PSEUDO-CHAOTIC SEQUENCES GENERATED USING INTEGER-NUMBER ITERATIONS

Vladimír ŠEBESTA, Jaromír KOLOUCH
Institute of Radio Electronics
Brno University of Technology
Purkyňova 118, 612 00 Brno
Czech Republic

Abstract

A proposed system generates a pseudo-chaotic sequence using integer-number look-up-table (LUT). The current output of LUT is used as LUT input address in the next step. The generated sequence approximates or simulates a chaotic sequence. The main facility of the method is high speed of the generating; the main drawback is bounded length of the non-periodic part of the pseudo-chaotic sequence.

Keywords

Chaos, sequence generation, digital chaos

1. Introduction

The aim of the research was to develop a fast near-to-chaotic generator. The integer-number generator was chosen for study. This brings two advantages:

1. The generator works fast.
2. It can be realised identically using many different software and hardware tools.

Such properties can be useful in communications applications.

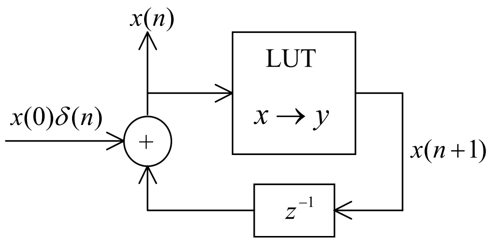

Fig. 1 Pseudo-chaotic generator.

The analysed structure of the pseudo-chaotic (PCH) generator is drawn in Fig. 1. The symbol $x(n)$ denotes an element of the PCH sequence in current time n, $x(n+1)$ is the next value of the sequence, $x \rightarrow y$ denotes PCH mapping realised via LUT and $x(0)$ is the initial value of the sequence. Zero state of the memory element z^{-1} is assumed in the instant $n = 0$. The LUT is filled up by integer numbers. The numbers has been obtained using quantisation and scaling of the results of chaotic mapping.

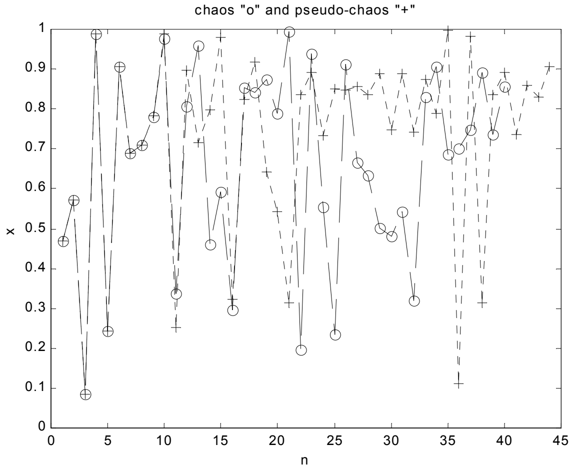

Fig. 2 Chaos and pseudo-chaos.

The set $\{x(n)\}$ used during chaotic mapping consist of all integer numbers from the interval <1, N>, where N is maximum value of $x(n)$. Each number x is normalised as

$$x_{\text{nor}} = (x - 0.5) / N \, . \tag{1}$$

Then, using chaotic map, normalised number y_{nor} is determined. After that, integer number y is calculated as follows

$$y = \text{round}(N y_{\text{nor}} + 0.5) \, , \tag{2}$$

the round(.) function rounds to the nearest integer from the interval <1, N>.

2. Theory

There are two desired properties of the PCH sequence:

1. Long sequence without repetition.
2. Different sequences for different initial value $x(0)$.

A state diagram of the PCH generator is a useful tool for finding fundamental properties of the generator from this aspect. An example of state diagram is shown in Fig. 3 for N = 16. The states are denoted by integer numbers x. Sequence of the integer numbers x creates the integer-number PCH signal. All possible initial values $x(0)$ are inscribed in squares. Consequent states are put down in circles.

An analysis of the state diagrams leads to the further conclusions. Typically, the sequence consists of non-periodic or transient part and periodic sequence. Existence of the sequences without transient part is possible. Periodic sequence closes every sequence.

