ПЕРЕДАЧА ДАННЫХ В ПОСЛЕДОВАТЕЛЬНОСТИ СЛУЧАЙНЫХ ЧИСЕЛ

Беспалов Е.С., Мусянков М.И., Родичев П.В.

Московский государственный институт радиотехники,
электроники и автоматики (технический университет)
Кафедра космических информационных технологий
117454, Москва, проспект Вернадского, 78, тел. 434-93-83

Реферат. Рассматривается способ передачи данных в последовательности случайных чисел с помощью переключаемых генераторов хаотических колебаний. Приведены алгоритмы расчета информационных параметров для ряда квадратичных отображений. Описана процедура обработки последовательности с малым временем расцепления корреляции между элементами.

Для генерации хаотических цифровых последовательностей [1,2] используются алгоритмы, построенные на основе конечноразностных отображений [3,4], а в качестве одного из способов ввода информации рассматривается модуляция управляющих параметров этих отображений [5].

Однако собственно хаос наблюдается лишь при определенных оптимальных значениях управляющих параметров, поэтому модуляция может нарушить условия наибольшей глубины хаоса или привести к увеличению времени расцепления корреляции между элементами последовательности [1,6].

Вместе с тем, для построения бинарных систем передачи данных с помощью мультиплексора можно создать поток случайных чисел от двух генераторов, в каждом из которых управляющие параметры выбраны оптимальными или, по крайней мере, обеспечивается малое время расцепления корреляции. При этом управляющий параметр служит передаваемым символом.

В данной работе приведены алгоритмы расчета указанных информационных параметров для ряда известных отображений и дан пример обработки последовательности , в которой сохраняется малое время расцепления корреляции между элементами.

Рассматривается квадратичное отображение вида:

$$x_{n+1} = \alpha \cdot x_{n-1} + \beta \cdot x_n + \gamma \cdot x_n^2 + \delta, \qquad n = 1,2,..., \tag{1}$$

где: n – дискретное время;
x_n – n-ый элемент последовательности;
α, β, γ, δ – управляющие параметры.

Согласно (1), любой из четырех параметров α, β, γ, δ может быть рассчитан, если известны шесть соседних элементов цифровой последовательности, полученной с помощью данного отображения.

В ряде классических частных случаев оптимальные значения управляющих параметров известны. При α=0, β=4, γ= –4, δ=0 из (1) следует отображение Ферхюльста. Для α=0.3, β=0, γ= –1.4, δ=1 из (1) получается отображение Хенона. Если в (1) положить α=0, β= –1.57, γ=2, δ=0, получится отображение, рассмотренное в [6].

Для отображений, в которых α=0, δ=0 из (1) следует:

$$x_{n+1} = \beta \cdot x_n + \gamma \cdot x_n^2, \tag{2}$$

$$x_{n+2} = \beta \cdot x_{n+1} + \gamma \cdot x_{n+1}^2, \tag{3}$$

Тогда из (2), (3) получится:

$$\gamma = \frac{B^2 - A \cdot C}{A \cdot B \cdot (A - B)}; \tag{4}$$

$$\beta = \frac{A^2 \cdot C - B^3}{A \cdot B \cdot (A - B)}, \tag{5}$$

где: $A=x_n$; $B=x_{n+1}$; $C=x_{n+2}$.

Согласно (4), (5), управляющие параметры генераторов подобного типа могут быть рассчитаны в результате нелинейной обработки трех соседних чисел последовательности.

Если на приемной стороне известен тип генератора и один из параметров, то для расчета другого параметра достаточно двух соседних чисел. Так, для генератора Ферхюльста из (2) получится:

$$\gamma = \frac{B - 4 \cdot A}{A^2}; \tag{6}$$

$$\beta = \frac{B + 4 \cdot A^2}{A}; \tag{7}$$

Для отображения, рассмотренного в [6], из (2) следует:

$$\gamma = \frac{B + 4 \cdot A^2}{A}; \tag{8}$$

$$\beta = \frac{B - 2 \cdot A^2}{A}; \tag{9}$$

Для случая β=0, γ=1 из (1) получится:

$$\alpha = \frac{B^2 \cdot (1 - D) - C^2 \cdot (1 - C)}{A \cdot C^2 - B^3}; \tag{10}$$

$$\gamma = \frac{B \cdot (1 - C) - A \cdot (1 - D)}{A \cdot C^2 - B^3}, \tag{11}$$

где: $A=x_{n-1}$; $B=x_n$; $C=x_{n+1}$; $D=x_{n+2}$.

