Regular Synthesis Method of a Complete Class of Ternary Bent-Sequences and Their Nonlinear Properties

A.V. Sokolov[1], O.N. Zhdanov[2]
[1]*Odessa National Polytechnic University, Ukraine.*
[2]*Siberian State Aerospace University Named After Academician M.F. Reshetnev, Krasnoyarsk, Russia.*
radiosquid@gmail.com

***Abstract*—A regular synthesis method of the full class of ternary bent-sequences based on their representation in the form of 3-bent-squares is developed. The formula for the nonlinearity estimation of ternary sequences, based on their Vilenkin-Christenson spectral coefficients is introduced. The distribution of nonlinearity of the full code of length $N=9$ is researched.**

***Index Terms*—Bent-Sequence; Many-Valued Logic; Vilenkin-Christenson Transform; Nonlinearity.**

I. Introduction

In recent years, the use of advanced algebraic constructions in modern telecommunication technology is becoming more widespread. This fact has attracted the attention of researchers for the development of methods of synthesis of such advanced algebraic constructions as perfect binary arrays [1], binary [2] and many-valued [3] de Bruijn sequences, constructions of the Galois fields [4], etc. Amongst the advanced algebraic constructions, a special place is occupied by bent-sequences, which have uniform absolute values of spectral coefficients and maximum value of nonlinearity. Since its introduction by O. Rothaus [5], bent-functions have been used in modern science and technology. The uniform spectral properties of bent-functions lead to their application in the form of C-codes in MC-CDMA (Multi Code Code Division Multiple Access) technology for reducing the PAPR (Peak-to-Average Power Ratio) of signals [6] and in cryptography for constructing highly nonlinear S-boxes [7], and building pseudo-random key sequence generators [8, 9].

Another trend in the development of modern methods in the branch of telecommunications and information security is the implementation of the principles of many-valued logic [10]. Thus, the method of a code division multiple access based on Vilenkin-Christenson functions is proposed in [11], the method of synthesis of S-boxes, optimal according to the criterion of correlation dependence between output and input vectors is proposed in [12], the generation method of ternary pseudorandom key sequences is proposed in [13], and in particular, for application of quantum cryptography in [14]. Many of the perspective applications of many-valued logic are in some way connected with the advanced algebraic constructions over the Galois field $GF(3)$ of three elements $\{0,1,2\}$, particularly with the bent-functions.

However, the bent-functions over $GF(3)$ are not sufficiently researched, in particular, there are no regular (non brute force) methods of their synthesis or even a way to estimate the level of nonlinearity of an arbitrary ternary function compared to that of bent-functions.

The purpose of this paper is to develop a regular synthesis method of ternary bent-functions of two variables and the criteria of estimation of nonlinearity of arbitrary ternary functions.

In Section II of this paper, we consider the basic definition of ternary bent-functions and introduce a new form of representation of ternary bent-sequences. Section III is devoted to the development of a regular synthesis method of ternary bent-functions of two variables. In Section IV, we introduce a method of estimation of nonlinearity of an arbitrary ternary function (NL -coefficient).

II. Main Definitions

Let a ternary complex matrix of Vilenkin-Christenson transform of order $N=9$ be:

