Nonlinear Dynamics of PN-Sequences

Alexander L. Baranovski[1], Frank Dachselt[2] and Wolfgang Rave[3]

[1]Insitut Royal Météorologique de Belgique, Bruxelles Belgium

[2]Institut für Grundlagen der Elektrotechnik und Elektronik, Technische Universität Dresden, Dresden Germany

[3]Vodafone Stiftungslehrstuhl Mobile Nachrichtensysteme, Technische Universität Dresden, Dresden Germany

***Abstract*— This paper demonstrates a generation method for δ-correlated integer-valued sequences using modified linear feedback shift registers. We start from the well-known fact that *M*-sequence generation by conventional linear feedback shift registers approximates the Bernoulli map. Changing the next state map in such a way that it approximates the tent map, leads to sequences with nearly two-valued autocorrelation functions. The proposed method can be extended to the approximation of arbitrary maps in order to generate sequences with given autocorrelation properties.**

I. Introduction

Pseudorandom (PR) sequences or pseudo noise (PN) sequences are the best known class of digital sequences. The interest in pseudorandom sequences and their applications began to emerge in the 1950s [1]. PR sequences have found various applications in civil and military fields, for example, in radar and synchronization systems, channel estimation, crypto-graphy, system identification, test, measurement, as the basis of the noise generators, etc. Nowadays, they are widely used for practical application in modern cellular communication systems.

Digital sequences have been classified under three main categories [1]: binary, non-binary and other types.

The category of binary sequences can be taken as the most frequently used class of sequences.

Non-binary sequences became practical implementations by embedding in powerful digital signal processing devices. In many aspects, they possess properties, which are superior to those of binary sequences, with quaternary sequences being a typical case [1].

The third category of other types includes sequences, which have been considered to meet specific application requirements. For example, for image processing systems, as radar and pulse compression waveforms, in frequency-hopping spread-spectrum systems etc.

We will distinguish two most important application areas of PR sequences:

1. Applications requiring specified autocorrelation properties;
2. Applications requiring sets of sequences with specified cross-correlation properties.

In terms of communication systems, sequences with specified autocorrelation properties conform to synchronization tasks. In general, there are three synchronization problems: carrier, symbol, and frame synchronization [1]. It is common in practice to use a transmission preamble to generate the required timing reference point for a data frame. The preamble sequence, which is used for this purpose, has to be detected by means of a matched filter.

II. Binary PN Sequences

Pseudorandom or pseudo noise sequences are used in data scrambling as well as for spread-spectrum modulation. Data scrambling is achieved by changing the data sequence "randomly" before transmission. At the receiver, the scrambled sequence is "changed back" to the original data sequence. The two concepts, "randomness" and "changed back", are the key ideas involved in understanding CDMA techniques. Two fundamental requirements on a random sequence, or more precisely, a pseudo-random sequence, are the following [2]

- It must be reproducible at the receiver;
- It must be reproduced in synchronism with the scrambling sequence at the transmitter.

As a matter of principle the following general definition of "pseudo" randomness is possible: A deterministic signal is called a pseudorandom signal, if there is sufficient similarity between its properties and given parameters of the random signal. But, upon closer inspection, they can be shown to have certain regularities.

The following three properties or randomness criteria are correct especially for a binary sequence that is qualified as a pseudorandom sequence:

1. *The balance property*. In a complete period of a PN sequence, the number of 1s differs from the number of 0s by at most 1.
2. *The run property*. There are $(2^n - 1 + 1)/2 = 2^{n-1}$ runs consecutive 1s or 0s, and half of the runs are of length 1, $1/2^2$ of the runs are of length 2, $1/2^3$ of the runs are of length 3, etc.

Corresponding author address: Dr. A. L. Baranovski, Institut Royal Météorologique de Belgique, 3 Avénue Circulaire, 1180 Bruxelles Belgium; e-mail : Aleksander.Baranovsky@oma.be. He was with the Vodafone Chair at Dresden University of Technology during the preparation of this work.

3. *The correlation property*. If a complete sequence is compared with any shift of the sequence, the number of agreements minus the number of disagreements is always -1, i.e. the periodic autocorrelation function is two-valued.

The most important method of generating pseudorandom binary sequences is by means of a linear feedback shift register (LFSR). The output sequence of an LFSR sequence generator with *m* stages will always be periodic. An output sequence of shift register with maximal period $N = 2^m-1$ is called a maximal length sequence or *M-sequence*.

