p можно трактовать как независимые, одинаково распределенные дискретные случайные величины, с одинаковой вероятностью $^1/_2$ принимающие значения 0 или 1 [18]. Независимость двоичных разрядов проявляется в том, что совместное вероятностное распределение любой их совокупности представляется произведением вероятностных законов для отдельных разрядов. В случае же, когда начальное значение x_0 не является

равномерно распределенной случайной величиной, его двоичные разряды «теряют» свою независимость. Для двоичного числа в [18] это положение доказывается необыкновенно изящно с использованием тригонометрической формулы Виета. В приложении к статье независимость разрядов случайного числа показывается (непосредственным расчетом многомерного распределения) в общем виде - для совместного распределения разрядов G-ичного числа ($G \geq 2$): в случае равномерного распределения числа x_0 его G-ичные разряды являются независимыми и принимающими значения от 0 до G-1 с равной вероятностью $1/G$. Вопрос этот интересен и в контексте сравнения свойств сдвигов Бернулли с другим фундаментальным отображением в теории чисел - отображением Гаусса, для которого распределение начального значения по инвариантному закону не приводит к независимости коэффициентов разложения числа в непрерывную дробь [19].

С двоичными разрядами числа как его функциями можно соотнести центрированные случайные значения, образующие последовательность Радемахера

$$r_p = (\beta_p - \overline{\beta_p})/\sigma_p = 2\beta_p - 1. \qquad (10)$$

Здесь введены моменты дискретной случайной величины β_p (среднее значение, второй начальный момент, дисперсия)

$$\overline{\beta_p} = {}^1/_2, \ \overline{\beta_p}^2 = {}^1/_2, \ \sigma_\beta{}^2 = \overline{\beta_p}^2 - \overline{\beta_p}^2 = {}^1/_4.$$

Случайные величины (10) принимают два значения, -1, +1, причем с равной вероятностью $^1/_2$, и характеризуются нулевым средним и единичной дисперсией. Выражаемые линейно через β_p величины r_p также являются «независимыми» в указанном выше смысле. В самом деле, начальное значение x_0 через члены последовательности Радемахера может быть выражено как

$$Z_0 = 2X_0 - 1 = \Sigma_{k=1}^{\infty} r_k/2^k.$$

Характеристическая функция случайной величины $Z_0=2X_0-1$ (значение X_0 считается равномерно распределенным) суть

$$\varphi_{Z_0}(t) = \int_0^1 \exp(jt(1-x_0))dx_0 = \sin t/t = \prod_{k=1}^{\infty} \cos(t/2^k)$$

(тригонометрическое равенство и есть формула Виета). В то же время характеристическая функция случайной величины $\varsigma_p=r_p/2^p$ есть

$$\varphi_{\varsigma_p}(t) = {}^1/_2 (\exp(jt/2^p) + \exp(-jt/2^p)) = \cos(t/2^p).$$

Следовательно, производящая функция случайной величины $Z_0=2X_0-1$ как суммы случайных величин $\varsigma_p=r_k/2^k$ представляется в виде произведения характеристических функций отдельных слагаемых

$$\varphi_{Z_0}(t) = \prod_{k=1}^{\infty} \varphi_{\varsigma_k}(t),$$

что и говорит о независимости этих слагаемых. (Данная логика доказательства независимости разрядов двоичного числа использована в [18].)

Случайный характер начального условия x_0 позволяет нам трактовать разностное уравнение (9) как своего рода авторегрессионное уравнение первого порядка (линейный цифровой фильтр), в котором переменная y_{n+1} линейно выражается через переменную y_n и случайный «импульс» $\beta_{n+1}/2$, определяемый

двоичным разрядом начального условия. В других терминах можно говорить, что преобразование пекаря также осуществляет линейную фильтрацию стохастической последовательности Радемахера.