$$V_9=\begin{bmatrix}
e^{j0^{o}} & e^{j0^{o}} & e^{j0^{o}} & e^{j0^{o}} & e^{j0^{o}} & e^{j0^{o}} & e^{j0^{o}} & e^{j0^{o}} & e^{j0^{o}} \\
e^{j0^{o}} & e^{j120^{o}} & e^{j240^{o}} & e^{j0^{o}} & e^{j120^{o}} & e^{j240^{o}} & e^{j0^{o}} & e^{j120^{o}} & e^{j240^{o}} \\
e^{j0^{o}} & e^{j240^{o}} & e^{j120^{o}} & e^{j0^{o}} & e^{j240^{o}} & e^{j120^{o}} & e^{j0^{o}} & e^{j240^{o}} & e^{j120^{o}} \\
e^{j0^{o}} & e^{j0^{o}} & e^{j0^{o}} & e^{j120^{o}} & e^{j120^{o}} & e^{j120^{o}} & e^{j240^{o}} & e^{j240^{o}} & e^{j240^{o}} \\
e^{j0^{o}} & e^{j120^{o}} & e^{j240^{o}} & e^{j120^{o}} & e^{j240^{o}} & e^{j0^{o}} & e^{j240^{o}} & e^{j0^{o}} & e^{j120^{o}} \\
e^{j0^{o}} & e^{j240^{o}} & e^{j120^{o}} & e^{j120^{o}} & e^{j0^{o}} & e^{j240^{o}} & e^{j240^{o}} & e^{j120^{o}} & e^{j0^{o}} \\
e^{j0^{o}} & e^{j0^{o}} & e^{j0^{o}} & e^{j240^{o}} & e^{j240^{o}} & e^{j240^{o}} & e^{j120^{o}} & e^{j120^{o}} & e^{j120^{o}} \\
e^{j0^{o}} & e^{j120^{o}} & e^{j240^{o}} & e^{j240^{o}} & e^{j0^{o}} & e^{j120^{o}} & e^{j120^{o}} & e^{j240^{o}} & e^{j0^{o}} \\
e^{j0^{o}} & e^{j240^{o}} & e^{j120^{o}} & e^{j240^{o}} & e^{j120^{o}} & e^{j0^{o}} & e^{j120^{o}} & e^{j0^{o}} & e^{j240^{o}}
\end{bmatrix}. \qquad (1)$$

A. Definition 1 [13]

Ternary sequence $H=[h_0,h_1,...,h_i,...,h_{N-1}]$ of length $N=3^{2m}$, $m=1,2,3,...$, where the coefficients are $h_i\in\left\{e^{j0},e^{j120},e^{j240}\right\}$ called a ternary bent-sequence, if it has a uniform distribution of absolute values of Vilenkin-

Christenson transform coefficients, which can be represented in matrix form:

$$\left|\Omega_B(\omega)\right| = \left|H \cdot \overline{V}_N\right| = const, \quad \omega = \overline{0, N-1} \qquad (2)$$

where V_N is Vilenkin-Christenson matrix [15] of order N and $\overline{V}_N$ is the matrix from complex conjugate elements of V_N.

Bent-sequences are considered as the truth tables of corresponding bent-functions, which can be represented, for example, in algebraic normal form [16]; hence, bent-sequences and bent-functions are just different ways to describe the same natural phenomenon.

An important and actual task is to develop the regular method of synthesis of the full class of ternary bent-sequences of two variables. To solve this task, in this paper we propose a new form of representation of ternary bent-sequences as 3-bent-squares.

Consider the Vilenkin-Christenson matrix of order $n = \sqrt{N}$, i.e., in our case, $n = 3$:

$$V_3 = \begin{bmatrix} e^{j0} & e^{j0} & e^{j0} \\ e^{j0} & e^{j120} & e^{j240} \\ e^{j0} & e^{j240} & e^{j120} \end{bmatrix} \qquad (3)$$

and also let us represent the original ternary bent-sequence in the form of a sequence of three segments:

$$H = [h_0, h_1, h_2, h_3, h_4, h_5, h_6, h_7, h_8] \Rightarrow$$
$$\Rightarrow \begin{bmatrix} \chi_1 \\ \chi_2 \\ \chi_3 \end{bmatrix} = \begin{bmatrix} h_0 & h_1 & h_2 \\ h_3 & h_4 & h_5 \\ h_6 & h_7 & h_8 \end{bmatrix} = \begin{bmatrix} e^{ja_0} & e^{ja_1} & e^{ja_2} \\ e^{ja_3} & e^{ja_4} & e^{ja_5} \\ e^{ja_6} & e^{ja_7} & e^{ja_8} \end{bmatrix}, \qquad (4)$$

where $a_i = \arg(h_i) \in \{0^{\text{o}}, 120^{\text{o}}, 240^{\text{o}}\}, i = \overline{0, N-1}$.

In order to develop a regular method for the synthesis of full class of ternary bent-sequences, we introduce the following definition.