M-sequences satisfy all three required randomness properties. A primitive polynomial $p(x)=x^m + p_{m-1}x^{m-1} + p_{m-2}x^{m-2} + \cdots + p_1 x + 1$ of degree m is needed as a basis to construct an M-sequence. The sum is calculated modulo-two, i.e. the polynomial is calculated over GF(2) and all p_i take values of either 0 or 1.

The operation of an LFSR can be described by a dynamic matrix equation:

$$\bar{y}_{n+1} = B\,\bar{y}_n, \qquad (1)$$

where the vector $\bar{y}_n = \left(y_{n,0}\ y_{n,1} \ldots y_{n,m-1}\right)^T$ is the state of the LFSR at time *n*, ***B*** is a transition matrix such that

$$B = \begin{pmatrix} p_{m-1} & p_{m-2} & \cdots & p_1 & 1 \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ldots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix} \qquad (2)$$

The output of the shift register is $y_{n,m-1}$. In other words, the LFSR generates an infinite sequence $\{y_{n,m-1},\ n = 0,1,2,...\}$. In order to generate an M-sequence, an initial loading $\bar{y}_0 \neq 0$ has to be specified.

III. Non-Binary Sequences

For the generation of discrete non-binary sequences we introduce the transformation

$$z_n = \sum_{i=0}^{m-1} \alpha_i y_{n,i}, \qquad (3)$$

where α_i are some weighting coefficients. It is clear that the statistical properties of the sequence $\{z_n, n = 0,1,2,...\}$ depend on the coefficients and properties of the M-sequence.

We study the special case with $\alpha_i = 2^i$. Then (3) gives the binary expansion of the decimal number z_n which takes values from the set $Z = \{0,1,2,...,2^m - 1\}$.

Taking into account (1) and (2), an arbitrary primitive polynomial *p(x)* defines a unique permutation of elements in *Z*. Let us take, for example, two primitive polynomials $p_1(x) = x^4 + x^3 + 1$ and $p_2(x) = x^4 + x + 1$ with $m = 4$. Using (2) we easily get two matrices B_1 and B_2 and calculate vector-states of the LFSRs by (1). Then the filtering (3) forms the following sequences:

$Z_1 = \{z_n^{(1)}, n = 0,1,...,15\} \equiv \{1,3,7,15,14,13,10,5,11,6,12,9,2,4,8\}$

$Z_2 = \{z_n^{(2)}, n = 0,1,...,15\} \equiv \{1,2,4,9,3,6,13,10,5,11,7,15,14,12,8\}$

respectively.

We note that $\{z_n^{(i)}\}$ are one dimensional processes, the lag one or next state plots of $(z_n^{(i)}, z_{n+1}^{(i)})$ are given in Fig. 1 and Fig. 2, respectively.

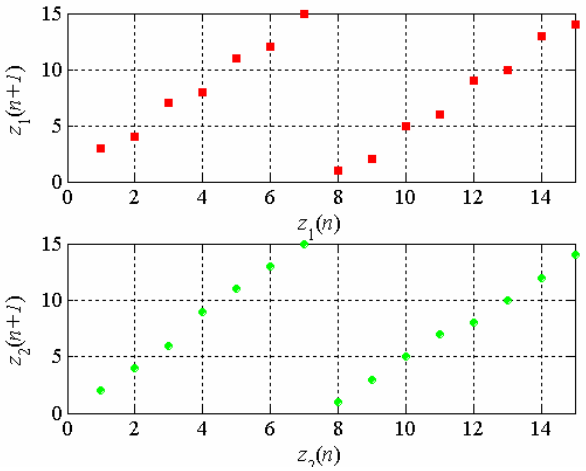

Fig. 1. Next state plots of decimal sequences $z_n^{(1)}$ and $z_n^{(2)}$.

