DEMONSTRATIO MATHEMATICA
Vol. XXIX No 1 1996

Zdzisław Grodzki

THE CONTROLLED $(n, \vec{k})$-NETS OF SHIFT-REGISTERS

1. Introduction

The k-shift-registers have been widely used in technics (automatic regulation, radar, coding theory, cryptology, computer technics and many others) for more than forty years. Although the monographs [1, 9] related to this topic have been published, this theory is not complete.

In some applications (especially in coding theory and cryptology) the nets of shift–registers (sequential, parallel or mixed) rather than singular ones have been used [11, 12, 14]. The sequential nets of k-shift-registers have been studied by many authors [2, 3, 4, 5, 10, 13, 15]. Szuster [15] has adopted an algebraical method of [9] to the study of sequential nets of k-shift-registers.

The theory of parallel and parallelly-sequential nets of shift-registers is in the initial stage of development. Only few papers related to singular classes of such nets have been published [6, 7, 8].

The aim of this paper is to introduce a new class $\mathcal{NSR}^n_{\vec{k}}$ ($(\vec{k} = (k_1, \ldots, k_m)$) of the controlled $(n, \vec{k})$-nets of shift-registers (briefly $(n, \vec{k})$-nets). This class covers over the deterministic as well as the nondeterministic $(n, \vec{k})$-nets. The subclas $\overline{\mathcal{NSR}}^n_{\vec{k}}$, of $\mathcal{NSR}^n_{\vec{k}}$ will be distinguished and briefly characterized. Every $(n, \vec{k})$-net $N_{n,\vec{k}}$ of this subclass determines the sequential $(1, \vec{k})$-nets $N^j_{1,\vec{k}}$ $(j = 1, 2, \ldots, n)$, also deterministic or nondeterministic, such that each $N^j_{1,\vec{k}}$ computes an infinite sequence T_j over an alphabet A and $(T_1, \ldots, T_n)$ is a computation of the $(n, \vec{k})$-net $N_{n,\vec{k}}$.

Every $(n, \vec{k})$-net $N_{n,\vec{k}}$ can be characterized by the set of all its computations which are the n-tuples $(T_1, \ldots, T_n)$ of infinite sequences, each over an alphabet A.

A necessary and sufficient condition for a nonempty set $\mathbf{E} \subseteq (A^\omega)^n$ to be the computation set of any $(n, \vec{k})$-net of $\mathcal{NSR}^n_{\vec{k}}$ will be formulated.

The periodicity problem of the computation sets will be investigated too.

A class $\mathcal{GNSR}_{\vec{k}}^{n}$ of the graph controlled $(n,\vec{k})$-nets of shift-registers will be also introduced. The relationship between the classes of computation sets of the $(n,\vec{k})$-nets of $\mathcal{NSR}_{\vec{k}}^{n}$ and $\mathcal{GNSR}_{\vec{k}}^{n}$ will be established.

2. Preliminaries

The set of all positive integers will be denoted by N. For a nonempty finite alphabet A and a number $k \geq 1$ the elements of $(A^k)^n$ will be written in the form $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_n)$, $\mathbf{y} = (\mathbf{y}_1, \ldots, \mathbf{y}_n)$ and $\mathbf{z} = (\mathbf{z}_1, \ldots, \mathbf{z}_n)$.

The set of all infinite sequences over A will be denoted by A^ω and its elements (resp. subsets) by upper case Latin letters T, U, V, W (resp. E, F).

For $n \geq 1$, $(A^\omega)^n$ will denote the n-th Cartesian product of A^ω. The elements (resp. subsets) of $(A^\omega)^n$ will be denoted by upper case boldface Latin letters.

The symbols A_{pd}^{ω} and $(A_{pd}^{\omega})^n$ will denote the subsets of A^ω and $(A^\omega)^n$ of all periodic sequences.

For $T = t_1, t_2, \ldots \in A^\omega$ and $1 \leq i \leq j$, $T[i,j]$ will denote the restricted sequence $t_i, \ldots, t_j$ and $T[i,\infty)$ — the infinite sequence $t_i, t_{i+1}, \ldots$ For brevity we shall write $T[i]$ instead of $T[i,i]$.