B. Definition 2

3-bent-square is the matrix B whose lines are Vilenkin-Christenson transform coefficients of vectors $\{\chi_i\}$.

In the case of ternary bent-functions of two variables, it is easy to write down the values of these coefficients.

$$B = \begin{bmatrix} \chi_1 \overline{V_3} \\ \chi_2 \overline{V_3} \\ \chi_3 \overline{V_3} \end{bmatrix} = \begin{bmatrix} \begin{bmatrix} e^{ja_0} & e^{ja_1} & e^{ja_2} \end{bmatrix} \cdot \begin{bmatrix} e^{j0} & e^{j0} & e^{j0} \\ e^{j0} & e^{j240} & e^{j120} \\ e^{j0} & e^{j120} & e^{j240} \end{bmatrix} \\ \begin{bmatrix} e^{ja_3} & e^{ja_4} & e^{ja_5} \end{bmatrix} \cdot \begin{bmatrix} e^{j0} & e^{j0} & e^{j0} \\ e^{j0} & e^{j240} & e^{j120} \\ e^{j0} & e^{j120} & e^{j240} \end{bmatrix} \\ \begin{bmatrix} e^{ja_6} & e^{ja_7} & e^{ja_8} \end{bmatrix} \cdot \begin{bmatrix} e^{j0} & e^{j0} & e^{j0} \\ e^{j0} & e^{j240} & e^{j120} \\ e^{j0} & e^{j120} & e^{j240} \end{bmatrix} \end{bmatrix} = \qquad (5)$$
$$= \begin{bmatrix} e^{ja_0} + e^{ja_1} + e^{ja_2} & e^{ja_0} + e^{j(a_1+240)} + e^{j(a_2+120)} & e^{ja_0} + e^{j(a_1+120)} + e^{j(a_2+240)} \\ e^{ja_3} + e^{ja_4} + e^{ja_5} & e^{ja_3} + e^{j(a_4+240)} + e^{j(a_5+120)} & e^{ja_3} + e^{j(a_4+120)} + e^{j(a_5+240)} \\ e^{ja_6} + e^{ja_7} + e^{ja_8} & e^{ja_6} + e^{j(a_7+240)} + e^{j(a_8+120)} & e^{ja_6} + e^{j(a_7+120)} + e^{j(a_8+240)} \end{bmatrix}.$$

III. Regular Synthesis Method of the Ternary Bent-Functions of Two Variables

Let us consider a bent-sequence:

$$H_1 = [e^{j0} \; e^{j0} \; e^{j0} \; e^{j0} \; e^{j120} \; e^{j240} \; e^{j0} \; e^{j240} \; e^{j120}] \qquad (6)$$

which is formed by concatenation of rows of Vilenkin-Christenson matrix V_3. By multiplying sequence (6) on a Vilenkin-Christenson matrix V_9 (1) we find its spectral coefficients:

$$\Omega_B(\omega) = [3e^{j0} \; 3e^{j0} \; 3e^{j0} \; 3e^{j0} \; 3e^{j240} \; 3e^{j120} \; 3e^{j0} \; 3e^{j120} \; 3e^{j240}] \qquad (7)$$

which fully satisfy condition (2), and thus, the sequence (6) is a bent-sequence.

For the sequence (6) by means of Definition 2 and (5), we can write down its 3-bent-square:

$$B = \begin{bmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{bmatrix} \qquad (8)$$

which is a ternary analogue of the binary Agievich bent-square [17], which represents the Maiorana-McFarland construction.

It is easy to make a transition from a 3-bent-squere to the temporal representation of ternary bent-sequence using the following formula:

$$H = \frac{cat(B \cdot V)}{n}. \qquad (9)$$

where cat — is the operation of concatenation.

Proposition 1.1. 3-bent-square (8) generates a set of cardinality $J_{11} = n! = 3! = 6$ of 3-bent-squeres by applying all the possible permutations of its rows.

