TECHNIQUE OF CONSTRUCTION OF ONE CLASS ORTHOGONAL BINARY $3D$-SEQUENCES

Fikrat Feyziyev[1] and Zamina Samadova[2]

[1]Sumgayit State University, Sumgayit, Azerbaijan, *FeyziyevFG@mail.ru*
[2]Azerbaijan University of Languages, Baku, Azerbaijan

In the report the question of obtain of conditions of orthogonality of input sequences for one class $3D$-nonlinear modular dynamical systems *(*$3D$ - NMDS*)* [1,2] and on the basis of it development of a technique of construction of orthogonal input sequences for this system is considered. Such sequences are used in the solution of a problem of synthesis for various classes binary modular dynamic systems [1].

Let's consider NMDS with the maximal degree of the nonlinearity s, fixed depth of memory n_0 and sets of limited connection $P = P_1 \times P_2 = \{p_1(1),..., p_1(r_1)\} \times \{p_2(1),..., p_2(r_2)\}$, which is described following two valued analogues of Volterra's polynomial [2]

$$y[n,c_1,c_2] = \sum_{i=1}^{s} \sum_{i_1=1}^{\lambda_i} \sum_{\bar{j}\in L_1(\ell_1)} \sum_{\bar{\tau}\in L_2(\ell_2)} \sum_{\bar{n}_2\in\Gamma(\ell_1,\ell_2,\bar{m})} h_{i,i_1}[\bar{j},\bar{\tau},\bar{n}_2]\times$$
$$\times \prod_{(\alpha,\beta,\sigma)\in Q_1(i,i_1)} \vartheta_{i,i_1}[n-n_1(\alpha,\beta,\sigma), c_1+p_1(j_\alpha), c_2+p_2(\tau_\beta)],\ GF(2). \qquad (1)$$

Here $n \in T = \{0,1,2,...\}$, $c_i \in \{...,-1,0,1,...\}$, $i = \overline{1,2}$; $y[n,c_1,c_2] \in GF(2)$ is output sequence of NMDS ; $\vartheta_{i,i_1}[n,c_1,c_2] \in GF(2)$ is input sequence of NMDS and enters in its those inputs, which correspond i_1 – th trio $(\ell_1,\ell_2,\bar{m})$ from sets $F(i)$; λ_i there is the number of elements of set $F(i)$;

$P_i = \{p_i(1),..., p_i(r_i)\}$, $p_i(1) < ... < p_i(r_i)$, $p_i(j) \in \{...,-1,0,1...\}$ $j = 1,...,r_i$ $\quad i = \overline{1,2}$,
besides, $p_i(1)$ and $p_i(r_i)$ are finite integers $(i = \overline{1,2})$;

$$F(i) = \{(\ell_1,\ell_2,\bar{m}) \mid \bar{m} = (m_{1,1},...,m_{1,\ell_2},...,m_{\ell_1,\ell_2}), \sum_{\alpha=1}^{\ell_1}\sum_{\beta=1}^{\ell_2} m_{\alpha,\beta} = i; \quad m_{\alpha,\beta} \in \{0,...,n_0+1\},$$
$\alpha = \overline{1,\ell_1}$, $\beta = \overline{1,\ell_2}$; For all $\alpha \in \{1,...,\ell_1\}$ exists such $\beta \in \{1,...,\ell_2\}$, that $m_{\alpha,\beta} \neq 0$ and for all $\beta \in \{1,...,\ell_2\}$ exists such $\alpha \in \{1,...,\ell_1\}$, that $m_{\alpha,\beta} \neq 0$; $\ell_i \in \{1,...,r_i\}$, $i = \overline{1,2}\}$;

$Q_0(i,\ell_1,\ell_2,\bar{m}) = \{(\alpha,\beta) \mid m_{\alpha,\beta}$ is komponent of vektors $\bar{m}$ and $m_{\alpha,\beta} \neq 0, \alpha = \overline{1,\ell_1}$, $\beta = \overline{1,\ell_2}\}$;

$L_1(\ell_1) = \{(j_1,...,j_{\ell_1}) \mid 1 \le j_1 < ... < j_{\ell_1} \le r_1\}$, $\quad L_2(\ell_2) = \{(\tau_1,...,\tau_{\ell_2}) \mid 1 \le \tau_1 < ... < \tau_{\ell_2} \le r_2\}$;