For $\mathbf{T}=(T_1, \ldots, T_n) \in (A^\omega)^n$, and $1 \leq i \leq j$, $\mathbf{T}[i,j]$ will denote the vector $(T_1[i,j], \ldots, T_n[i,j])$ and $\mathbf{T}[i,\infty]$ — the infinite sequence $(T_1[i,\infty], \ldots, T_n[i,\infty])$; $\mathbf{T}[i]$ will denote $\mathbf{T}[i,i]$.

Let us introduce at the end some auxiliary notions.

A sequence $T = t_1, t_2, \ldots \in A^\omega$ is said to be *almost periodic* iff there exist the numbers $j, p \in N$ such that

$$\forall (i \geq p) \quad (t_{i+j} = t_i).$$

If the above equality holds for $p = 1$ then T is said to be *periodic* and $t_1, \ldots, t_j$, with the minimal j, is said to be its *period*. In this case T will be denoted by $(t_1, \ldots, t_j)_\infty$. On the other hand T is said to be *aperiodic* if it is not almost periodic. A notion of almost periodicity can be analogously introduced for the sequences of $(A^\omega)^n$.

3. Basic definitions

Let $k_1, \ldots, k_m, n$ be the arbitrary positive integers and $\vec{k} = (k_1, \ldots, k_m)$.

Every *controlled* $(n,\vec{k})$*-net of shift-registers* $N_{n,\vec{k}}$ (briefly $(n,\vec{k})$-net) is a triple (A, Φ, Ψ), where $\Phi = \{\Phi_1^{k_1}, \ldots, \Phi_m^{k_m}\}$ $(m \geq 1)$ and every $\Phi_i^{k_i}$ $(1 \leq i \leq m)$ is a nonempty set consisting of the total functions of A^{k_i} into A (the feedback functions of $N_{n,\vec{k}}$) and Ψ is a control. A control Ψ is a partial

function of $((A^{k_1})^n \cup \ldots \cup (A^{k_m})^n) \times N$ into $2^{(\Phi_1^{k_1})^n \cup \ldots \cup (\Phi_m^{k_m})^n} - \{\emptyset\}$ such that for all $k_i, k_j \in \{k_1, \ldots, k_m\}$, $\mathbf{x}_1 \in (A^{k_j})^n$, $\mathbf{x} \in (A^{k_i})^n$ and $p \geq 1$, if $(\mathbf{x}_1, 1) \in D_\Psi$, $(\mathbf{x}, p) \in D_\Psi$ then we have[1]: $\Psi(\mathbf{x}_1, 1) \subseteq 2^{(\Phi_j^{k_j})^n}$, $\Psi(\mathbf{x}, p) \subseteq 2^{(\Phi_i^{k_i})^n}$ and additionally the power condition holds:

$$k_i \leq k_j + p. \tag{1}$$

The vectors $\mathbf{x}_1$ and $\mathbf{x}$ as above are called *the states* of $N_{n,\vec{k}}$ at the moment 1 and p, respectively.

If the control Ψ is a function of $((A^{k_1})^n \cup \ldots \cup (A^{k_m})^n) \times N$ into $(\Phi_1^{k_1})^n \cup \ldots \cup (\Phi_m^{k_m})^n$ then $N_{n,\vec{k}}$ is said to be *deterministic,* otherwise *a nondeterministic* one.

Let $\overline{\mathcal{NSR}}_{\vec{k}}^n$ denote a subclass of $\mathcal{NSR}_{\vec{k}}^n$ of all $(n, \vec{k})$-nets such that their controls are the total functions of N into $2^{(\Phi_1^{k_1})^n \cup \ldots \cup (\Phi_m^{k_m})^n} - \{\emptyset\}$.

The classes $\mathcal{NSR}_{\vec{k}}^1$, $\overline{\mathcal{NSR}}_{\vec{k}}^1$ will be denoted simply by $\mathcal{NSR}_{\vec{k}}$, $\overline{\mathcal{NSR}}_{\vec{k}}$ and their elements will be called the sequential $\vec{k}$-nets.

The deterministic subclasses of the classes mentioned above will be denoted by the same symbols which are preceeded by the letter $\mathcal{D}$.