Therefore, on the basis of 3-bent-square (8), the following six 3-bent-squares can be built, each of which defines its corresponding ternary bent-sequence:

$$B_{11}=\begin{bmatrix}3&0&0\\0&3&0\\0&0&3\end{bmatrix};B_{12}=\begin{bmatrix}3&0&0\\0&0&3\\0&3&0\end{bmatrix};B_{13}=\begin{bmatrix}0&3&0\\3&0&0\\0&0&3\end{bmatrix};$$

$$B_{14}=\begin{bmatrix}0&3&0\\0&0&3\\3&0&0\end{bmatrix};B_{15}=\begin{bmatrix}0&0&3\\0&3&0\\3&0&0\end{bmatrix};B_{16}=\begin{bmatrix}0&0&3\\3&0&0\\0&3&0\end{bmatrix};$$

$$H_{11}=\left\{e^{j0}\ e^{j0}\ e^{j0}\ e^{j0}\ e^{j240}\ e^{j120}\ e^{j0}\ e^{j120}\ e^{j240}\right\}; \quad (10)$$

$$H_{12}=\left\{e^{j0}\ e^{j0}\ e^{j0}\ e^{j0}\ e^{j120}\ e^{j240}\ e^{j0}\ e^{j240}\ e^{j120}\right\};$$

$$H_{13}=\left\{e^{j0}\ e^{j240}\ e^{j120}\ e^{j0}\ e^{j0}\ e^{j0}\ e^{j0}\ e^{j120}\ e^{j240}\right\};$$

$$H_{14}=\left\{e^{j0}\ e^{j240}\ e^{j120}\ e^{j0}\ e^{j120}\ e^{j240}\ e^{j0}\ e^{j0}\ e^{j0}\right\};$$

$$H_{15}=\left\{e^{j0}\ e^{j120}\ e^{j240}\ e^{j0}\ e^{j240}\ e^{j120}\ e^{j0}\ e^{j0}\ e^{j0}\right\};$$

$$H_{16}=\left\{e^{j0}\ e^{j120}\ e^{j240}\ e^{j0}\ e^{j0}\ e^{j0}\ e^{j0}\ e^{j240}\ e^{j120}\right\}.$$

Proposition 1.2. The rows of each matrix $B_i, i=1,2,...,6$ (10) may be multiplied element by element (encoded) by one of a ternary sequence of length $n=3$. The total number of new structures of 3-bent-squares and, respectively, ternary bent-sequences which can be derived from each of an initial 3-bent-squares is $J_{12}=n^3=27$.

For example, let us show the process of coding of 3-bent-square (8) with the sequence $\alpha=\{e^{j0}\ \ e^{j120}\ \ e^{j240}\}$. We get the result of a new 3-bent-square and the corresponding ternary bent-sequence.

$$B_{121}=\begin{bmatrix}3&0&0\\0&3e^{j120}&0\\0&0&3e^{j240}\end{bmatrix}; \quad (11)$$

$$H_{121}=[e^{j0}\ \ e^{j0}\ \ e^{j0}\ \ e^{j120}\ \ e^{j0}\ \ e^{j240}\ \ e^{j240}\ \ e^{j0}\ \ e^{j120}].$$

Thus, on the basis of **Propositions 1.1., 1.2.,** we can build a Maiorana-McFarland class of ternary bent-sequences with total cardinality $J_1=J_{11}\cdot J_{12}=n!\cdot 3^n=6\cdot 27=162$ of ternary bent-sequences.

However, the experimental data obtained in [13] show that the total number of ternary bent-functions of two variables reaches the value $J_0=486$; thus, there are other sequences that do not belong to the Maiorana-McFarland class [18].

In this paper, it is shown that the remaining $J_2=J_0-J_1=486-162=324$ ternary bent-sequences may be represented by the following generic structure

$$B_2=\begin{bmatrix}\sqrt{3}e^{j\beta_{11}^{o}}&\sqrt{3}e^{j\beta_{12}^{o}}&\sqrt{3}e^{j\beta_{13}^{o}}\\\sqrt{3}e^{j\beta_{21}^{o}}&\sqrt{3}e^{j\beta_{22}^{o}}&\sqrt{3}e^{j\beta_{23}^{o}}\\\sqrt{3}e^{j\beta_{31}^{o}}&\sqrt{3}e^{j\beta_{32}^{o}}&\sqrt{3}e^{j\beta_{33}^{o}}\end{bmatrix}, \quad (12)$$

where, depending on the structure of the angular coefficients β_{ij} we can classify 3-bent-squares of the second type to 2 subtypes.