The plots demonstrate that there is a first order map linking successive values. It holds true for arbitrary primitive polynomials *p(x)*. We demonstrate this map for the polynomial $p(x) = x^{18} + x^7 + 1$ which is used in the downlink scrambling code generator of the 3GPP standard [3]:

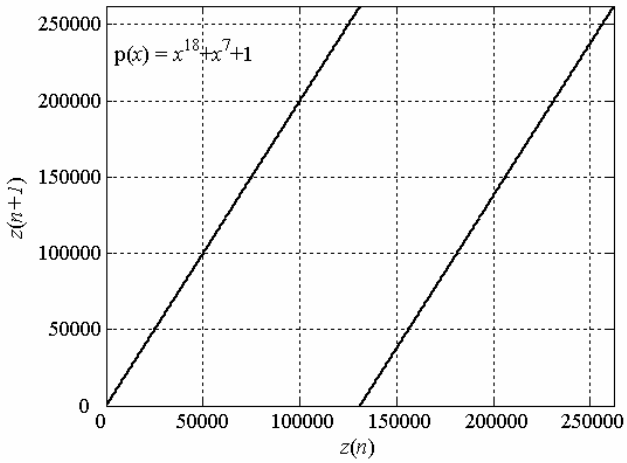

Fig. 2. Next state plot of values z_n for $p(x) = x^{18} + x^7 + 1$.

We note that the plotted map being rescaled to the unit interval for the asymptotic case $m \to \infty$ gives the Bernoulli shift map

$$z_{n+1} = 2z_n \mod 1 \qquad (4)$$

This mapping has been carefully investigated in the field of chaos theory [4], ergodic theory and information theory [6].

This map is characterized by an uniform invariant probabilistic measure (i.e. z_n is uniformly distributed over the unit inter-val) and exponentially decaying autocorrelation function [5]:

$$c_z(n) = \frac{1}{12} 2^{-n} \tag{5}$$

An idea to use chaotic maps for a generation of the digital sequences with prescribed statistical properties has been firstly discussed in [7] and a plenty of the important results on this topic have been already presented in [e.g. 8,9,10] . Here we continue to develop this idea.

Fig. 3 shows the normalized autocorrelation function of a decimal M-sequence which is numerically obtained for m = 18.

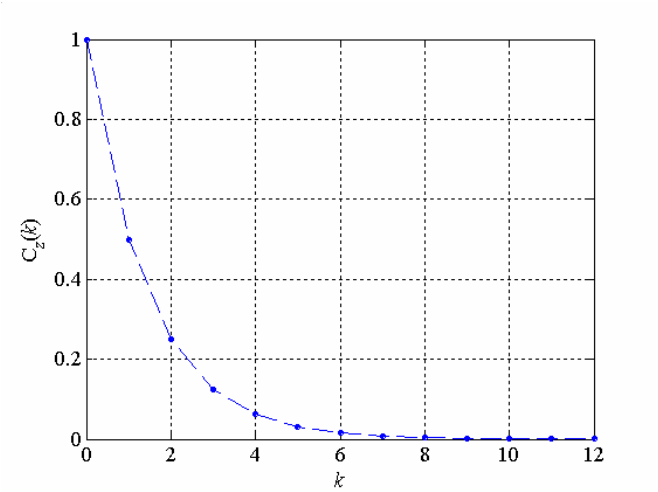

Fig. 3. Autocorrelation function $C_z(k)$ for small values of k.

Thus we establish that the filtering (3) of a binary M-sequence produces a uniformly distributed decimal M-sequence with exponentially decaying autocorrelation function:

$$\lim_{m\to\infty} C_z(k) = \begin{cases} 1, & k = 0, 2^m - 1, 2^{m+1} - 2, \ldots \\ 2^{-k}, & \text{otherwise} \end{cases}$$

IV. Approximation of arbitrary Next State Maps

For different application reasons we define the following problem: how can a known binary M-sequence generation scheme be modified in order to provide δ-correlation of decimal M-sequences.

For this purpose we introduce a vector $\overline{x}_n = \left(x_{n,0}\ x_{n,1} \ldots x_{n,N}\right)^T$ such that $x_{n,i} = \begin{cases} 0, & if\ i \neq z_n \\ 1, & if\ i = z_n \end{cases}$, i.e. $z_n \equiv \sum_{i=0}^{N} i \cdot x_{n,i}$.

Then $\overline{x}_n$ is the decimal position code of the integer z_n.

