2005 International Symposium on Nonlinear
Theory and its Applications (NOLTA2005)
Bruges, Belgium, October 18-21, 2005

On Generation of Chaotic *M*-Sequences

Alexander L. Baranovski
Royal Meteorological Institute of Belgium,
Av. Circulaire 3, 1180 Brussels, Belgium,
Email: Alexander.Baranovsky@oma.be

Abstract– This paper deals with the linear generation methods of binary and decimal-valued maximal-length sequences. We show their topological equivalence, provide necessary and sufficient conditions for that and find a matrix-homeomorphism whose rows are the consecutive *Rademacher* sequences. We investigate a number of maximal linear sequences and give its formula. We demonstrate different patterns generated from the sequences, classify them and especially focus on ones whose shapes are similar to chaotic real-valued maps. It gives us an opportunity to establish a similarity in the statistical characteristics of both *m*-bit decimal integer and chaotic real-valued sequences on the one hand and design a *m*-sequence generator with given autocorrelation properties on the other one.

1. Introduction

The theory of maximal-length sequences is well and more developed for binary ones as they are more commonly used in communications and related engineering applications than non-binary sequences. A modern statistical theory of chaotic dynamical systems can reduce this theoretical lack and show potentially considerable practical importance of this. In [1] authors realize a concept of the utilization of chaotic sequences with finite bits by means of a nonlinear feedback shift register and demonstrate that the maximal-period sequences can be generated by properly quantized chaotic maps. A necessary condition for that is one-to-one mapping. At the same time the sufficient conditions have not been obtained.

A work [2] gives a *m*-word-length approximation to a tent map and shows topological equivalence of *M*-sequence of *m*-bit decimal integers and its conjugated binary *m*-sequence. In this paper we extend this approach and indicate the necessary and sufficient conditions for generation of decimal *m*-sequences. We also investigate a number of maximal linear sequences and study their auto- and cross- correlation properties. On this base we describe an algorithmic approach how to design a decimal *m*-sequence with prescribed autocorrelation function (acf).

2. Topological Equivalence of Binary and Decimal Integer M-Sequences Generators

We start from a linear generation method of binary sequences based on the following dynamic matrix equation:

$$\bar{y}_{n+1} = B\,\bar{y}_n\,, \tag{1}$$

where $\bar{y}_n = \left(y_{n,0}\ y_{n,1}\dots y_{n,m-1}\right)^T$ is the state vector at time n, B is a transition binary matrix ($b_{i,j}$).
It is known that if a characteristic polynomial of B

$$p(x) = x^m + p_{m-1}\,x^{m-1} + \dots + p_1\,x + p_0 \tag{2}$$

is primitive, the system (1) generates a *m*-sequence $\{\,y_{n,m-1},\ n = 0,1,2,\dots\,\}$ with a maximal period $N = 2^m-1$.
A linear feedback shift register (LFSR) with a matrix

$$B = \begin{pmatrix} p_{m-1} & p_{m-2} & \cdots p_1 & 1 \\ 1 & 0 & \dots 0 & 0 \\ 0 & 1 & \dots 0 & 0 \\ \vdots & \vdots & \dots \vdots & \vdots \\ 0 & 0 & \dots\ 1 & 0 \end{pmatrix} \tag{3}$$

is the most studied case [e.g. 3]of a system (1) .
From a binary *m*-sequence with an initial loading $\bar{y}_0 \neq 0$ we construct a *m*-sequence of *m*-bit decimal numbers by the transformation

$$z_n = \sum_{i=0}^{m-1} 2^i\, y_{n,i}\,. \tag{4}$$

Then (4) gives the binary expansion of the decimal number z_n which takes values from the set Z={1,2,…, 2^m-1}. It is clear that an arbitrary B having a primitive characteristic polynomial $p(x)$ defines a unique permutation of elements in Z . We define N_M as the number of all these possible permutations and continue the analysis of the number of *m*-sequences in a section 3.
Here we introduce a vector $\bar{x}_n = \left(x_{n,0}\ x_{n,1}\dots x_{n,N}\right)^T$ such that $x_{n,i} = \begin{cases} 0, & if\ i \neq z_n \\ 1, & if\ i = z_n \end{cases}$, i.e. $z_n \equiv \sum_{i=0}^{N} i \cdot x_{n,i}$. $\bar{x}_n$ is the decimal position code of the integer z_n. Then for any dynamical system (1) with a primitive characteristic polynomial a new dynamical system