Если адресату известен тип генератора и один из оптимальных параметров, то необходимое для расчета количество соседних элементов последовательности уменьшится.

Так, в случае генератора Хенона можно получить следующие формулы:

$$\alpha = \frac{1.4 \cdot B^2 + C - 1}{A}; \tag{12}$$

Факторами, определяющими подбор пар коммутируемых генераторов, являются:

количество чисел последовательности, необходимое для оценки информационного параметра;

интервал чисел генерируемой последовательности;

время, затрачиваемое на расчет по данному алгоритму;

близость статистических характеристик генерируемых последовательностей.

$$\gamma = \frac{C - 0.3 \cdot A - 1}{B^2}, \tag{13}$$

В качестве меры, определяющей пригодность генератора, можно использовать время расцепления корреляции между элементами последовательностей.

Например, для отображения вида:

$$x_{n+1} = \{k \cdot x_n\}, \qquad n = 1,2,..., \tag{14}$$

где знак {...} обозначает дробную часть заключенного в скобки аргумента, а управляющий параметр k>1, время расцепления корреляции τ определяется выражением:

$$\tau = \frac{1}{\ln k} \tag{15}$$

Для k>>1 элементы последовательности могут считаться статистически независимыми [1]. Согласно (14), двоичный символ следует передавать двумя числами последовательности. Например, при передаче «нуля» используются два числа от генератора с k=5π, а при передаче «единицы» передаются числа с генератора с k=10π. В рассматриваемом ниже примере оба генератора запускаются одновременно при начальном значении x=0.1.

Пусть требуется передать сообщение Λ вида «0; 0; 0; 1; 1; 0; 1; 0». Если предельная ошибка округления числа равна 0.0005, то в линию поступит последовательность чисел: «0.1; 0.571; 0.966; 0.175; 0.743; 0.673; 0.246; 0.719; 0.596; 0.710; 0.233; 0.665; 0.165; 0.186; 0.245; 0.849». Процедура обработки этой последовательности в приемнике поясняется схемой на рис. 1, где приняты следующие обозначения:

БН – буфер-накопитель;

БПОПР – блок поиска, обработки и принятия решения;

Δx^*_{n+1} ошибка канала 5π;

$\Delta \tilde{x}_{n+1}$ ошибка канала 10π;

Λ – полученная двоичная последовательность;

$f_в$ – частота выбора пар чисел x_n и x_{n+1} (в два раза меньшая частота следования цифр).

Верным считается сообщение канала, в котором ошибка Δx_{n+1} меньше. В рассмотренном примере отношение ошибок ложного и истинного каналов в наихудшем случае превышает 25 раз.

Сформированные подобным образом цифровые последовательности могут быть использованы и в аналоговых системах, например, в ЧМ-генераторах с хаотической частотой поднесущего колебания.