Для нахождения решения разностного уравнения (9), то есть представления y_n через y_0 и номер шага итерации n, воспользуемся техникой одностороннего z-преобразования [20]. Умножим каждый член (9) на z^{-n} и просуммируем от 0 до ∞. Вводя z-преобразование для односторонней бесконечной последовательности y_n

$$Y(z) = \Sigma_{n=0}^{\infty} y_n z^{-n}, \tag{11}$$

z-преобразования для односторонних бесконечных числовых последовательностей 2^{-n} и $2^{-(n+1)}$

$$H_0(z) = \Sigma_{n=0}^{\infty} 2^{-n} z^{-n} = 1/(1-(2z)^{-1}), \tag{12}$$

$$H(z) = \Sigma_{n=0}^{\infty} 2^{-(n+1)} z^{-n} = 1/(2-z^{-1}) \tag{13}$$

и z-преобразование односторонней бесконечной последовательности двоичных разрядов числа x_0

$$B(z) = \Sigma_{n=0}^{\infty} \beta_n z^{-n}, \quad \beta_0 = 0, \tag{14}$$

получим из (9), что $Y(z)$ удовлетворяет уравнению

$$Y(z) = H_0(z) y_0 + H(z) B(z) = 1/(1-(2z)^{-1}) y_0 + 1/(2-z^{-1}) B(z). \tag{15}$$

Соотношения (12)-(15) справедливы для области комплексного z, удовлетворяющей условию $|z|>1$. Вычисляя обратное преобразование от (11), найдем представление для n-й итерации координаты y

$$\begin{aligned} y_n = (1/2)^n y_0 + (1/2)^{n+1} \otimes \beta_n = \Sigma_{p=1}^{\infty} \gamma_p / 2^{p+n} + \Sigma_{p=0}^{n} \beta_p / 2^{n+1-p} = \\ = 0.\beta_n \beta_{n-1} \beta_{n-2} \ldots \beta_2 \beta_1 \gamma_1 \gamma_2 \ldots . \end{aligned} \tag{16}$$

Здесь символом $\otimes$ обозначена свертка последовательностей β_p и

$$h(n) = (1/2)^{n+1} \Theta(n), \quad \Theta(n) = \begin{cases} 1, & n \geq 0, \\ 0, & n < 0. \end{cases}$$

Нахождение точных решений (8) и (12) нелинейных разностных уравнений (1), определяющих динамику отображения пекаря, позволяет четко выявить следующие его свойства.

1. «Сжимающая» координата y_n на каждом шаге итераций выражается двоичной дробью, первыми n разрядами которой являются записанные в обратном порядке n первых разрядов стартового значения x_0 «растягивающей» координаты, а последующие позиции занимают двоичные разряды стартового значения y_0.

2. С каждой итерацией последовательность разрядов, отвечающих y_0, в представлении для y_n сдвигается вправо на одну позицию.

3. В асимптотике (при $n \to \infty$) главную роль в формировании значения y_n играют первые n разрядов начального значения x_0; «ценность» (значимость) же разрядов начального значения y_0 самой «сжимающей» координаты в представлении y_n «утрачивается».

4. Установившийся стационарный режим пары (x_n, y_n) можно принимать как

стационарный режим авторегрессионной системы, не зависящий от распределения начального условия y_0.

2. «Инверсное» отображение пекаря

Классическое отображение пекаря (1) (или в покоординатной форме (3), (4)) строится на основе двоичного сдвига Бернулли, применяемого для описания динамики «растягивающей» координаты. Если в правых частях названных уравнений провести замену переменных по правилу $x \leftarrow 1-x$, $y \leftarrow 1-y$, получим двумерное отображение в форме:

$$x_{n+1} = 1 - \{2x_n\} = (1-2x_n)\theta_{0,1/2}(x_n) + (2-2x_n)\theta_{1/2,1}(x_n), \qquad (17)$$

$$y_{n+1} = {}^1\!/_2\,(1-y_n)\theta_{0,1/2}(x_n) + (1-{}^1\!/_2\,y_n)\theta_{1/2,1}(x_n). \qquad (18)$$