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

can be derived.
Matrix $A = (a_{i,j})$ has dimension 2^m x 2^m and contains units along the trajectory of the *m*-sequence Z_M ={z_1, z_2,…, z_N}, where z_n are calculated by (4):

$$a_{1,1} = 1,\ \ a_{z_{n+1}+1,\, z_n+1} = 1,\ \ n = 1,2,\dots,2^m - 1 \tag{7}$$

and with zeros at the remaining positions. We call this procedure as a quantizing of a map.
It means that this matrix looks like the turned next state plot (a map) of successive values of z_n as shown in Table 1.

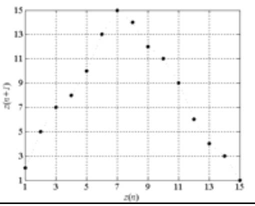
a map of *m*-sequence	matrix *A*
	$\begin{pmatrix} 1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1 \\ 0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0 \\ 0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0 \\ 0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0 \end{pmatrix}$

Table 1. Tent map of a *m*-sequence Z_M (m=4) and its transition matrix

Now we are able to collect some properties of matrix *A*:

$$a_{i,i} = 0, \forall i > 1; \sum_{i=1}^{N+1} a_{i,j} = \sum_{j=1}^{N+1} a_{i,j} = 1 \ \forall i,j; \ rank(A) = 2^m \quad (8)$$

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 x 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:

$$\overline{y}_n = C\,\overline{x}_n \quad (9)$$

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

$$B \cdot C = C \cdot A \quad (10)$$

It allows us to construct either matrix *A* for a given *B* or otherwise matrix *B* for a given *A*. A Moore-Penrose matrix inverse method fails here since the matrices in (10) are not real-valued but binary ones with modulo 2 addition. We develop a new method for this case.

A way from *B* to *A* (necessity) can be now specified: the equations (4) and (7) with properties (8) define an unique matrix *A*. An inverse way from given *A* to *B* (sufficiency) being linked to the design problem of decimal-valued *m*-sequences with given autocorrelations will be derived in section 4.

2.1. Patterns generated by *M*-sequences

M-sequences form patterns on a plane (z_n , z_{n+1}) and some of them can be described by quantized chaotic maps. We demonstrate these cases by two examples.

Example 1. Fractal-like pattern. Consider a matrix

$$\mathbf{B}= \begin{pmatrix} 1&1&0&0&0&1&1&0&0&1&0&0&1 \\ 1&1&0&0&0&0&0&0&0&0&0&0&0 \\ 1&1&1&0&0&0&0&0&0&0&0&0&0 \\ 1&0&1&1&0&0&0&0&0&0&0&0&0 \\ 1&0&0&1&1&0&0&0&0&0&0&0&0 \\ 1&0&0&0&1&1&0&0&0&0&0&0&0 \\ 1&0&0&0&0&1&1&0&0&0&0&0&0 \\ 1&0&0&0&0&0&1&1&0&0&0&0&0 \\ 1&0&0&0&0&0&0&1&1&0&0&0&0 \\ 1&0&0&0&0&0&0&0&1&1&0&0&0 \\ 1&0&0&0&0&0&0&0&0&1&1&0&0 \\ 1&0&0&0&0&0&0&0&0&0&1&1&0 \\ 1&1&1&1&1&1&1&1&1&1&1&1&0 \end{pmatrix}$$

with a polynomial $p(x) = x^{13} + x^{11} + x^{10} + x^3 + x^2 + x + 1$. A plot of successive points (z_n , z_{n+1}) defines a fractal-like pattern depicted in Fig. 1.