Subtype 1. 3-bent-squares of the first subtype containing two identical rows. It is found that a complete class of 3-bent-squares of the first subtype can be constructed on the basis of the generating class containing 12 elements, which is listed in Table 1. In order of brevity, Table 1 contains only the angular coefficients β_{ij}.

Table 1
The angular coefficients of 3-bent-squeres of the first subtype

$\begin{bmatrix}30&30&270\\30&30&270\\150&150&30\end{bmatrix}$	$\begin{bmatrix}30&30&270\\30&30&270\\270&270&150\end{bmatrix}$	$\begin{bmatrix}30&30&270\\150&150&30\\150&150&30\end{bmatrix}$	$\begin{bmatrix}30&30&270\\270&270&150\\270&270&150\end{bmatrix}$
$\begin{bmatrix}330&90&330\\330&90&330\\90&210&90\end{bmatrix}$	$\begin{bmatrix}330&90&330\\330&90&330\\210&330&210\end{bmatrix}$	$\begin{bmatrix}330&90&330\\90&210&90\\90&210&90\end{bmatrix}$	$\begin{bmatrix}330&90&330\\210&330&210\\210&330&210\end{bmatrix}$
$\begin{bmatrix}30&150&150\\30&150&150\\150&270&270\end{bmatrix}$	$\begin{bmatrix}30&150&150\\150&270&270\\150&270&270\end{bmatrix}$	$\begin{bmatrix}90&90&210\\90&90&210\\210&210&330\end{bmatrix}$	$\begin{bmatrix}90&90&210\\210&210&330\\210&210&330\end{bmatrix}$

Let us formulate the rules of the reproduction of 3-bent-squares of the first subtype on the basis of the following proposition:

Proposition 2.1. Each 3-bent-square of form (12) of the first subtype generates a new six 3-bent-squares on the basis of the following basic permutations of rows and columns

$$P=\begin{bmatrix}1&2&3\\2&3&1\\3&1&2\end{bmatrix}. \quad (13)$$

Thus, the cardinality of the 3-bent-squares set of the first subtype, taking into account **Proposition 2.1.**, and the structure of the angular coefficients matrices is $J_{21}=12\cdot 3\cdot 3=108$.

Subtype 2. All lines of 3-bent-squeres of the second subtype are different. It is found that the generating class of the 3-bent-squares angular matrices of second subtype contains 36 elements, which are presented in Table 2.