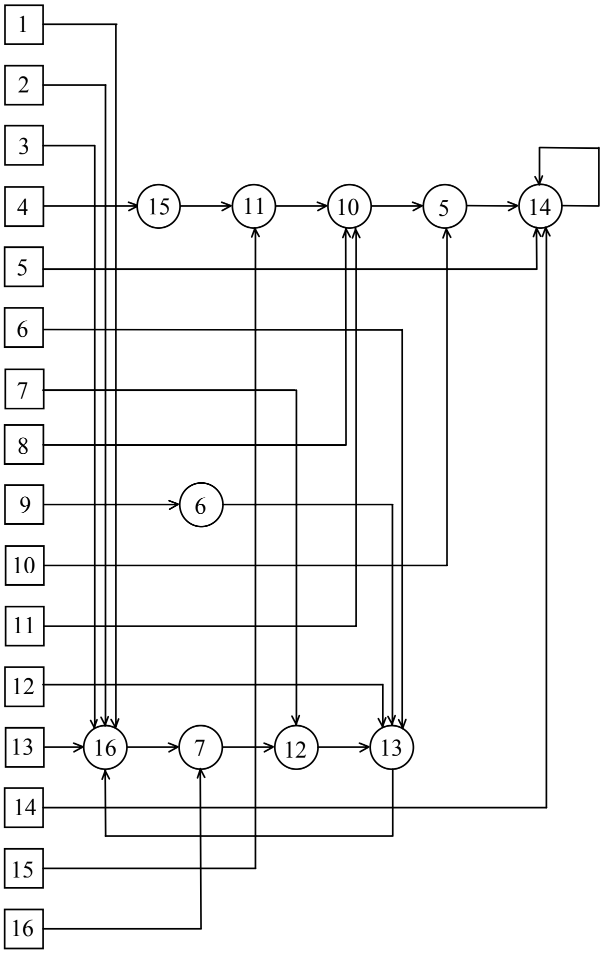

Fig. 3 State diagram of the PCH generator.

Theorem 1. Let $x_A(0)$ is an initial value of the sequence $x_A(n)$ and $x_B(0) \neq x_A(0)$ is an initial value of the sequence $x_B(n)$. Suppose, L_A and L_B denote lengths of the periods in periodic parts of $x_A(n)$ and $x_B(n)$ respectively. If $L_A \neq L_B$, then numbers in the periodic part of $x_A(n)$ and numbers in the periodic part of $x_B(n)$ are different.

Theorem 2. If any number from the periodic part of the sequence $x_A(n)$ is equal to some number from the periodic part of the sequence $x_B(n)$, then periodic parts of the both sequences contain the same numbers.

Theorem 3. If an element of the periodic part of the sequence $x_A(n)$ exists which is different from all elements of the periodic part of $x_B(n)$ then transient parts of sequences $x_A(n)$ and $x_B(n)$ are different.

Next theorem is a consequence of the theorems 1, 3.

Theorem 4. Number of the quite different transient parts is equal or greater than number of different lengths of the periods.

The number of possible states for $n \geq 1$ is mostly less than the number N of possible initial states $n(0)$. The reached lengths of the transients are proportional to the total number of possible states for $n \geq 1$.

3. Computer experiment

Examples of the chaotic and normalised pseudo-chaotic sequences are shown in the Fig. 2. The first 9 samples of the sequences are almost identical. Next parts of the sequences show similar behaviour. Number of possible initial states $N = 2^{18}$ has been used.

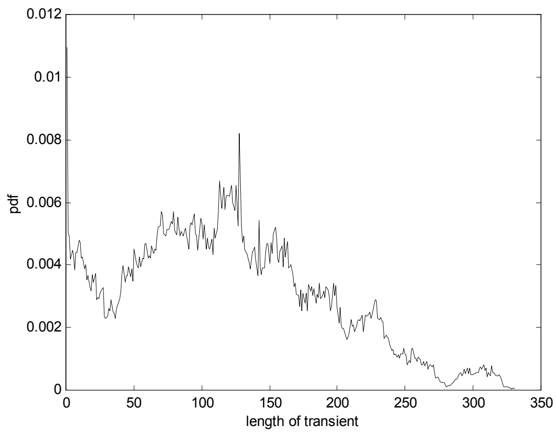

Fig. 4 The distribution of the lengths of the transients.