$\Gamma_1(m_{\alpha,\beta}) = \{\bar{n}_{\alpha,\beta} = (n_1(\alpha,\beta,1),...,n_1(\alpha,\beta,m_{\alpha,\beta})) \mid 0 \le n_1(\alpha,\beta,1) < ... < n_1(\alpha,\beta,m_{\alpha,\beta}) \le n_0\}$;

$$\bar{m} = (m_{1,1},...,m_{1,\ell_2},...,m_{\ell_1,\ell_2})\ \bar{n}_2 = (\bar{n}_{1,1},...,\bar{n}_{1,\ell_2},...,\bar{n}_{\ell_1,\ell_2});$$
$$Q_1(i,i_1) = \{(\alpha,\beta,\sigma) \mid \sigma \in \{1,...,m_{\alpha,\beta}\},\ (\alpha,\beta) \in Q_0(i,\ell_1,\ell_2\bar{m})\};$$

For all $\bar{n}_{\alpha,\beta} \in \Gamma_1(m_{\alpha,\beta})$, $\alpha = \overline{1,\ell_1}$, $\beta = \overline{1,\ell_2}$ set of all block vectors (collections) $\bar{n}_2$ is designated as $\Gamma(\ell_1,\ell_2,\bar{m})$.

Let $n \in [0,N] \equiv \{0,1,...,N\}$, $c_1 \in [0,C_1] \equiv \{0,1,...C_1\}$, $c_2 \in [0,C_2] \equiv \{0,1,...C_2\}$.

By $\bar{n}_{2,k}$ we shall designate k - th an element in $\Gamma(\ell_1,\ell_2,\bar{m})$, and components of a vectors $\bar{n}_{2,k}$ is designated as $n_1^{(k)}(\alpha,\beta,\sigma)$. Let

$$V_0(i,i_1,\bar{j},\bar{\tau},\bar{n}_{2,k}) = \left\{ \prod_{(\alpha,\beta,\sigma)\in Q_1(i,i_1)} \vartheta_{i,i_1}[n - n_1^{(k)}(\alpha,\beta,\sigma), c_1 + p_1(j_\alpha), c_2 + p_2(\tau_\beta)] \right\}. \quad (2)$$

To each trio (n,c_1,c_2), $n \in [0,N]$, $c_1 \in [0,C_1]$, $c_2 \in [0,C_2]$ in a matrix $V_0(i,i_1,\bar{j},\bar{\tau},\bar{n}_{2,k})$ corresponds a line. Let

$$V_1(i,i_1,\bar{j},\bar{\tau}) = (V_0(i,i_1,\bar{j},\bar{\tau},\bar{n}_{2,1}) \ ... \ V_0(i,i_1,\bar{j},\bar{\tau},\bar{n}_{2,|\Gamma(\ell_1,\ell_2,\bar{m})|}))$$
$$V_2(i,i_1) = (V_1(i,i_1,\bar{j}_1,\bar{\tau}_1) \ ... \ V_1(i,i_1,\bar{j}_1,\bar{\tau}_{|L_2(\ell_2)|}) \ ... \ V_1(i,i_1,\bar{j}_{|L_1(\ell_1)|},\bar{\tau}_{|L_2(\ell_2)|})) \quad (3)$$
$$V_3(i) = (V_2(i,1) \ ... \ V_2(i,|F(i)|) \ V = (V_3(1) \ ... \ V_3(s)).$$

If in a block matrix V for all sub matrixes we shall write it all elements, then we shall receive an simple matrix with dimensions $(N+1)(C_1+1)(C_2+1) \times r^*$, where $r^* = \sum_{i=1}^{s} C^i_{(n_0+1)r_1r_2}$.

If a matrix V formed from

$$\{\vartheta_{i,i_1}[n,c_1,c_2] : n \in [0,N], \ c_1 \in [0,C_1], \ c_2 \in [0,C_2]\}, \ i_1 = \overline{1,\lambda_i}, \quad i = \overline{1,s} \quad (4)$$

by formulas (2), (3) and satisfies to conditions of orthogonality

$$V^T \cdot V = diag[\hat{\vartheta}_{1,1},...,\hat{\vartheta}_{r^*,r^*}]; \quad \hat{\vartheta}_{\alpha,\alpha} > 0, \ \alpha = 1,...,r^*, \quad (5)$$

then sequences (4) are called orthogonal input sequences for $3D$-NMDS (1).

Let's consider the problem findings of conditions of orthogonality for sequences.

Let's designate by $r_1(i,i_1)$, $r_2(i,i_1)$, $r_3(i)$ are designate number of columns of a matrix $V_1(i,i_1,\bar{j},\bar{\tau})$, $V_2(i,i_1)$, $V_3(i)$ accordingly.