Table 2
The angular coefficients of 3-bent-squeres of the second subtype

$\begin{bmatrix}30&30&270\\30&270&30\\270&30&30\end{bmatrix}$	$\begin{bmatrix}30&30&270\\30&270&30\\150&270&270\end{bmatrix}$	$\begin{bmatrix}30&30&270\\270&30&30\\270&150&270\end{bmatrix}$	$\begin{bmatrix}30&30&270\\30&150&150\\150&30&150\end{bmatrix}$
$\begin{bmatrix}30&30&270\\30&150&150\\270&150&270\end{bmatrix}$	$\begin{bmatrix}30&30&270\\150&30&150\\150&270&270\end{bmatrix}$	$\begin{bmatrix}330&90&330\\90&330&330\\330&330&90\end{bmatrix}$	$\begin{bmatrix}330&90&330\\90&330&330\\90&90&210\end{bmatrix}$
$\begin{bmatrix}330&90&330\\330&330&90\\210&90&90\end{bmatrix}$	$\begin{bmatrix}330&90&330\\90&90&210\\330&210&210\end{bmatrix}$	$\begin{bmatrix}330&90&330\\210&90&90\\210&210&330\end{bmatrix}$	$\begin{bmatrix}330&90&330\\330&210&210\\210&210&330\end{bmatrix}$
$\begin{bmatrix}30&270&30\\270&30&30\\270&270&150\end{bmatrix}$	$\begin{bmatrix}30&270&30\\30&150&150\\150&150&30\end{bmatrix}$	$\begin{bmatrix}30&270&30\\30&150&150\\270&270&150\end{bmatrix}$	$\begin{bmatrix}30&270&30\\150&150&30\\150&270&270\end{bmatrix}$
$\begin{bmatrix}90&330&330\\330&330&90\\90&210&90\end{bmatrix}$	$\begin{bmatrix}90&330&330\\90&90&210\\210&330&210\end{bmatrix}$	$\begin{bmatrix}90&330&330\\90&210&90\\210&210&330\end{bmatrix}$	$\begin{bmatrix}90&330&330\\210&210&330\\210&330&210\end{bmatrix}$
$\begin{bmatrix}330&330&90\\90&210&90\\330&210&210\end{bmatrix}$	$\begin{bmatrix}330&330&90\\210&90&90\\210&330&210\end{bmatrix}$	$\begin{bmatrix}330&330&90\\330&210&210\\210&330&210\end{bmatrix}$	$\begin{bmatrix}270&30&30\\150&150&30\\150&30&150\end{bmatrix}$
$\begin{bmatrix}270&30&30\\150&150&30\\270&150&270\end{bmatrix}$	$\begin{bmatrix}270&30&30\\150&30&150\\270&270&150\end{bmatrix}$	$\begin{bmatrix}30&150&150\\150&150&30\\150&30&150\end{bmatrix}$	$\begin{bmatrix}30&150&150\\270&150&270\\270&270&150\end{bmatrix}$
$\begin{bmatrix}90&90&210\\90&210&90\\210&90&90\end{bmatrix}$	$\begin{bmatrix}90&90&210\\90&210&90\\330&210&210\end{bmatrix}$	$\begin{bmatrix}90&90&210\\210&90&90\\210&330&210\end{bmatrix}$	$\begin{bmatrix}90&210&90\\210&90&90\\210&210&330\end{bmatrix}$

$\begin{bmatrix}150 & 150 & 30\\270 & 150 & 270\\150 & 270 & 270\end{bmatrix}$	$\begin{bmatrix}150 & 30 & 150\\150 & 270 & 270\\270 & 270 & 150\end{bmatrix}$	$\begin{bmatrix}330 & 210 & 210\\210 & 210 & 330\\210 & 330 & 210\end{bmatrix}$	$\begin{bmatrix}270 & 150 & 270\\150 & 270 & 270\\270 & 270 & 150\end{bmatrix}$

New structures of 3-bent-squares of the second subtype, and respectively, new ternary bent-sequences can be obtained on the basis of following statement:

Proposition 2.2. Each 3-bent-square of form (12) of the second subtype generates a new six 3-bent-squares on the basis of all possible $3! = 6$ permutations of rows

$$P = \begin{bmatrix}1 & 2 & 3\\1 & 3 & 2\\2 & 1 & 3\\2 & 3 & 1\\3 & 2 & 1\\3 & 1 & 2\end{bmatrix}. \qquad (14)$$

Therefore, with consideration of **Proposition 2.2.** and the table of angular coefficients matrices of the second subtype (Table 2), we can build $6 \cdot 36 = 216$ new structures of 3-bent-squares.

The total cardinality of the second class of 3-bent-squares is $J_2 = 108 + 216 = 324$ which is different from the 3-bent-squares, and accordingly, ternary bent-sequences.

The cardinality of class of all synthesised by the regular method ternary bent-sequences is

$$J = J_1 + J_2 = 162 + 324 = 486, \qquad (15)$$

which is full class and complies with the results obtained in [13].

IV. NONLINEARITY ESTIMATION METHOD OF AN ARBITRARY TERNARY SEQUENCE

The most important characteristic of any construction, which is used in cryptography is nonlinearity. Nonlinearity is generally estimated as the degree of similarity of the algebraic construction with a variety of constructions, which are considered to be linear [19]. Examples of such constructions are the Walsh functions or their many-valued analogues — Vilenkin-Christenson functions.