Fig. 4 shows the probability density function of the lengths of the transient. Number of possible initial states $N = 2^{16}$ has been used in this case.

Fig. 5 shows the maximum lengths of the transient and of the period as a function of the number of bits b in the binary expression of the state number, $b = \log_2 N$. In our experiment, the total number of possible states for $n \geq 1$ is approximately 58 % of the N.

The prototype from [1] was used. It is based on recurrent using of the three-step map as follows.

1. The first non-linear map $y = x^2$.
2. The piecewise linear map.
3. The inverse non-linear map $y = x^{1/2}$.

4. Conclusion

Pseudo-chaotic sequences have properties less or more close to the properties of the prototype discrete chaotic signal. Practical reasons leads to limitation of LUT size and consequently to the limited lengths of the transients and limited number of the different transients.

Chaotic behaviour of the PCH sequence can be supported via careful choice of the generator parameters and choice a type and parameters of chaotic prototype. The four founded theorems make the choice easier.

The advantage of the analysed PCH generator is relatively high rate, which is necessary in possible applications in modern communications systems.

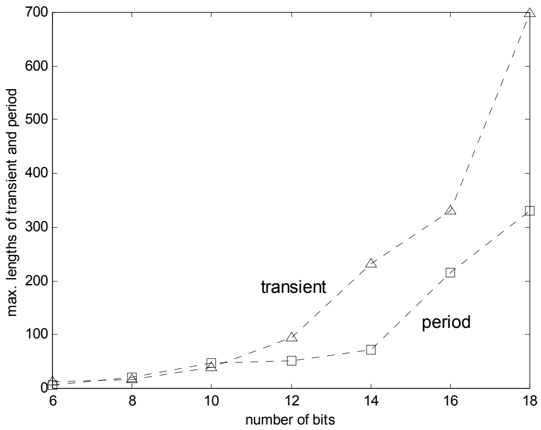

Fig. 5 The largest reached lengths of the transient and of the period.

Acknowledgment

This research is supported by the Grant Agency of the Czech Republic – Grant No. 102/99/0203 and Research program No. CEZ: J22/98:262200011.

References

[1] SANG, T., WANG. R., YAN, Y. Constructing Chaotic Discrete Sequences for Digital Communications Based on Correlation Analysis. IEEE Transactions on Signal Processing. 2000, vol. 48, no. 9, p. 2557-2565.

[2] WANG, S., YIP, P. C., LEUNG, H. Estimating Initial Conditions of Noisy Chaotic signals Generated by Piece-Wise Linear Markov Maps Using Itineraties. IEEE Transactions on Signal Processing. 1999, vol. 47, no. 12, p. 3289-3302.

[3] ISABELLE, S., WORNEL, G. Statistical analysis and spectral estimation techniques for 1D chaotic maps. IEEE Trans. on Signal Processing. 1994, vol. 45, p. 1524-1527.

[4] ZHOU, L. H., FENG, Z. J. A New Idea of Using One-Dimensional PWL Map in Digital Secure Communications - Dual-Resolution Approach. IEEE Transactions on Circuits and Systems - II: Analog and Digital Signal Processing. 2000, vol. 47, p. 1107-1111.

About authors...

Vladimír ŠEBESTA was born in Předín, Czech Republic, in 1938. Currently, he is a Professor with the Brno University of Technology, Czech Republic. Prof. Šebesta is a Member of the IEEE.

Jaromír KOLOUCH was born in Brno, Czech Republic, in 1945. Currently, he is an Associated Professor with the Institute of Radio Electronics, Brno University of Technology, Czech Republic.