Уравнение (17) определяет так называемый «зеркальный» сдвиг Бернулли (reflected Bernoulli map) [21]. Оно характеризуется отрицательным угловым коэффициентом линейных составляющих. Двумерное отображение (17)-(18) по этой причине можно назвать «зеркальным» отображением пекаря. Даваемая им картина перемешивания точек - зеркальный аналог картины двумерной динамики, даваемой обычным отображением пекаря. С отображением (17)-(18) можно соотнести и термин «инверсное» отображение пекаря, поскольку точные решения для координат выражаются через инвертированные двоичные разряды начального значения x_0 [22]. В самом деле, с учетом представлений (6) и (8) получим точное решение для уравнения (17)

$$x_n = \Sigma_{p=1}^{\infty}\,{}^1\!/_2{}^p - \Sigma_{p=1}^{\infty}\beta_{n+p}2^p = \Sigma_{p=1}^{\infty}(1-\beta_{n+p})/2^p = \Sigma_{p=1}^{\infty}\overline{\beta}_{n+p}/2^p, \qquad (19)$$

где $\overline{\beta}_k = 1-\beta_k$ - инвертированные двоичные разряды начального значения x_0. В то же время закон преобразования второй компоненты отображения имеет вид

$$y_{n+1} = -\,{}^1\!/_2\,y_n + {}^1\!/_2 + {}^1\!/_2\lfloor 2x_n \rfloor = -\,{}^1\!/_2\,y_n + {}^1\!/_2 + {}^1\!/_2\,\overline{\beta}_{n+1}, \qquad (20)$$

или

$$y_{n+1} = {}^1\!/_2\,(1-y_n+\lfloor 2\{(-2)^n x_0\}\rfloor),$$

где

$$\{(-2)^n x_0\} = \begin{cases} \{2^n x_0\}, & n = 2k, \\ 1 - \{2^n x_0\}, & n = 2k+1, \quad k = 0,1,\ldots . \end{cases}$$

В отличие от классического варианта (9) в уравнении для «инверсного» отображения (20) изменился знак при y_n и появился постоянный член ${}^1\!/_2$. Если применить z-преобразование к (20), возникает положительная составляющая в решении относительно y_n, дополнительно обусловливающая положительность этого значения. Но отмеченная для классического преобразования пекаря тенденция сохраняется: с ростом n начальное значение y_0 все в меньшей степени влияет на y_n, поскольку в решение оно входит как $(-{}^1\!/_2)^n y_0$. Однако замещение начальных разрядов y_0 в решении для y_n происходит по более сложному правилу, чем в соответствующем выражении для классического случая (16) - инвертированные разряды $\overline{\beta}_p$ начального значения x_0 участвуют в формировании y_n с множителем $(-1)^{n+1-p}$.

Инверсное отображение пекаря, как и классический аналог, имеет равномерную инвариантную плотность. Это следует из вида оператора Перрона - Фробениуса этого отображения

$$P\psi(x,y) = \psi((1\text{-}x)/2, 1\text{-}2y)\,\theta_{0,1/2}(x) + \psi((2\text{-}x)/2, 2(1\text{-}y))\,\theta_{1/2,1}(x). \qquad (21)$$

Для сравнения приведем запись эволюционного оператора для классического отображения [7]

$$P\psi(x,y) = \psi(x/2, 2y)\,\theta_{0,1/2}(y) + \psi((x+1)/2, 2y\text{-}1)\,\theta_{1/2,1}(y). \qquad (22)$$

Первые аргументы функций, представленных в правых частях выражений (21) и (22), преобразуются по закону для y-компоненты отображения пекаря, а вторые аргументы - по закону для x-компоненты. Первой собственной функцией (с единичным собственным числом) операторов (21) и (22) является плотность равномерного распределения в единичном квадрате $f(x,y)=1$.

3. G-адическое отображение пекаря

В отличие от классического отображения пекаря в G-адическом преобразовании управляющим является G-ичный сдвиг Бернулли [23]. Запишем это отображение в обозначениях раздела 1

$$x_{n+1} = \{Gx_n\} = \begin{cases} Gx_n, & 0 \le x_n < 1/G, \\ Gx_n - 1, & 1/G \le x_n < 2/G, \\ \cdots & \\ Gx_n - k, & k/G \le x_n < (k+1)/G, \\ \cdots & \\ Gx_n - (G\text{-}1), & (G\text{-}1)/G \le x_n \le 1. \end{cases} \qquad (23)$$

$$y_{n+1} = 1/Gy_n + 1/G\lfloor Gx_n \rfloor = \begin{cases} y_n/G, & 0 \le x_n < 1/G, \\ (y_n+1)/G, & 1/G \le x_n < 2/G, \\ \cdots & \\ (y_n+k)/G, & k/G \le x_n < (k+1)/G, \\ \cdots & \\ (y_n+G\text{-}1)/G, & (G\text{-}1)/G \le x_n \le 1. \end{cases} \qquad (24)$$