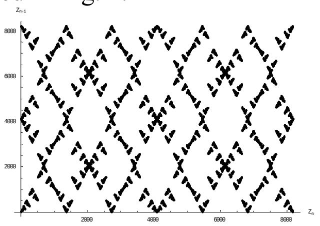


Fig. 1. Fractal-like pattern

The pattern is one-to-one mapping and contains 2^{13}- 1 points.

Example 2. Split-shift Bernoulli map.

Here we start from the well-known fact that a *m*-sequence generation by conventional linear feedback shift registers approximates the Bernoulli map [4]. Let a transition matrix *B* in a form (3) be slightly modified such that $b_{13,13}$=1,$b_{1,1}$=$b_{1,2}$=…=$b_{1,8}$=$b_{1,10}$= $b_{1,11}$= $b_{1,12}$=1, $b_{1,9}$= $b_{1,13}$=0. *B* has a primitive polynomial $p(x) = x^{13} + x^4 + x^3 + 1$. A new pattern of the corresponding *m*-sequence of 13-bit decimal numbers, shown in Fig. 2

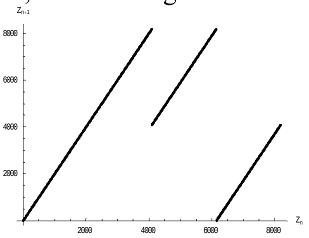


Fig. 2.A pattern: quantized split-shift Bernoulli map

can be described by the split-shift Bernoulli map:

$$\varphi(x) = \begin{cases} 2x & 0 < x < 1/2 \\ 2x - 1/2 & 1/2 < x < 3/4 \\ 2x - 3/2 & 3/4 < x < 1 \end{cases} \quad (11)$$

with a uniform probabilistic measure on the unit interval.

3. Number of *M*-sequences: Numerical Experiment and Analytical Results

We numerically investigate the characteristic polynomials for all 2^{m^2} possible variants of the matrix *B*. We count those matrices which have primitive characteristic polynomials. As a result we get the following table

m	1	2	3	4	5
N_M	1	2	48	2688	1935360

Table 2. Number of *m*-sequences for different *m*

A number of primitive polynomials over GF(2) is known to be [3]

$$N_p(m) = \frac{\phi(2^m - 1)}{m} \quad (12)$$

where $\phi(x)$ is the Euler's totient function. We introduce a new parameter

$$K_m = \frac{N_M(m)}{N_p(m)} \qquad (13)$$

which characterizes the number of different patterns for fixed m. From Table 2 and by use of (12) and (13) we easily get a chain of the values K_m with a common property for all $m > 1$

$$\frac{K_m}{K_{m-1}} = 2^{m-1}\left(2^{m-1}-1\right) \qquad (14)$$

which can be inductively proven. The recurrence equation (14) with an initial parameter $K_1 = 1$ has a solution

$$K_m = \prod_{i=1}^{m-1} 2^i\left(2^i - 1\right) = 2^{m(m-1)/2}\prod_{i=1}^{m-1}\left(2^i-1\right).$$

Then from (13) a total number of m-sequences generated by both dynamical systems (1) and (6) is given by

$$N_M(m) = \frac{\phi\left(2^m-1\right)}{m}2^{m(m-1)/2}\prod_{i=1}^{m-1}\left(2^i-1\right) \qquad (15)$$

Fig. 3 shows the number as a function of m in a log scale.

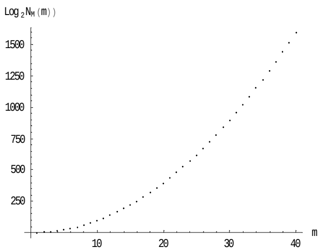


Fig. 3. A curve of dependence $log_2(N_M)$ on m

The number exponentially increases with m and due to a smooth character of the depicted curve, simple approximations for $N_M(m)$ can be found.