Theorem 1. Let: a) for each $i_1 \in \{1,...,\lambda_i\}$, $i \in \{1,...,s\}$ sequence $\bar{\vartheta}_{i,i_1}[n,c_1,c_2]$ is $\{0,1\}-$sequence with the period $T_{i,i_1}+1$, $A_1(i,i_1)+1$ and $A_2(i,i_1)+1$ accordingly on argument n, c_1 and c_2, and besides,

$$\bar{V}_2(i,i_1)^{\mathrm{T}} \cdot \bar{V}_2(i,i_1) = diag\{d_{1,1}(2,i,i_1),...,d_{r_2(i,i_1),r_2(i,i_1)}(2,i,i_1)\},$$
$$d_{\alpha,\alpha}(2,i,i_1) > 0, \alpha = 1,...,r_2(i,i_1), \quad (6)$$

where $d_{\alpha,\alpha}(2,i,i_1)-$elements of a matrix $\bar{V}_2(i,i_1)^{\mathrm{T}} \cdot \bar{V}_2(i,i_1)$, and a matrix $\bar{V}_0(i,i_1,\bar{j},\bar{\tau},\bar{n}_{2,k})$, $\bar{V}_1(i,i_1,\bar{j},\bar{\tau})$, $\bar{V}_2(i,i_1)$, $\bar{V}_3(i)$, $\bar{V}$ it is formed from sequences

$$\{ \ \bar{\vartheta}_{i,i_1}[n,c_1,c_2] : n \in [0,T_{i,i_1}], \ c_1 \in [0,A_{i,i_1}], \ c_2 \in [0,B_{i,i_1}] \}$$

analogies by formulas (2), (3);

b) For each $i_1 \in \{1,...,\lambda_i\}, i \in \{1,...,s\}$ and $(n,c_1,c_2) \in [0,T'] \times [0,C_1'] \times [0,C_2'] \subset \subset [0,N] \times [0,C_1] \times [0,C_2]$ sequence $\vartheta'_{i,i_1}[n,c_1,c_2]$ is defining by follows relation:

$$\vartheta'_{i,i_1}[n,c_1,c_2]=\begin{cases}\overline{\vartheta}_{i,i_1}[n,c_1,c_2], & if \quad (n,c_1,c_2)\in F(i,i_1)\times G_1(i,i_1)\times G_2(i,i_2),\\ 0 & ,if \quad (n,c_1,c_2)\notin F(i,i_1)\times G_1(i,i_1)\times G_2(i,i_2),\end{cases} \tag{7}$$

where $F(i,i_1)=\lfloor N_1(i,i_1)-\tau_{i,i_1}, N_1(i,i_1)-\tau_{i,i_1}+T_{i,i_1}\rfloor\subset[0,T']$,

$$G_1(i,i_1)=[D_1(i,i_1),D_1(i,i_1)+A_1(i,i_1)]\subset[0,C'_1],$$
$$G_2(i,i_1)=[D_2(i,i_1),D_2(i,i_1)+A_2(i,i_1)]\subset[0,C'_2]$$

and

$$t_{i,i_1}=\begin{cases}\max\{m_{1,1},...,m_{1,\ell_2},..,m_{\ell_1,\ell_2}\}-1, if \ N_1(i,i_1)>0,\\ 0 \qquad ,if \ N_1(i,i_1)=0.\end{cases}$$

For each $i_1\in\{1,...,\lambda_i\}, i\in\{1,...,s\}$ natural numbers $N_1(i,i_1), D_1(i,i_1), D_2(i,i_1)$ and domain $[0,T']\times[0,C'_1]\times[0,C'_2]$ are those, that for each $i_1\in\{1,...,\lambda_i\}$, $i\in\{1,...,s\}$ $i'_1\in\{1,...,\lambda_{i'}\}$, $i'\in\{1,...,s\}$, where $(i,i_1)\neq(i',i'_1)$, are true a relation $F(i,i_1)\cap F(i',i'_1)=\varnothing$ or $G_1(i,i_1)\cap G_1(i',i'_1)=\varnothing$ or $G_2(i,i_1)\cap G_2(i',i'_1)=\varnothing$;

c) $\vartheta_{i,i_1}[n,c_1,c_2]$, $i_1=1,...,\lambda(i)$, $i=1,..,s$ are periodic continuation of $\vartheta'_{i,i_1}[n,c_1,c_2]$ from $[0,T']\times[0,C'_1]\times[0,C'_2]$ to other parts of domain $[0,N]\times[0,C_1]\times[0,C_2]$ with the period $T_{i,i_1}+1$, $A_1(i,i_1)+1$ и $A_2(i,i_1)+1$ accordingly on arguments n, c_1 and c_2. Then a matrix V is orthogonally in sense (5).