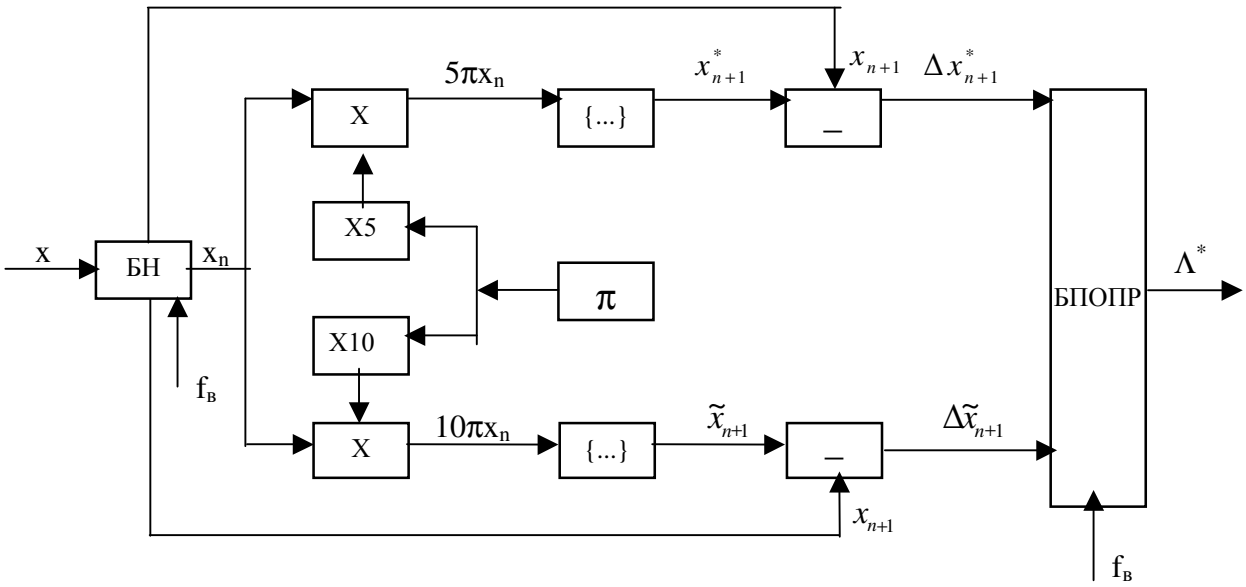

Рис. 1.

Литература

1. Заславский Г.М. Статистическая необратимость в нелинейных системах. – Москва.: Наука, 1970. – 144 с.

2. Бельский Ю.Л., Дмитриев А.С. Передача информации с использованием детерминированного хаоса // Радиотехника и электроника, 1993, №7. – с. 1310–1315.

3. Кулешов В.Н., Ларионова М.В., Удалов Н.Н. Система передачи информации с хаотической несущей // Вестник МЭИ, 1997, №5. – с. 54–61.

4. Дмитриев А.С., Панас А.И., Старков С.О. Динамический хаос как парадигма современных систем связи // Зарубежная радиоэлектроника. Успехи современной радиоэлектроники, 1997, №10. – с. 4–26.

5. Капранов М.В., Морозов А.Г. Использование хаотической модуляции для передачи информации // Радиотехнические тетради, 1998, №4. – с. 66–71.

6. Основы теории колебаний: Учеб. руководство / В.В. Мигулин, В.И. Медведев, Е.Р. Мустель, В.Н. Парыгин; под. ред. В.В. Мигулина. – М.: Наука, 1998. – 392 с.

DATA TRANSFER IN A SEQUENCE OF RANDOM NUMBERS

Bespalov E.S., Musyankov M.I., Rodichev P.V.

Moscow state institute of radioengineering,
electronics and automatics (technical university)
Department of space informational technologies
117454, Russia, Moscow, Vernadskogo avenue, 78, ph. 434-93-83

Abstract. The mode of data transfer in a random numbers sequence with the help of switched generators of chaotic oscillations is considered. The calculation algorithms of information parameters for a series of square-law maps are led. The procedure of handling of a sequence with small unhook correlation time between the elements is described.

For generation of chaotic digital sequences [1,2] the algorithms based on finite differences maps are used [3,4], and as one of modes of input an information the modulation of controlling parameters of these maps [5] is considered.

However purely chaos is observed only at particular best values of controlling parameters, therefore modulation can break conditions of the greatest chaos depth or to increase an unhook correlation time between sequence's elements [1,6].

At the same time, for a construction of binary data transfer systems with the help of multiplexer it is possible to create a stream of random numbers from two generators, in each of which the controlling parameters are selected optimum or, at any rate, the small unhook correlation time is ensured. Thus the controlling parameter is a transmitted symbol.

In this work the calculation algorithms of indicated information parameters for a series of known maps are led and the example of handling of a sequence is given, in which the small unhook correlation time between the elements is a constant.

The square-law map of an aspect is considered:

$$x_{n+1} = \alpha \cdot x_{n-1} + \beta \cdot x_n + \gamma \cdot x_n^2 + \delta, \qquad n = 1,2,..., \tag{1}$$

where: n – discrete time;
x_n – n-th element of the sequence;
α, β, γ, δ – controlling parameters.