Сдвиг Бернулли с целым коэффициентом G соотносится с G-ичным представлением числа. Так, начальное значение x_0 в этой системе счисления будет иметь вид

$$x_0 = \Sigma_{p=1}^{\infty} \beta_p/G^p = (0.\beta_1\beta_2\ldots\beta_n\ldots)_G,$$

где β_k играют роль G-ичных цифр. Соответственно точное решение для разностного уравнения (23) представится как

$$x_n = \{G^n x_n\} = (0.\beta_{n+1}\beta_{n+2}\ldots)_G = \Sigma_{p=1}^{\infty}\beta_{n+p}/G^p. \qquad (25)$$

Подставляя (25) в (24), найдем, что вторая координата обобщенного отображения пекаря удовлетворяет разностному уравнению

$$y_{n+1} = (y_n + \beta_{n+1})/G. \tag{26}$$

Применяя к (26) z-преобразование для односторонних последовательностей, найдем, что функция

$$Y(z) = \Sigma_{n=0}^{\infty} y_n z^{-n}$$

удовлетворяет уравнению

$$Y(z) = H_0(z)y_0 + H(z)B(z), \tag{28}$$

где

$$H_0(z) = Gz/(Gz\text{-}1), \quad H(z) = z/(Gz\text{-}1), \quad B(z) = \Sigma_{n=1}^{\infty}\beta_n z^{-n}.$$

Обратное преобразование от (28) дает решение для итерированных значений y_n:

$$\begin{aligned} y_n = y_0/G^n + \Sigma_{p=1}^{n}\beta_n/G^{n+1-p} = (0.00\ldots0\gamma_1\gamma_2\ldots\gamma_n\ldots)_G + (0.\beta_n\,\beta_{n-1}\ldots\beta_1)_G = \\ = (0.\beta_n\,\beta_{n-1}\ldots\beta_1\gamma_1\gamma_2\ldots\gamma_n\ldots)_G, \end{aligned} \tag{29}$$

где первые n позиций числа y_0/G^n занимают нули.

Решения (25) и (29), отвечающие обобщенному отображению пекаря, имеют структуру, совершенно аналогичную классическому случаю, и выводы для G=2 сохраняют силу и для произвольного целого G>2, а именно: G-ичное представление для y_n имеет в составе первые n G-ичные разряды x_0, записанные в обратном порядке, продолжаемые G-ичными разрядами y_0. С ростом n разряды, отвечающие y_0, оттесняются вправо разрядами x_0. А компонента y_n удовлетворяет уравнению линейного цифрового фильтра первого порядка, в котором роль возмущения играет (n+1)-й разряд в G-ичной записи x_0.

4. В каком смысле обратимо преобразование пекаря?

Остановимся на трактовке понятия «обратимости» преобразования пекаря в контексте представления его каузальным линейным цифровым фильтром, описываемым уравнениями (9), (15) и (16). Этот фильтр характеризуется передаточной функцией (13), которая имеет особенности (нуль и полюс) внутри круга |z|<1 на комплексной плоскости. Следовательно, за пределами этого круга, где определено z-преобразование для разностного уравнения (9), передаточная функция обратима. Соответственно для обратной передаточной функции $H^{-1}(z)=2\text{-}z^{-1}$ «входная» последовательность β_p может быть однозначно определена через «выходную» последовательность y_n.