For example, consider a 3-function:

$$A = \left\{ e^{j120} \;\; e^{j0} \;\; e^{j240} \;\; e^{j120} \;\; e^{j0} \;\; e^{j240} \;\; e^{j120} \;\; e^{j0} \;\; e^{j240} \right\}, \; (16)$$

which has the following Vilenkin-Christenson spectral coefficients:

$$\Omega_A = A \cdot \overline{V}_9 = \\ = \left\{ 0 \quad 0 \quad 9e^{j120^{\circ}} \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \right\}. \qquad (17)$$

Each Vilenkin-Christenson spectral coefficient (17) characterises the value of the content of each Vilenkin-Christenson function (the row of V_N matrix) in the investigated sequence.

As the set of Vilenkin-Christenson functions is taken as the set of the most linear functions, we can estimate the value of the linearity of the function by the maximum value of the spectral coefficients. Thus, the maximum spectral coefficient of sequence (16) is $L = \max\left\{ |S| \right\} = 9$, which is said to be the value of linearity. Indeed, it is easy to verify that the sequence (16) is the modified third row of the Vilenkin-Christenson matrix, which causes the absolute value of the third coefficient of the spectrum (17) to obtain the maximum possible value, equals to the length N.

Since the full ternary code can be regarded as a linear vector space, in which Vilenkin-Christenson functions are the orthonormal basis, then Parseval's equality is justified for Vilenkin-Christenson transform [20]

$$\sum_{\omega=1}^{N} \left| \Omega(\omega) \right|^2 = 3^{2k}, \qquad (18)$$

where k — is the number of variables, in which the equivalent 3-function depends, $k = \log_3 N$ and $k = n = \sqrt{N}$ for ternary bent-functions.

Thus, the minimum absolute value of Vilenkin-Christenson transform coefficients is achieved when their absolute values are constant and equal to

$$\left| \Omega(\omega) \right| = \sqrt{\frac{3^{2k}}{3^k}} = 3^{k/2}, \quad \omega = 0,1,...,N-1. \qquad (19)$$

As an estimation of the nonlinearity of 3-functions, it is rational to use the difference between the maximum possible value of Vilenkin-Christenson transform coefficients (absolute value) and Vilenkin-Christenson transform maximal coefficient (absolute value) of the investigated 3-function. This thesis can be easily generalised to the case of q-function

$$NL = \begin{cases} q^k - \max\left\{ |S| \right\}, & q > 2; \\ 2^{k-1} - \dfrac{1}{2}\max\left\{ |S| \right\}, & q = 2. \end{cases} \qquad (20)$$

Table 3 shows the distribution of NL-coefficients for the full code of length $N = 9$.

Table 3
Distribution of the NL-coefficients for full code of length $N = 9$

NL	0	1.4502	2.7550	3	3.8038	4.4174	6
Number of vector	27	486	1944	1944	4104	10692	486
Comment	Affine functions	—	—	—	—	—	Bent-functions

In this paper, we consider the case $q = 3$ in detail, whereas the case of $q > 3$ may be the subject of further research.

Conclusion

Here are the main results of the research:

1. For the first time with help of a regular method, the full class of ternary bent-sequences of length $N = 9$ was synthesised. The main structures used for the synthesis were the analogues of Agievich 3-bent-squares.
2. The concept of the NL -coefficient, which characterises the degree of nonlinearity of an arbitrary ternary function was introduced. The results of research of the distribution of vectors of ternary full code of length $N = 9$ are listed.
3. Received results are the basis for the development of cryptographic constructions based on the principles of many-valued logic, such as many-valued block encryption algorithms, many-valued pseudorandom key sequences generators, many-valued nonlinear transforms. The full class of ternary bent-sequences is also the basis for the construction of C-codes used to reduce the Peak-to-Average Power Ratio values in the CDMA technology.

Expansion of the received results on Galois fields of characteristics $p > 3$, is of interest.

References

[1] M.I. Mazurkov, V.Ya. Chechel'nitskii, “The classes of equivalent and generative perfect binary arrays for CDMA-technologies,” Radioelectron. Commun. Syst., vol. 46, no. 5, pp. 48-57, 2003.