Then for any dynamical system (1) with a transition matrix B a new dynamical system

$$\overline{x}_{n+1} = A\,\overline{x}_n \tag{6}$$

can be derived. Matrix A has dimension $2^m \times 2^m$ and can be easily constructed from the next state plot of successive values of z_n as shown in Fig. 2. This is done by filling the matrix A with ones at those positions where a point in the next state map occurs and with zeros at the remaining positions.

$$A = \begin{pmatrix}
0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0 & 15\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1} & 14\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0 & 13\\
0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0 & 12\\
0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0 & 11\\
0&0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0 & 10\\
0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0 & 9\\
0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0 & 8\\
0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0 & 7\\
0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0 & 6\\
0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0 & 5\\
0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0&0 & 4\\
0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0&0&0 & 3\\
0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0 & 2\\
0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0 & 1\\
\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 & 0
\end{pmatrix}$$

In terms of the theory of dynamical systems (1) and (6) are topologically equivalent. A homeomorphism conjugated to these dynamical systems is given by the $m \times 2^m$ matrix whose rows are the consecutive m *Rademacher* sequences. So, for m = 4 this matrix is

$$C = \begin{pmatrix}
0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \\
0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\
0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \\
0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1
\end{pmatrix}.$$

In other words, the iterates of both dynamical systems (1) and (6) are related for all n through:

$$\overline{y}_n = C\,\overline{x}_n \tag{7}$$

From this we derive the relationships

$$\overline{y}_{n+1} = B \cdot \overline{y}_n = B \cdot C \cdot \overline{x}_n$$
$$\overline{y}_{n+1} = C \cdot \overline{x}_{n+1} = C \cdot A \cdot \overline{x}_n$$

finally leading to an equation

$$B \cdot C = C \cdot A \tag{8}$$

It allows us in principle to construct either matrix A for a given B or otherwise matrix B for a given A.

From the theory of chaotic maps it is known that for example the tent map

$$z_{n+1} = \begin{cases} 2z_n & 0 \le z_n < 0.5 \\ 2(1 - z_n) & 0.5 \le z_n \le 1 \end{cases} \tag{9}$$

is an ideal generator of δ-correlated real-valued sequences. We expect this property for a decimal M-sequence generator based on a triangular type of matrix A.

Let us show this for m = 4. We fix a "tent" like matrix A

$$A = \begin{pmatrix}
0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0 & 15\\
0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0 & 14\\
0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0 & 13\\
0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0 & 12\\
0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0 & 11\\
0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0 & 10\\
0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0 & 9\\
0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0 & 8\\
0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0 & 7\\
0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0 & 6\\
0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0&0 & 5\\
0&0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0 & 4\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0 & 3\\
0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0&0&0 & 2\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1} & 1\\
\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 & 0
\end{pmatrix}$$

which defines the following sequence given in Fig. 4:

$$Z=\{z_n, n=1,...,15\}\equiv\{1,2,5,10,11,9,12,6,13,4,8,14,3,7,15\}$$

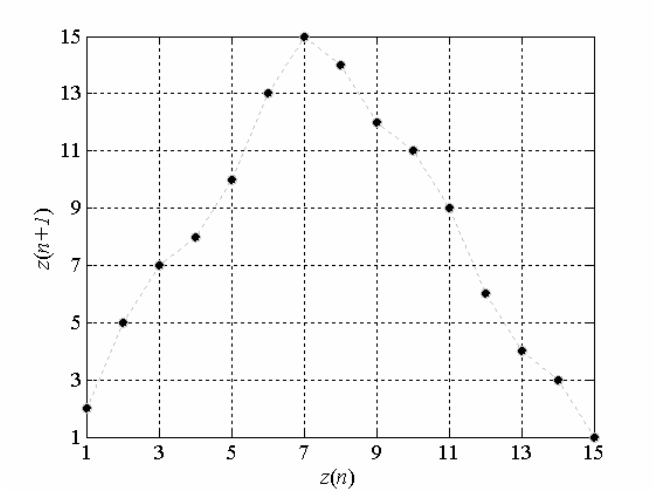

Fig. 4. Approximation to the tent map by a decimal-valued sequence *Z*.

Then matrix *B* can be computed from (8) as

$$B=\begin{pmatrix}0&1&0&0\\1&0&0&1\\0&1&0&1\\0&0&1&1\end{pmatrix}, \tag{10}$$

which defines a new scheme for the LFSR.