Agrees (1), anyone from this four parameters a, b, g, d can be calculated, if six adjacent elements of a digital sequence obtained with the help of this map are known.

In a series of classical special cases the best values of controlling parameters are known. At, α=0, β=4, γ = –4, δ=0 from (1) the Verhulst's map follows. For α=0.3, β=0, γ= –1.4, δ=1 from (1) the Henon's map is gained. If in (1) to put α=0, β= –1.57, γ=2, δ=0, will be received the map surveyed in [6].

For maps, in which α=0, δ=0 from (1) follows:

$$x_{n+1} = \beta \cdot x_n + \gamma \cdot x_n^2, \tag{2}$$

$$x_{n+2} = \beta \cdot x_{n+1} + \gamma \cdot x_{n+1}^2, \tag{3}$$

Then from (2), (3) will be received:

$$\gamma = \frac{B^2 - A \cdot C}{A \cdot B \cdot (A - B)}; \tag{4}$$

$$\beta = \frac{A^2 \cdot C - B^3}{A \cdot B \cdot (A - B)}, \tag{5}$$

where: $A=x_n$; $B=x_{n+1}$; $C=x_{n+2}$.

Agrees (4), (5), the generators controlling parameters of a similar type can be calculated by non-linear handling of three adjacent numbers of a sequence.

If at the receive side we know the generator's type and one of its parameters then for calculation of other parameter there are enough of two adjacent numbers. So, for a Verhulst's generator from (2) will be received:

For map surveyed in [6], from (2) follows:

$$\gamma = \frac{B - 4 \cdot A}{A^2}; \quad (6)$$

$$\beta = \frac{B + 4 \cdot A^2}{A}; \quad (7)$$

$$\gamma = \frac{B + 4 \cdot A^2}{A}; \quad (8)$$

For case β=0, γ=1 from (1) will be received:
where: $A=x_{n-1}$; $B=x_n$; $C=x_{n+1}$; $D=x_{n+2}$.

$$\alpha = \frac{B^2 \cdot (1 - D) - C^2 \cdot (1 - C)}{A \cdot C^2 - B^3}; \quad (10)$$

$$\gamma = \frac{B \cdot (1 - C) - A \cdot (1 - D)}{A \cdot C^2 - B^3}, \quad (11)$$

If the generator's type and one of the optimum parameters is known at the receive side, the amount of adjacent elements of the sequence, necessary for calculation, will decrease.

So, in case of a Henon's generator it is possible to receive the following formulas:

$$\alpha = \frac{1.4 \cdot B^2 + C - 1}{A}; \quad (12)$$

$$\gamma = \frac{C - 0.3 \cdot A - 1}{B^2}, \quad (13)$$

The factors, defining selection of pairs of commuted generators, are:

- amount of numbers of a sequence necessary for an information parameter evaluation;
- interval of numbers of a generated sequence;
- time expended on calculation for this algorithm;
- closeness of statistical performances of generated sequences.