[2] M.I. Mazurkov, A.V. Sokolov, “Synthesis methods of pseudo-random binary sequences with the property of the k-gram distribution for encryption tasks,” Works of the Odessa polytechnic univer., no. 1(38), pp.188-198, 2012.

[3] M. I. Mazurkov, A.V. Sokolov, “Constructive method for synthesis of complete classes of multilevel de Bruijn sequences,” Radioelectron. Commun. Syst., vol. 56, no. 1, pp. 36-41, 2013.

[4] M. I. Mazurkov, A. V. Sokolov, “Nonlinear transformations based on complete classes of isomorphic and automorphic representations of field GF(256),” Radioelectron. Commun. Syst., vol. 56, no. 11, pp. 513-521, 2013.

[5] O.S. Rothaus, “On “bent” functions,” J. Comb. Theory Ser. A. — USA: Academic Press Inc, no. 20(3), pp. 300-305, 1976.

[6] K.G. Paterson, “Sequences For OFDM and Multi-code CDMA: two problems in algebraic coding theory”, Sequences and their applications. Seta 2001. Second Int. Conference. Proc. Berlin: Springer, pp. 46–71, 2002.

[7] A.V. Sokolov, “Constructive method for the synthesis of nonlinear S-boxes satisfying the strict avalanche criterion”, Radioelectron. Commun. Syst., vol. 56, no. 8, pp. 415-423, 2013.

[8] M.I. Mazurkov, N.A. Barabanov, A.V. Sokolov, “The key sequences generator based on bent functions dual couples,” Works of the Odessa Polytechnic Univer., vol. 3(42), pp. 150-156, 2013.

[9] A.V.Sokolov, “The cellular automata key sequences generator,” Works of the Odessa Polytechnic University, vol. 1 (43), pp. 180-186, 2014.

[10] L. Bolc, P. Borowik, “Many-valued Logics 2: Automated reasoning and practical applications,” Springer Science & Business Media, 2003, p. 303.

[11] M.I. Mazurkov, A.V. Sokolov, N.A. Barabanov, “On the effect of the type of orthogonal transform on PAPR of signal spectrum in CDMA systems,” Informatics and Math. Methods in Sim., vol. 5, no. 1, pp. 28-37, 2015.

[12] O.N. Zhdanov, A.V. Sokolov, “Algorithm of construction of optimal according to criterion of zero correlation non-binary S-boxes,” PFMT, no. 3(24), pp. 94-97, 2015.

[13] A.V. Sokolov, O.N. Zhdanov, N.A. Barabanov, “Pseudo-random key sequence generator based on triple sets of bent-functions,” PFMT, no. 1 (26), pp. 85-91, 2016.

[14] S.O. Gnatyuk, T.S. Zhmurko, V.M. Kinzeryavy, N.A. Seylova, “Method of trit pseudorandom sequences generating for quantum cryptography systems,” Inf. Sec., vol. 22, no. 2, pp. 140-147, 2015.

[15] A.M. Trakhtman, V.A. Trakhtman, “Elements of the Theory of Discrete Signals on Finite Intervals,” Moscow, Sov. Radio, 1975 p. 208.

[16] A.V. Sokolov, O.N. Zhdanov, O.A. Ayvazian “Synthesis methods of algebraic normal form of many-valued logic functions,” System analysis and applied inform. sc., no.1, pp. 69-76, 2016.

[17] S.V. Agievich “On the representation of bent functions by bent rectangles,” Probabilistic Methods in Discrete Mathematics: Proceedings of the Fifth International Petrozavodsk Conference. Utrecht, Boston: VSP, pp. 121-135, 2002.

[18] N. Tokareva “Bent Functions: Results and Applications to Cryptography,” Academic Press, 2015, p. 220.

[19] W. Maier, O. Staffelbach “Nonlinearity criteria for cryptographic functions,” In Advances in Cryptology, EUROCRYPT’89, vol.434, Lecture Notes in Computer Science, Springer-Verlag, pp.549-562, 1990.

[20] G.B. Arfken, H. J. Weber, “Mathematical Methods for Physicists,” Harcourt: San Diego, 2005, p. 1182.