3.1. Classification of patterns

All $N_M(m)$ patterns can be collected in $N_p(m)$ sets with K_m patterns. It means that every pattern in a set is characterized by the same characteristic polynomial. Moreover, all these patterns are topologically equivalent, i.e.

$$\begin{cases} B_i \cdot H_{i,j} = H_{i,j} \cdot B_j \\ A_i \cdot \tilde{H}_{i,j} = \tilde{H}_{i,j} \cdot A_j \end{cases}; \; i,j \in \{1,2,\ldots,K_m\} \qquad (16)$$

where B_i and A_i are pattern matrices from the set, $H_{i,j}$ and $\tilde{H}_{i,j}$ are the homeomorphisms. $H_{i,i}$ and $\tilde{H}_{i,i}$ are the identity matrices with dimensions m x m and 2^m x 2^m, respectively. One can show a transitivity property for matrices H:

$$\begin{cases} H_{i,k} = H_{i,j} \cdot H_{j,k} \\ \tilde{H}_{i,k} = \tilde{H}_{i,j} \cdot \tilde{H}_{j,k} \end{cases}; \; i,j,k \in \{1,2,\ldots,K_m\}$$

and $C \cdot \tilde{H}_{i,j} = H_{i,j} \cdot C$ since $B_i \cdot C = C \cdot A_i \quad \forall i \in \{1,\ldots,K_m\}$.

Any matrix B_i with a primitive characteristic polynomial $p_l(x)$ ($l = 1,2,\ldots, N_p(m)$) has the following structure

$$B_i = \begin{pmatrix} b_1^{(i)} \; b_2^{(i)} \ldots b_{m-1}^{(i)} \, b_m^{(i)} \\ \Omega_l^{(i)} \end{pmatrix},$$

where $\Omega_l{}^{(i)}$ is a (m - 1 x m) sub-matrix with an unique configuration of bits for every pattern. Table 3 collects a few examples of this sub-matrix for different patterns.

Bernoulli map	Tent map	Split-shift Bernoulli map
$\Omega_l^{(1)} = \begin{pmatrix} 1 & 0 & \ldots 0 & 0 \\ 0 & 1 & \ldots 0 & 0 \\ \vdots & \vdots \ldots & \vdots & \vdots \\ 0 & 0 \ldots & 1 & 0 \end{pmatrix}$	$\Omega_l^{(2)} = \begin{pmatrix} 1 & 0 & \ldots 0 & 1 \\ 0 & 1 & \ldots 0 & 1 \\ \vdots & \vdots \ldots & \vdots & \vdots \\ 0 & 0 \ldots & 1 & 1 \end{pmatrix}$	$\Omega_l^{(3)} = \begin{pmatrix} 1 & 0 & \ldots 0 & 0 \\ 0 & 1 & \ldots 0 & 0 \\ \vdots & \vdots \ldots & \vdots & \vdots \\ 0 & 0 \ldots & 1 & 1 \end{pmatrix}$

Table 3. Sub-structures of binary transition matrices

The following system of binary equations

$$\left\{\det\left(B_i + x \cdot I\right) = p_l(x), i = 1,2,\ldots,K_m\right\}$$

allows to find an unique solution $\{b_1{}^{(i)}, b_2{}^{(i)}, \ldots\, b_m{}^{(i)}\}$ for every $i = 1,\ldots, K_m$. For example, for the second and third patterns we define their characteristic polynomials:

$$\det\left(B_2 + x\cdot I\right) = x^m + \sum_{j=1}^{m-1}\left(1 + \sum_{i=1}^{m-j} b_i^{(2)}\right)x^j + \sum_{i=1}^{m} b_i^{(2)}$$

$$\det\left(B_3 + x\cdot I\right) = x^m + \left(1 + b_1^{(3)}\right)x^{m-1} + \left(b_1^{(3)} + b_2^{(3)}\right)x^{m-2}$$
$$+\ldots+\left(b_{m-2}^{(3)} + b_{m-1}^{(3)}\right)x + \left(b_{m-1}^{(3)} + b_m^{(3)}\right)$$