С отображением пекаря можно соотнести преобразование, описывающее движение в «прошлое», в направлении уменьшения индекса n. Оно задается теми же самыми (по форме) уравнениями, что и «прямое» движение в «будущее», в сторону возрастания n. В самом деле, из (23) можно получить, что

$$x_{n+1} = Gx_n - \lfloor Gx_n \rfloor = Gx_n - \lfloor G\{G^n x_0\} \rfloor = Gx_n - \lfloor G{\cdot}0.\beta_{n+1}\beta_{n+2}\ldots \rfloor = Gx_n - \beta_{n+1},$$

откуда следует, что

$$x_n = (x_{n+1}+\beta_{n+1})/G. \tag{30}$$

В то же время из (26) вытекает, что

$$\{Gy_{n+1}\} = \{y_n+\beta_{n+1}\} = \{y_n\} = y_n, \qquad (31)$$

поскольку β_k не имеет дробной части, принимая либо нулевое значение, либо целое из диапазона от 1 до G-1. Формально меняя в (30) и (31) обозначения переменных ($x \leftrightarrow y$), придем к уравнениям

$$x_n = \{Gx_{n+1}\}, \qquad (32)$$

$$y_n = (y_{n+1}+\beta_{n+1})/G. \qquad (33)$$

Сравнение систем уравнений (23), (26) и (32), (33) показывает, что заданные отображения пригодны (при обмене ролями между пространственными координатами) как для описания «будущего», так и для описания «прошлого». И только в этом смысле их можно считать «обратимыми».

В то же время отдельный закон изменения «растягивающей» координаты, даваемый сдвигом Бернулли, не является взаимно-однозначным преобразованием, то есть не является обратимым в общепринятом теоретико-функциональном смысле.

Заключение

Классическое отображение пекаря в известной авторам литературе описывается, в основном, на качественном уровне, и соотносимые с ним определения тоже носят скорее интуитивный характер. Поскольку это отображение является базовым при иллюстрации понятий эргодичности и перемешиваемости в эргодической теории (теории хаотических динамических систем), в этой работе представлены точные решения для координатных составляющих этого отображения - как для «классического» варианта, так и для некоторых разновидностей этого отображения. Отображения, характеризуемые одной и той же инвариантной плотностью, имеет смысл изучать по той простой причине, что они отличаются друг от друга рядом других важных характеристик, например, скоростью перемешивания (значением показателя Ляпунова), поведением автокорреляционных функций, решением спектральных задач для оператора Перрона - Фробениуса.

Основной вывод, следующий из проведенного математического описания, таков: уравнение «сжимающей» координаты отображения пекаря в любой из своих модификаций - это уравнение для выходного сигнала дискретного устойчивого, каузального, обратимого фильтра, на входе которого действует случайная последовательность в форме G-ичных (инвертированных G-ичных) разрядов начального значения x_0. Этот фильтр описывается линейной авторегрессионной моделью первого порядка. В асимптотике эта модель обладает свойством «забывчивости» по отношению к начальному значению «сжимающей» координаты y_0.

Приложение

О распределении G-ичных разрядов случайного числа

Рассмотрим G-ичное представление некоторого числа x_0:

$$x_0 = 0.\beta_1\beta_2\ldots\beta_n\ldots = \Sigma_{p=1}^{\infty}\beta_p/G^p. \qquad (A1)$$

G-ичные разряды β_n числа как его функции определяются посредством операции сдвига

$$\beta_n(x_0) = \lfloor 2\{2^{n-1}x_0\}\rfloor, \quad n = 1,2,\ldots . \tag{A2}$$

Предположим, что рассматриваемое число является случайным, имеющим плотность распределения $f_0(x_0)$ и интегральный закон $F_0(x_0)=\int_0^{x_0} f_0(x)dx$. На основе представления (А2) возможно определение одномерного закона распределения для G-ичных разрядов числа $\beta_n(x_0)$

$$f_n(\beta_n) = \int_0^1 \delta(\beta_n-\lfloor G\{G^{n-1}x_0\}\rfloor) f_0(x_0)dx_0 = \sum_{q=0}^{G-1} \delta(\beta_n-q)P(\beta_n=q), \tag{A3}$$

где вероятность принятия разрядом значения q (q=0,1,...,G-1) определяется выражением

$$P(\beta_n=q) = \sum_{p=0}^{G^{n-1}-1} (F_0(p/G^{n-1}+q/G^n+1/G^n)-F_0(p/G^{n-1}+q/G^n)). \tag{A4}$$