$\overline{\mathcal{PDNSR}}_{\vec{k}}^n$ will denote a subclass of $\overline{\mathcal{DNSR}}_{\vec{k}}^n$ of all deterministic $(n, \vec{k})$-nets with the periodic controls.

Let us look on the $(n, \vec{k})$-nets as on the technical objects.

Every $(n, \vec{k})$-net $N_{n,\vec{k}}$ of $\mathcal{NSR}_{\vec{k}}^n$ consists of n memories $M_1, \ldots, M_n$, each with k cells ($k = \max\{k_1, \ldots, k_m\}$), where symbols of a nonempty alphabet A can be stored. As has been said, a net $N_{n,\vec{k}}$ is equipped with the nonempty sets $\Phi_1^{k_1}, \ldots, \Phi_m^{k_m}$ of feedback functions and with a control Ψ. Let us suppose that the control Ψ assigns to a state $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_n) \in (A^{k_i})^n$ and a moment $p \geq 1$ a nonempty subset of vectors of $(\Phi_i^{k_i})^n$ which will be used to obtain the new states (or a unique state in a deterministic case) of $N_{n,\vec{k}}$ at the moment $p + 1$. The content of all cells of every memory M_q, $1 < q \leq n$, is moved one place leftward and simultaneously the value $\varphi_q(\mathbf{x}_q)$ is inserted in the last cell of M_q, where $(\varphi_1, \ldots, \varphi_n)$ is one of the vectors of $\Psi(\mathbf{x}, p)$. A vector $\mathbf{y} = (\mathbf{y}_1, \ldots, \mathbf{y}_n) \in (A^{k_j})^n$ whose all components are inserted in the last k_j cells of the memories $M_1, \ldots, M_n$ is a state of $N_{n,\vec{k}}$ at the moment $p + 1$, where $(\mathbf{y}, p + 1) \in D_\Psi$.

But it is possible to give another characterization of the $(n, \vec{k})$-nets. If we add the right-hand side infinite tape $\mathcal{T}_i$ to every memory M_i, $1 \leq i \leq n$, and note on it the initial state of M_i and the elements of the alphabet A which

[1] D_Ψ denotes the domain of Ψ

appear in the last cell of M_i in the successive moments, then the content of $\mathcal{T}_1 \times \ldots \times \mathcal{T}_n$ is said to be a computation of $N_{n,\vec{k}}$.

Now let us define (inductively) *a computation* $\mathbf{T} = (T_1, \ldots, T_n) \in (A^\omega)^n$ of a $(n, \vec{k})$-net $N_{n,\vec{k}} = (A, \{\Phi_1^{k_1}, \ldots, \Phi_m^{k_m}\}, \Psi) \in \mathcal{NSR}_{\vec{k}}^n$ as follows:

(1) For arbitrary $\mathbf{x} \in (A^{k_i})^n$ $(1 \leq i \leq n)$, if $(\mathbf{x},1) \in D_\Psi$ then we put $\mathbf{T}[1, k_i] = \mathbf{x}$;

(2) Let us suppose that $\mathbf{T}[1,p]$ for some $p \geq k_i$ has been defined; if

$$\Psi(\mathbf{T}[p - k_j + 1, p], p - k_j + 1) \subseteq 2^{(\Phi_j^{k_j})^n}$$

for some $1 \leq j \leq m$ then we put

$$T_q[p+1] = \varphi_{i_q}(T_q[p - k_j + 1, p])$$

for all $1 \leq q \leq n$, where $(\varphi_{i_1}, \ldots, \varphi_{i_n})$ is any vector of

$$\Psi(\mathbf{T}[p - k_j + 1, p], p - k_j + 1).$$

The set of all computations of $N_{n,\vec{k}}$, called its *computation set*, will be denoted by $\mathrm{C}(N_{n,\vec{k}})$.

Let us see few examples illustrating the above notions.