Comparing both polynomials to a primitive polynomial $p_l(x) = p(x)$ leads to two equation systems for the coefficients of the first rows of B_2 and B_3:

$$b_1^{(2)} = p_{m-1} + 1,\; b_i^{(2)} = p_{m-i} + p_{m-i+1},\; i = 2,\ldots,m-1; b_m^{(2)} = p_1;$$

$$b_1^{(3)} = p_{m-1} + 1,\; b_i^{(3)} = \sum_{i=1}^{i} p_{m-i} + 1, i = 2,\ldots,m-1; b_m^{(3)} = \sum_{i=1}^{m-1} p_i.$$

When a pair of matrices B_i and B_j is given (16) is a system of m x m equations with respect to m x m elements of the matrix $H_{i,j}$ .Here we show a simple solution of this system with a polynomial $p(x)= x^3+ x^2+1$, i.e. $m = 3, p_2 =1, p_1 = 1$, for a topological conjugation between quantized Bernoulli and tent maps:

$$H_{1,2} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

4. Autocorrelation properties of *m*-sequences

We have shown that there exist quantized chaotic maps in a set of all K_m patterns. For given m they can be in principle catalogued. Auto-correlation properties of these maps are similar to ones of their real-valued prototypes as already shown for a tent [2] and Bernoulli [4] maps. These maps belong to a class of onto chaotic maps with well-known statistical properties. In this section we analyze auto-correlation function of quantized chaotic map (Fig.3) not belonging to the onto maps class. A general expression for the autocorrelation at lag n of its prototype split-shift Bernoulli map (11) is given by

$$c_\varphi(n) = \int_0^1 x\varphi^{(n)}(x)dx - \frac{1}{4} \qquad (17)$$

where $\varphi^{(n)}$ is the n-fold of the map function φ. In [5] authors have investigated autocorrelations of the split-shift Bernoulli maps and shown their chaotic behaviour with asymptotical $(n \to \infty)$ Gaussian distribution. Contrary to the real-valued map an acf of a quantized map is fully deterministic and can be calculated by

$$c_z\left(n\right)=\frac{1}{N}\sum_{i=1}^{N}z_i z_{i+n}-2^{2(m-1)}\ ,$$

where $Z_M=\{z_1, z_2,\ldots, z_N\}$ is a decimal m-sequence. Fig. 4 compares both normalized autocorrelation functions and shows a poor agreement between them for large n as was theoretically predicted.

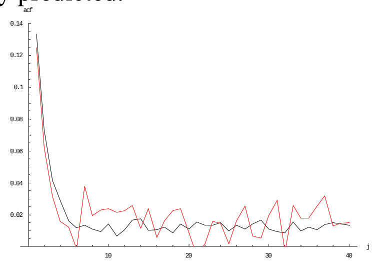


Fig. 4 Autocorrelations of real- (red curve) and decimal-valued (black curve) split-shift Bernoulli maps.

The autocorrelation functions of the binary m-sequences generated by LFSRs with the transition matrices B of the type (3) are well-known to be two-valued. This property holds for all binary m-sequences formed by (1) with an arbitrary matrix B having a primitive characteristic polynomial. We also note that a croscorrelation function of a pair of binary m-sequences generated by any matrices B_i and B_j from different sets (see definition in section 3) with a preferred pair of polynomials is three-valued. Thus, for example, the Gold sequences, widely used in spread spectrum communication systems, can be easily formed from such pairs of binary m-sequences.

4.1. Design of decimal M-sequences with prescribed autocorrelation properties

We define the following problem: how can a binary m-sequence generation scheme (1) be modified in order to provide a given autocorrelation of decimal m-sequences. A work [2] demonstrates a design of both generators (1) and (6) of δ-correlated m-sequences on a base of a tent map. Here we present a general algorithmic approach for an arbitrary autocorrelation.