Техника получения (А4) является типичной при подсчете и многомерных распределений, поэтому остановимся на ней несколько более подробнее. Проводя в (А3) замену переменных по правилу $\xi=G^{n-1}x_0$, получим

$$f_n(\beta_n) = \int_0^{G^{n-1}} \delta(\beta_n-\lfloor G\{\xi\}\rfloor) f_0(\xi/G^{n-1})d\xi/G^{n-1} = \sum_{p=0}^{G^{n-1}-1} \int_p^{p+1} \delta(\beta_n-\lfloor G\{\xi\}\rfloor) f_0(\xi/G^{n-1})d\xi/G^{n-1} =$$

$$= \sum_{p=0}^{G^{n-1}-1} \int_0^1 \delta(\beta_n-\lfloor G\eta\rfloor) f_0((p+\eta)/G^{n-1})d\eta/G^{n-1} .$$

Вводя переменную $\varsigma=G\eta$, получим далее

$$f_n(\beta_n) = \sum_{p=0}^{G^{n-1}-1} \int_0^G \delta(\beta_n-\lfloor\varsigma\rfloor) f_0((p+\varsigma/G)/G^{n-1})d\varsigma/G^n =$$

$$\sum_{p=0}^{G^{n-1}-1} \sum_{q=0}^{G-1} \int_q^{q+1} \delta(\beta_n-\lfloor\varsigma\rfloor) f_0((p+\varsigma/G)/G^{n-1})d\varsigma/G^n =$$

$$= \sum_{p=0}^{G^{n-1}-1} \sum_{q=0}^{G-1} \int_0^1 \delta(\beta_n-q) f_0((Gp+q+\xi)/G^n)d\xi/G^n =$$

$$= \sum_{q=0}^{G-1} \delta(\beta_n-q) \sum_{p=0}^{G^{n-1}-1} \int_0^{1/G^n} f_0((Gp+q+\xi)/G^n)d\xi.$$

Отсюда следует, что

$$P(\beta_n=q) = \sum_{p=0}^{G^{n-1}-1} \int_0^{1/G^n} f_0((Gp+q+\xi)/G^n)d\xi,$$

что эквивалентно (А4).

Когда начальное распределение x_0 является равномерным ($F_0(x)=x$), из (А4) следует, что принятие *любым* G-ичным разрядом этого числа любого значения (0,1,...,G-1) является *равновероятным*

$$P(\beta_n=0) = P(\beta_n=1) = \ldots = P(\beta_n=G-1) = 1/G. \tag{A5}$$

Отличие распределения числа x_0 от равномерного ведет к нарушению (А5), то есть в общем случае вероятность принятия разрядом значений 0,1,2,...,G-1 не

является одинаковой, причем соответствующие вероятности становятся зависящими от номера разряда n

$$P(\beta_n=0) = \Sigma_{p=0}^{G^{n-1}-1} (F_0(p/G^{n-1} + 1/G^n) - F_0(p/G^{n-1})),$$

$$P(\beta_n=1) = \Sigma_{p=0}^{G^{n-1}-1} F_0(p/G^{n-1} + 2/G^n) - F_0(p/G^{n-1}+1/G^n)$$

и т.д., причем нормировочное соотношение выполняется

$$P(\beta_n = 0) + P(\beta_n = 1) +... + P(\beta_n = G - 1) = 1.$$

Соотношения (А4), (А5) дают вероятности принятия G-ичными разрядами числа значений 0, 1, 2, ..., G-1, но из них не следуют какие-либо выводы о статистической зависимости или независимости величин β_n. Для ответа на этот вопрос необходимо найти выражение для совместного распределения n G-ичных разрядов числа. Используя (А2) и развитую выше технику расчетов, найдем для n-мерной плотности распределения разрядов случайного числа x_0

$$f_n(\beta_1,\beta_2,\ldots,\beta_n) = \int_0^1 \delta(\beta_1-\lfloor Gx_0 \rfloor)\delta(\beta_2-\lfloor G\{Gx_0\} \rfloor)\ldots\delta(\beta_n-\lfloor G\{G^{n-1}x_0\} \rfloor) f_0(x_0)dx_0 =$$

$$= \Sigma_{p_1=0}^{G-1} \Sigma_{p_2=0}^{G-1} \ldots \Sigma_{p_n=0}^{G-1} \delta(\beta_1-p_1)\delta(\beta_2-p_2)\ldots\delta(\beta_n-p_n) \int_0^{1/G^n} f_0(\Sigma_{i=1}^{n} p_i/G^i+\xi)\, d\xi.$$