The theorem 1 gives a technique for construction of input test sequences. By this technique $\vartheta_{i,i_1}[n,c_1,c_2]$, $i_1=1,...,\lambda_i$, $i=1,...,s$ is construction as follows:

1. Construction of auxiliary test sequences $\overline{\vartheta}_{i,i_1}[n,c_1,c_2]$, $i_1=1,...,\lambda_i$, $i=1,..,s$ according to a condition of the theorem 1 separately, i.e. irrespective from $\overline{\vartheta}_{i,i_1}[n,c_1,c_2]$, $i'_1=1,...,\lambda_i$, $i'=1,...,s$, $(i',i'_1)\neq(i,i_1)$.

2. According to a condition of the theorem 1 dividing a domain of tests $\overline{\vartheta}_{i,i_1}[n,c]$, $i_1=1,...,\lambda_i$, $i=1,...,s$ on argument n or c_1 or c_2 or on two or three arguments by the formula (7) tests $\vartheta'_{i,i_1}[n,c_1,c_2]$, $i_1=1,...,\lambda_i$, $i=1,...,s$ are construction in the domain $[0,T']\times[0,C'_1]\times[0,C'_2]\subset[0,N]\times[0,C_1]\times[0,C_2]$.

3. According to a condition of the theorem 1 periodic continuation $\vartheta'_{i,i_1}[n,c_1,c_2]$, $i_1=1,...,\lambda_i$, $i=1,..,s$ from domain $[0,T']\times[0,C'_1]\times[0,C'_2]$ with the period $T'+1$, C'_1+1 and C'_2+1 accordingly arguments n, c_1 and c_2 in other parts of domain $[0,N]\times[0,C_1]\times[0,C_2]$ the test $\vartheta_{i,i_1}[n,c_1,c_2]$, $i_1=1,...,\lambda_i$, $i=1,...,s$ is construction of them.

Thus, one of the primary problems of construction of input test sequences $\vartheta_{i,i_1}[n,c_1,c_2]$, $i_1=1,...,\lambda_i$, $i=1,...,s$ is construction of auxiliary test sequences $\overline{\vartheta}_{i,i_1}[n,c_1,c_2]$, $i_1=1,...,\lambda_i$, $i=1,...,s$ according to a condition of orthogonality (6).

Let $\theta(i,i_1)$ there is an amount of nonzero components of a vector $\overline{m}$. Clearly, that $\theta(i,i_1)=|Q_0(i,\ell_1,\ell_2,\overline{m})|$. Let the sequence of nonzero components of a vector $\overline{m}$ is following sequence:

$$m_{\xi_{1,1},1},...,m_{\xi_{1,\nu_1},1},\ m_{\xi_{2,1},2},...,m_{\xi_{2,\nu_2},2},...,m_{\xi_{\ell_2,1},\ell_2},...,m_{\xi_{\ell_2,\nu_{\ell_2}},\ell_2}.$$

Clearly, that $\xi_{\alpha,\nu_\alpha} \le \ell_1, \alpha = 1,...,\ell_2, \bigcup_{\alpha=1}^{\ell_2} \{\xi_{\alpha,1},...,\xi_{\alpha,\nu_\alpha}\} = \{j_1, j_2,..., j_{\ell_1}\}, \quad \sum_{\ell=1}^{\ell_2} \nu_\ell = \theta(i,i_1).$

Let's give some data:

1. Let $A_1(i,i_1)$ also $A_2(i,i_1)$ there are any natural numbers and sets $R, M_1,..., M_{\theta(i,i_1)}$ are formed from elements of set $[0, A_1(i,i_1)] \times [0, A_2(i,i_2)]$. Numbers $A_1(i,i_1)$ and $A_2(i,i_1)$ are those, that:

a) For each pair $(c_1, c_2) \in [0, A_1(i,i_1)] \times [0, A_2(i,i_1)]$ true inequality

$$\left| \{(c_1,c_2) + P_1 \times P_2\} \cap (\bigcup_{\nu=1}^{\theta(i,i_1)} M_\nu) \right| \le \theta(i,i_1) \;;$$

b) If for any pair $(c_1, c_2) \in [0, A_1(i,i_1)] \times [0, A_2(i,i_1)]$ true relation