Let a map φ and its acf in a form (17) be given. We fix m and matrix A by quantizing a map φ such that the conditions (7) and (8) are satisfied. Thus a problem is to construct a matrix B with a primitive characteristic polynomial for a given A. The Eq. (10) is crucial for this.

Note that the conditions (7) and (8) are necessary but not sufficient to provide (10). In sequel we derive additional conditions for that.

Without loss of generality we take m = 4 and calculate right side of (10)

$$D=C\cdot A\ . \qquad (18)$$

On the other hand

$$B\cdot C=D\ . \qquad (19)$$

From (19) we derive a few first equations for binary elements of a first row of a matrix D :

$$0=d_{1,1};b_{1,1}=d_{1,2};b_{1,2}=d_{1,3}$$

A fourth one $b_{1,1}\cdot 1+b_{1,2}\cdot 1=d_{1,4}$ gives a first condition

$$d_{1,2}+d_{1,3}=d_{1,4}\,. \qquad (20)$$

If it is false, i.e. $d_{1,2}+d_{1,3}\neq d_{1,4}$, where $d_{i,j}$ are elements of D from (18) then a designed matrix A should be slightly modified to provide (20).

If (20) holds then step by step we continue derive conditions for elements $d_{i,j}$:

$$\begin{array}{l} b_{1,3}=d_{1,5};\ \ \left\{d_{1,i+1}+d_{1,5}=d_{1,i+9},\ i=1,2,3\right\} \\ b_{1,4}=d_{1,9};\ \ \left\{d_{1,i+1}+d_{1,9}=d_{1,i+9},\ i=1,\ldots,7\right\} \end{array} \qquad (21)$$

By analogy we find all conditions of type (20) and (21) for three other rows of matrix B. At the final step a modified matrix A meets (20) and (21) as well (7)-(8) and a system

$$\left\{b_{i,1}=d_{i,2},\ b_{i,2}=d_{i,3},\ b_{i,3}=d_{i,5},\ b_{i,4}=d_{i,9};\ \ i=1,2,3,4\right\}$$

where $d_{i,j}$ are calculated from (18) defines all elements of matrix B having a primitive characteristic polynomial. At the same time a dynamical system (6) with matrix A generates a decimal m-sequence with prescribed autocorrelations. The above approach has been successfully tested for the Bernoulli, tent and split-shift Bernoulli maps.

5. Conclusions

In this work we established a topological equivalence of binary and decimal-valued m-sequences and derived necessary and sufficient conditions for that. On this theoretical basis a method to obtain transition matrices for the recursive generation of integer sequences with desired autocorrelation properties is proposed.

Acknowledgments

Author is grateful to C. Nicolis and G. Nicolis for their interest in this work and F. Dachselt, B. Mohymont and S. Vannitsem for useful discussions. This work is supported by the Belgian Federal Science Policy Office under contract No MO/34/004 and European Commission Project under contract No 12975 (NEST).

References

[1] D. Yoshioka, A. Tsuneda and T. Inoue, “An algorithm for generation of maximal-period sequences based on one-dimensional chaos maps with finite bits”, *IEICE Trans. on Fundamentals,* vol. E87-A, no. 6, pp. 1371-1376, 2004.

[2] A. L. Baranovski, F. Dachselt and W. Rave, “Nonlinear dynamics of PN-sequences”, Proc. 14th IST Mobile and Wireless Communications Summit, June 2005.

[3] P. Fan, M. Darnell, “Sequence Design for Communications Applications”, New York: Wiley, 1996.

[4] T. Kohda and M. Fukushige, “Note on finite-word-length realization of Bernoulli shift by M-sequences”, *IEICE Trans. on Fundamentals,* vol. E74, no. 10, pp. 3024-3028, Oct. 1991.

[5] A. L. Baranovski and A.J.Lawrance, “Autocorrelation Chaos from Piecewise Linear Maps”, submitted to *Int. J. Bifuracations and Chaos*, 2005.