Здесь целочисленные величины p_i (i=1,2,...,n,) могут принимать значения от 0 до G-1. Поэтому совместное распределение n дискретных случайных величин $\beta_1,\beta_2,\ldots,\beta_n$ будет иметь вид

$$P(\beta_1=p_1, \beta_2=p_2, \ldots, \beta_n=p_n) = F_0(\Sigma_{i=1}^{n} p_i/G^i + 1/G^n) - F_0(\Sigma_{i=1}^{n} p_i/G^i). \qquad (A6)$$

Только для равномерного распределения числа его разряды оказываются независимыми величинами - совместная плотность распределения (А6) представляется произведением маргинальных плотностей $P(\beta_i=p_i)$

$$P(\beta_1=p_1, \beta_2=p_2, \ldots, \beta_n=p_n) = 1/G^n.$$

Таким образом, двоичные разряды случайного числа действительно могут считаться одинаково распределенными и независимыми в случае равномерного распределения этого числа (равномерное распределение является *инвариантным* для сдвигов Бернулли). В случае иного распределения числа его двоичные разряды оказываются зависимыми величинами с индивидуальными законами распределения.

Несколько иная ситуация имеет место при разложении случайного числа в непрерывную дробь, осуществляемом в результате преобразования Гаусса [19]. Равномерное распределение в данном случае не является инвариантным, причем коэффициенты разложения являются зависимыми величинами в любом случае, даже если распределение числа и будет описываться инвариантным для данного преобразования законом, хотя маргинальные законы для коэффициентов, как и для двоичного формата числа, будут одинаковыми.

Выражение членов числовых последовательностей x_n и y_n через x_0 и y_0 при случайном характере начальных значений суть формулировки *прямого* вероятностного описания случайных величин x_n и y_n. *Косвенное* вероятностное описание тех же самых величин (то есть через вероятностные распределения) заключается в формулировке уравнения Перрона - Фробениуса и нахождении его решений.

Библиографический список

1. *Хопф Э.* Эргодическая теория // УМН. 1949. Т. 4. Вып. 2(39). С. 113.

2. *Халмош П.* Лекции по эргодической теории. Ижевск: РХД, 2001. 132 с.

3. *Арнольд В.И., Авец А.* Эргодические проблемы классической механики. Ижевск: РХД, 1999. 284 с.

4. *Рид М., Саймон Б.* Методы современной математической физики. Функциональный анализ. М.: Мир, 1977. 360 с.

5. *Корнфельд И.П., Фомин С.В., Синай Я.Г.* Эргодическая теория. М.: Наука, 1980. 383 с.

6. *Лихтенберг А., Либерман М.* Регулярная и стохастическая динамика. М.: Мир, 1984. 528 с.

7. *Lasota A., Mackey M.C.* Probabilistic properties of deterministic systems. Cambridge: Cambridge University Press, 1985. 358 p.

8. *Николис Г., Пригожин И.* Познание сложного. М.: Мир, 1990. 334 с.

9. *Пригожин И.* Конец определенности. Время, хаос и новые законы природы. Ижевск: РХД, 2000. 208 с.

10. *Табор М.* Хаос и интегрируемость в нелинейной динамике. М.: Эдиториал УРСС. 2001. 320 с.

11. *Шредер М.* Фракталы, хаос, степенные законы. Миниатюры из бесконечного рая. Ижевск: РХД, 2001. 528 с.

12. *Кузнецов С.П.* Динамический хаос. Курс лекций. М.: Физматлит, 2001. 296 с.

13. *Gaspard P.* Diffusion, effusion and chaotic scattering: An exactly solvable Liouvillian dynamics // J. Stat. Phys.1992.Vol. 68, № 5/6. P. 673.

14. *Шустер Г.* Детерминированный хаос. Введение. М.: Мир, 1988. 240 с.

15. *Грэхем Р., Кнут Д., Паташник О.* Конкретная математика. Основание информатики. М.: Мир, 1998. 703 с.