For an arbitrary *m* the approach can be extended and then the transition matrix *B* which approximates the tent map can be written in the following form

$$B=\begin{pmatrix}b_{1,1}&b_{1,2}&\dots&b_{1,m-1}&b_{1,m}\\1&0&\dots&0&1\\0&1&\dots&0&1\\\vdots&\vdots&\dots&\vdots&\vdots\\0&0&\dots&1&1\end{pmatrix}, \tag{11}$$

In order to ensure the generation of an M-sequence the characteristic polynomial of *B* given by

$$\begin{aligned}\det(B+x\cdot I)=&\,x^m+(1+b_{1,1})x^{m-1}+(1+b_{1,1}+b_{1,2})x^{m-2}\\&+\dots\\&+(1+b_{1,1}+b_{1,2}+\dots+b_{1,m-1})x\\&+(b_{1,1}+b_{1,2}+\dots+b_{1,m-1}+b_{1,m})\end{aligned} \tag{12}$$

with *I* being the identity matrix, has to be a primitive polynomial of degree *m* [11]. Comparing the polynomial (12) to a primitive polynomial $p(x)$ leads to an equation system for the coefficients of the first row of matrix *B*:

$$\begin{aligned}b_{1,1}&=p_{m-1}+1\\b_{1,2}&=p_{m-2}+p_{m-1}\\b_{1,3}&=p_{m-3}+p_{m-2}\\&\vdots\\b_{1,m-1}&=p_1+p_2\\b_{1,m}&=p_1\end{aligned} \tag{13}$$

We illustrate this method for the previously mentioned primitive polynomial $p(x)=x^{18}+x^7+1$ used for scrambling in UMTS. From (13) we get $b_{1,1}=b_{1,11}=b_{1,12}=1$ and all other $b_{1,i}=0$. Then (1) defines a new dynamic equation for the states of an LFSR and (3) generates a sequence of decimal valuess $Z=\{z_n, n=0,1,...,262143\}$ with the next state plot of their successive values (z_n, z_{n+1}) shown in figure 5.

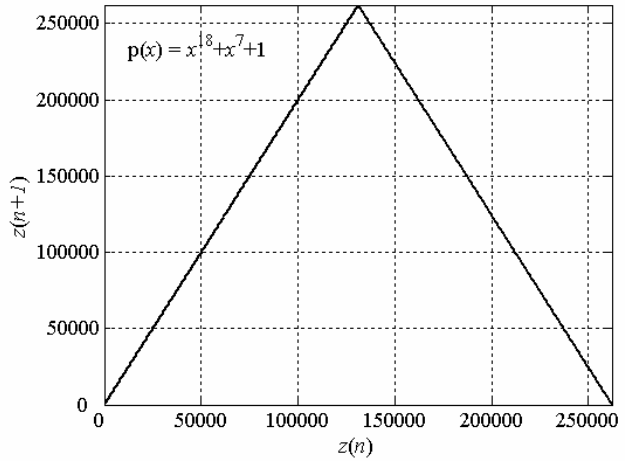

Fig. 5. Next state plot of the approximated tent map for polynomial degree *m* = 18.

A normalized autocorrelation function from a computational experiment is depicted in Fig. 6

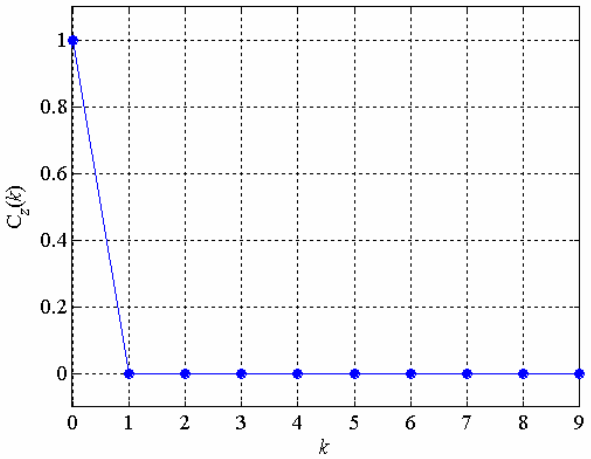

Fig. 6. Autocorrelation sequence of the M-sequence generated by the map in Fig. 5.