$$\left| \{(c_1,c_2) + P_1 \times P_2\} \cap (\bigcup_{\nu=1}^{\theta(i,i_1)} M_\nu) \right| = \theta(i,i_1),$$

then found such pair $(\bar{j}, \bar{\tau}) \in L_1(\ell_1) \times L_2(\ell_2)$ at which for all $\alpha = 1,...,\ell_1, \beta = 1,...,\ell_2$ it is carried out $(c_1 + p_1(j_\alpha), c_2 + p_2(\tau_\beta)) \in M_\nu$, where $\nu = \sum_{\ell=1}^{\beta-1} \nu_\ell + \alpha$, and for all $\alpha \notin \{j_1,..., j_{\ell_1}\}$ and $\beta \notin \{\tau_1,...,\tau_{\ell_2}\}$ will be executed $(c_1 + p_1(\alpha), c_2 + p_2(\beta)) \in R$;

c) For each $\bar{j} \in L_1(\ell_1)$ and $\bar{\tau} \in L_2(\ell_2)$ found such $c_1 \in [0, A_1(i,i_1)]$ and $c_2 \in [0, A_2(i,i_1)]$ at which for all $\alpha = 1,...,\ell_1$, $\beta = 1,...,\ell_2$ it is carried out $(c_1 + p_1(j_\alpha), c_2 + p_2(\tau_\beta)) \in M_\nu$, where $\nu = \sum_{\ell=1}^{\beta-1} \nu_\ell + \alpha$, and for all $\alpha \notin \{j_1,..., j_{\ell_1}\}$ and $\beta \notin \{\tau_1,...,\tau_{\ell_2}\}$ will be executed $(c_1 + p_1(\alpha),\ c_2 + p_2(\beta)) \in R$;

2. For every one $\nu \in \{1,...,\theta(i,i_1)\}$ two valued function $z_\ell[n]$ is function with the period $T'_\nu + 1$ and at $\sigma > T'_\nu$ a matrix

$$B_\nu(\sigma) = \left(\prod_{\ell=1}^{\delta_\nu} z_\nu[n - n'_k(\ell)] \right), n = \overline{0,\sigma}, k = \overline{1,|L|}$$

satisfies to conditions of orthogonality, where $(n'_k(1),..., n'_k(\delta_\nu))$ is k - th an element of set $L = \{ (n'(1),..., n'(\delta_\nu)) \,|\, 0 \le n'(1) < ... < n'(\delta_\nu) \le n_0 \}$ and $\delta_\nu = m_{\alpha,\beta}$, and between ν, α and β there is relation $\nu = \sum_{\ell=1}^{\beta-1} \nu_\ell + \alpha$.

3. For all $(n, c_1, c_2) \in [0, T_{i,i_1}] \times [0, A_1(i,i_1)] \times [0, A_2(i,i_1)]$ sequence $\vartheta_{i,i_1}[n, c_1, c_2]$ is defining by follows relation:

$$\vartheta_{i,i_1}[n, c_1, c_2] = \begin{cases} 0 & , \textit{if} \;\; (c_1,c_2) \in R, \\ z_1[n] & , \textit{if} \;\; (c_1,c_2) \in M_1, \\ \dots \; \dots \; \dots \; \dots & \dots \; \dots \; \dots \\ z_{\theta(i,i_1)}[n], & \textit{if} \;\; (c_1,c_2) \in M_{\theta(i,i_1)}, \end{cases}$$

where

$$T_{i,i_1} = \left(\prod_{\nu=1}^{\theta(i,i_1)} (T'_\nu + 1) \right) - 1.$$

Theorem 2. Let for fixed (i, i_1) conditions 1-3 are satisfied and $[0, T_{i,i_1}] \times [0, A_1(i,i_1)] \times [0, A_2(i,i_1)]$ there is area of definition of sequences $\overline{\vartheta}_{i,i_1}[n, c]$. If elements from set $\{T'_\nu + 1 | \nu = 1,..., \theta(i, i_1)\}$ mutually prime numbers, then the matrix $\overline{V_2}(i, i_1)$ satisfies to conditions of orthogonality (6).

References

1. Feyziyev F.G., Faradzeva M.R. The modular sequential machine: The basis results of theory and application (In Russian), "Elm" Publishing House, Baku (2006), 234 p.
2. Feyziyev F.G., Samedova Z.A. A problem of synthesis the binary 3D – nonlinear modular dynamical system// Transaction of Azerbaijan National Academy of Sciences, Series of Physical-Technical and Mathematical Sciences: Informatics and Control Problems, Vol. XXIX, No. 6, 2009, PP. 126-133.