16. *Голубенцев А.Ф., Аникин В.М., Ноянова С.А.* О связи преобразования пекаря с авторегрессионной моделью первого порядка // Вторая международная конференция «Фундаментальные проблемы физики». Саратов, Россия, 9-14 октября 2000. Материалы конференции. Саратов: ГосУНЦ «Колледж», 2000. С. 63.

17. *Goloubentsev A.F., Anikin V.M., Noyanova S.A., Barulina Y.A.* Baker transformation as autoregression system // Int. Conf. «Physics and Control». Proceedings. Saint Petersburg, Russia, August 20-22, 2003. P. 654.

18. *Кац М.* Статистическая независимость в теории вероятностей, анализе и теории чисел. М.: Иностранная литература, 1963. 165 с.

19. *Голубенцев А.Ф., Аникин В.М.* Евклид, Гаусс и детерминированный хаос // Известия Саратовского университета. Новая серия. 2003. Т. 3, вып. 2. С. 166.

20. *Рабинер Л., Гоулд Б.* Теория и применение цифровой обработки сигналов. М.: Мир, 1978. 848 с.

21. *Driebe D.J., Ordonez G.E.* Using symmetries of the Frobenius-Perron operator to determine spectral decompositions // Phys. Lett. A. 1996. Vol. 211. P. 204.

22. *Голубенцев А.Ф., Аникин В.М., Ноянова С.А.* «Инверсное» отображение пекаря // 6th International School on chaotic oscillations and pattern formation. Saratov, Russia, October 2-7, 2001. The Book of abstracts. Саратов, ГосУНЦ «Колледж», 2001. С. 59.

23. *Antoniou I., Tasaki S.* Generalized spectral decomposition of mixing dynamical systems // Int. J. of Quantum Chemistry. 1993. Vol. 46. P. 425.

Саратовский государственный университет

Поступила в редакцию 26.04.04

MODIFICATIONS OF THE BAKER TRANSFORMATION AND THEIR ASIMPTOTIC PROPERTIES

A.F. Goloubentsev, *V.M. Anikin, S.A. Noyanova*

Some modifications of the baker transformation are introduced. The equations for the brunches of the maps are solved exactly. It is shown that the y-component of baker transformations is represented by a linear autoregression equation of the first order where digits of the initial value x_0 play the role of an excitation (input signal) if x_0 is considered as a random value. It is shown that the digital filter corresponding to the baker transformation is causal, stable and reversible one. The asymptotic regime of baker transform dynamics does not depend on the distribution of the initial value y_0. Investigations of asymptotic properties of the baker map are important for chaos-based key cryptography schemes for digital communication.

Голубенцев Александр Федорович (1933 - 2003) - доктор физико-математических наук, профессор. Заведовал кафедрой вычислительной физики и автоматизации научных исследований СГУ. Автор 7 монографий, 7 учебных пособий и 150 статей по статистической электронике и радиофизике, нелинейной динамике.

Аникин Валерий Михайлович - родился в 1947 году в Аткарске Саратовской области. После окончания в 1970 году с отличием физического факультета СГУ работал в НИИ механики и физики СГУ, с 1984 года - на кафедре вычислительной физики и автоматизации научных исследований СГУ. Кандидат физико-математических наук, доцент. Область научных интересов - аналитическое моделирование стохастических и хаотических процессов. Автор 5 монографий и 70 научных статей, научный редактор специальных выпусков журналов «Applied Surface Science» и «Радиотехника», сборника памяти А.Ф. Голубенцева и др. изданий. С 1990 года - ученый секретарь докторского диссертационного совета при СГУ по радиофизике, физической электронике, оптике и твердотельной электронике. В 2000-2003 - секретарь Всемирной конференции по вакуумным источникам электронов (IVESC).

E-mail: Anikinvm@info.sgu.ru

Ноянова Светлана Анатольевна родилась в 1971 году во Львове. В 1993 с отличием окончила физический факультет Саратовского государственного университета. В 1993-1996 - аспирант кафедры ядерной физики, с 1998 - сотрудник кафедры вычислительной физики и автоматизации научных исследований СГУ, с марта 2003 - ассистент кафедры. Область научных интересов - нелинейная динамика.