For an increasing number of stages of the modified shift register, the approximation of the tent map becomes closer to the continuous-valued case and thus also the statistical properties of the generated integer sequences converge to those of their continuous-valued counterparts. Using the periodicity of decimal M-sequences the normalized auto-correlation function in the asymptotic case $m\to\infty$ can be written as

$$C_z(k) = \begin{cases} 1, & k = 0, 2^m - 1, 2^{m+1} - 2, \ldots \\ 0, & \text{otherwise} \end{cases} .$$

V. Generalization aspects

For arbitrary nonlinear one-dimensional maps generating *m*-bit decimal numbers there exist

$$N_P = \left(2^m - 1\right)! = N!$$

different possible m-sequences. For a consistent comparison the all-zero state is excluded from the sequence. Thus, the number N_P represents all permutations of the numbers 1, …, *N*.

If the generation method is restricted to the linear scheme (1) than the number of possible m-sequences is reduced. There exist [12]

$$N_L = \prod_{i=0}^{m-1} \left(2^m - 2^i\right)$$

different regular, i.e. invertible, binary $m \times m$ matrices over GF(2). Each matrix *B*, which generates an M-sequence, is regular and can be conjugated with an arbitrary regular matrix *R* into a new matrix [12]

$$\tilde{B} = R^{-1} \cdot B \cdot R$$

which again generates an M-sequence. Since all regular matrices *B* can be conjugated to each other, N_L is also the number of different m-sequences which can be generated by the linear equation (1).

The reduced number of possible m-sequences in the linear case makes it difficult to construct the position code matrices A for the approximation of arbitrary maps. While it is still feasible to construct a matrix *A* for a nonlinear generation scheme, the additional conditions for such a matrix *A* which guarantee the existence of a matrix *B* by equation (8) are still unknown.

VI. Conclusion

A method to obtain transition matrices for the recursive generation of integer sequences with desired autocorrelation properties is proposed. Using the approximation of certain next state maps allows to exploit the known properties of continuous-value sequences. The paper has demonstrated this method using the well-known tent map in order to generate δ-correlated sequences. Further consideration is necessary in order to extend the shown approach for the approximation of arbitrary continuous maps.

VII. Acknowledgments

A.L.B. is grateful to G. Fettweis for his interest in the work, I. Tarasov, and I. H. Dinwoodie for useful discussion during the Extended Workshop on Pseudorandom Number Generation in Montreal, 1996, and also acknowledge financial support from the Vodafone Chair at Dresden University of Technology in carrying out this work.

References

[1] Fan, Pingzhi; Darnell, Michael: *Sequence Design for Communications Applications*. – Research Studies Press LTD., 1996.

[2] Lee, Johng S.; Miller, Leonard E.: *CDMA systems engineering handbook*. – Boston-London: Artech House, 1998.

[3] 3GPP, Technical Specification Group (TSG) RAN WG4, "*Spreading and Modulation (FDD)*", TS 25.213 v5.3.0 (2003-03).

[4] Lasota, A., Mackey M, *Probabilistic Description of Deterministic Systems*, Cambridge Univ. Press, 1985

[5] A. L. Baranovski, D. Daems (1995). *Design of 1-D chaotic maps with prescribed statistical properties*. Int. Journal of Bifurcations and Chaos, 5, N 6, 1585-1598.

[6] P. Billinsley: *Ergodic Theory and Information*. –John Wiley & Sons, Inc. 1965.

[7] Yu.K.Rybin, A.L.Baranovski and A.M. Nosov *Design of the digital sequences generators with standardized metrological characteristics,* In Proceedings of the All-Union Conference on Automation of Means of Metrological Maintenance of a National Economy, pages 292-299, Tbilisi, 1989 (in Russian).

[8] T. Kilias (1994). Generation of pseudo-chaotic sequences. Int. Journal of Bifurcations and Chaos, 4, N 3, 709-713.

[9] Yoshioka D., Tsuneda A., Inoue T., *Equivalence of Periodic Sequences Generated by Bernoulli And Tent Maps with Finite Bits*, Int. Symp. On Nonlinear Theory and its Applications, Fukuoka 2004

[10] R. Rovatti, G. Mazzini, and G. Setti, "On the ultimate limits of chaos-based asynchronous DS-CDMA – I: basic definitions and results," *IEEE Trans. Circuits Syst. I,* vol. 51, pp. 1336-1347, July 2004.

[11] Golomb S. W., *Shift Register Sequences*, Aegean Park Press, 1982.

[12] Frank Dachselt: Modified linear feedback shift registers. Student project, Technische Universitaet Dresden, 1994 (in German).