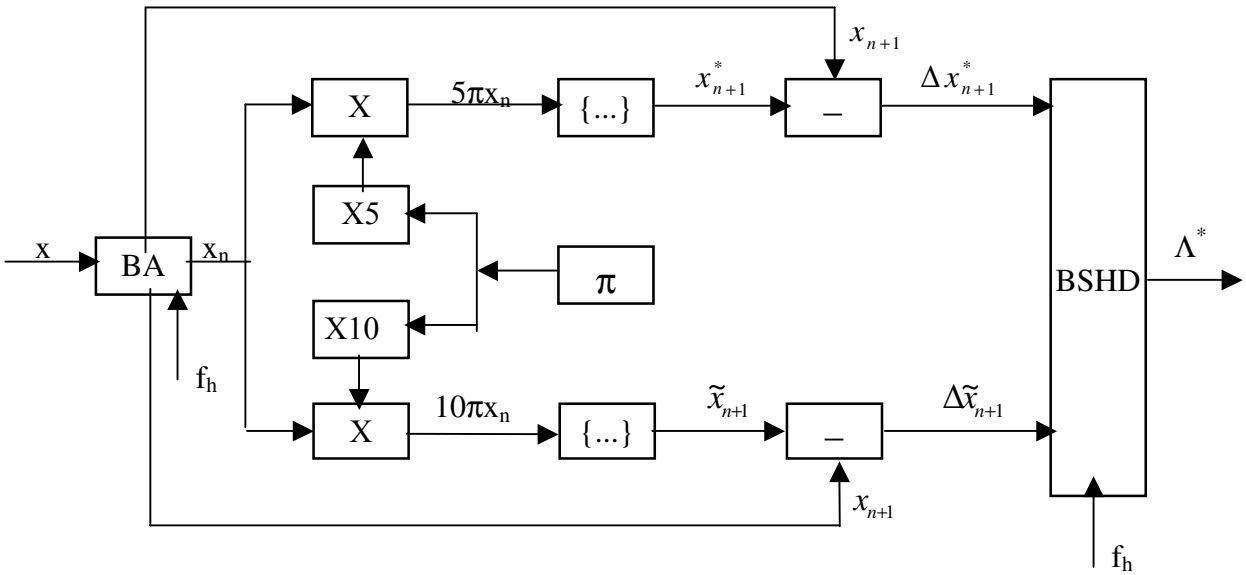

Fig. 1.

As a measure, defining fitness of a generator, it is possible to use unhook correlation time between the elements of sequences.

For example, for map of an aspect:

$$x_{n+1} = \{k \cdot x_n\}, \qquad n = 1,2,..., \quad (14)$$

where the sign {...} means a fractional part of argument, made in a bracket, and the controlling parameter k>1, the unhook correlation time τ is determined by expression:

$$\tau = \frac{1}{\ln k} \quad (15)$$

The sequence's elements for k>>1 can be considered statistically independent [1]. Agrees (14), the binary symbol should be transmitted by two numbers of the sequence. For example, at transmission of "zero" two numbers from a generator with k=5π are used, and at transmission of "unit" are transmitted numbers from a generator with k=10π. In the below considered example both generators are started simultaneously at an initial value x=0.1.

Let it is required to transmit the message Λ "0; 0; 0; 1; 1; 0; 1; 0". If the limiting round-off error of number is equal 0.0005, then in a line will arrive the sequence of numbers: "0.1; 0.571; 0.966; 0.175; 0.743; 0.673; 0.246; 0.719; 0.596; 0.710; 0.233; 0.665; 0.165; 0.186; 0.245; 0.849". The handling procedure of this sequence in the receiver is illustrated by the scheme in a fig. 1, where the following labels are accepted:

BA – buffer-accumulator;

BSHD – block of searching, handling and decisionmaking;

Δx^{*}_{n+1} an error of the 5π-channel;

$\Delta \tilde{x}_{n+1}$ an error of the 10π-channel;

Λ – obtained binary sequence;

f_h – choice frequency of pairs of numbers x_n and x_{n+1} (twice smaller then figures following frequency).

The valid message is considered in the channel where the error Δx_{n+1} is less. In a surveyed example the ratio of errors of false and true channels in the worst case exceeds 25 times.

The generated in similar way digital sequences can be also used in analogue systems, for example, in FM-generators with chaotic frequency of subcarrier oscillation.

Bibliography

1. Zaslavskii G.M. A statistical irreversibility in non-linear systems. - Moscow.: Science, 1970. - 144 p.

2. Belskii U.L., Dmitriev A.S. An information transfer with the use of determined chaos // Radioengineering and electronics, 1993, N.7. - p. 1310-1315.

3. Kuleshov V.N., Larionova M.V., Udalov N.N. A transfer information system with chaotic carrying // The Bulletin of MEI, 1997, N. 5. - p. 54-61.

4. Dmitriev A.S., Panas A.I., Starkov S.O. Dynamic chaos as paradigm of modern communication systems // The foreign radio electronics. Successes of a modern radio electronics, 1997, N. 10. - p. 4-26.

5. Kapranov M.V., Morozov A.G. The use of chaotic modulation for an information transfer // Radio engineering letters, 1998, N. 4. - p. 66-71.

6. Fundamentals of the vibration theory: Studies guiding / V.V. Migulin, V.I. Medvedev, E.R. Mustel, V.N. Parigin; edited by V.V. Migulin. - M.: Science, 1998. - 392 p.