EXAMPLE 3.1. Let us define two deterministic $(i,(2,3))$-nets $(i = 1,2)$

$$N_{i,(2,3)} = (\{0,1\}, \{\Phi_1^2, \Phi_2^3\}, \Psi_i) \in \mathcal{DNSR}_{(2,3)}^i,$$

where $\Phi_1^2 = \{\varphi_1, \varphi_2\}$ and $\Phi_2^3 = \{\varphi_3, \varphi_4\}$, as follows:

x	$\varphi_1(\mathbf{x})$	$\varphi_2(\mathbf{x})$	y	$\varphi_3(\mathbf{y})$	$\varphi_4(\mathbf{y})$
0 0	0	1	000	0	1
0 1	0	1	001	0	1
1 0	1	0	010	1	0
1 1	1	0	011	0	1
			100	1	0
			101	1	0
			110	0	1
			111	1	0

The controls Ψ_1 and Ψ_2 are defined as follows:

$$\Psi_1(\mathbf{y}_1, 2p+1) = \begin{cases} \varphi_3 & \text{if } S_1(\mathbf{y}_1) \\ \varphi_4 & \text{otherwise} \end{cases}$$

$$\Psi_1(\mathbf{x}_1, 2p+2) = \begin{cases} \varphi_1 & \text{if } R_1(\mathbf{x}_1) \\ \varphi_2 & \text{otherwise} \end{cases}$$

$$\Psi_2(\mathbf{y}_2, 4p+1) = \begin{cases} (\varphi_3, \varphi_4) & \text{if } S_2(\mathbf{y}_2) \\ (\varphi_4, \varphi_4) & \text{otherwise} \end{cases}$$

$$\Psi_2(\mathbf{x}_2, 4p+2) = \begin{cases} (\varphi_1, \varphi_2) & \text{if } R_2(\mathbf{x}_2) \\ (\varphi_2, \varphi_1) & \text{otherwise} \end{cases}$$

$$\Psi_2(\mathbf{y}_2, 4p+3) = \begin{cases} (\varphi_4, \varphi_3) & \text{if } S_2(\mathbf{y}_2) \\ (\varphi_3, \varphi_3) & \text{otherwise} \end{cases}$$

$$\Psi_2(\mathbf{x}_2, 4p+4) = \begin{cases} (\varphi_2, \varphi_1) & \text{if } R_2(\mathbf{x}_2) \\ (\varphi_1, \varphi_2) & \text{otherwise} \end{cases}$$

for all $\mathbf{x}_1 \in \{0,1\}^2$, $\mathbf{y}_1 \in \{0,1\}^3$, $\mathbf{x}_2 \in \{0,1\}^2 \times \{0,1\}^2$, $\mathbf{y}_2 \in \{0,1\}^3 \times \{0,1\}^3$ and $p \geq 0$, where $S_i(\mathbf{y}_i)$ iff the last elements of all sequences of $\mathbf{y}_i$ are equal to 0 and $R_i(\mathbf{x}_i)$ iff the last elements of all sequences of $\mathbf{x}_i$ are equal to 1.

Then all computations of both $(i,(2,3))$-nets are almost periodic. For example, one of the computations of $N_{1,(2,3)}$ has the form $001110(01)_\infty$ and of $N_{2,(2,3)}$ — $(00(001010011100)_\infty, 00(010111111011)_\infty)$.

EXAMPLE 3.2. Let us define a deterministic sequential (3,2)-net $N_{(3,2)} = (\{0,1\}, \{\Phi_1^2, \Phi_2^3\}, \Psi)$ where Φ_1^2, Φ_2^3 are the same as in Example 3.1; the control Ψ is the aperiodic sequence of the form:

$$\varphi_3\varphi_1\varphi_4\varphi_2\varphi_3\varphi_3\varphi_1\varphi_1\varphi_4\varphi_4\varphi_2\varphi_2\varphi_3\varphi_3\varphi_3\varphi_1\varphi_1\varphi_1\varphi_4\varphi_4\varphi_4\varphi_2\varphi_2\varphi_2\varphi_3 \cdots$$

All computations of $N_{3,2}$ are aperiodic as well.

EXAMPLE 3.3. Let us define the nondeterministic (2,(2,3))-net $N_{2,(2,3)} = (\{0,1\}, \{\Phi_1^2, \Phi_2^3\}, \Psi_2) \in \overline{\mathcal{NSR}}^2_{(2,3)}$ as follows: Φ_1^2, Φ_2^3 are the same as in Example 3.1; the control Ψ_2 is a function of N into $2^{(\Phi_1^2)^2 \cup (\Phi_2^3)^2} - \{\emptyset\}$ such that:

$$\Psi_2(4p+1) = \{(\varphi_3, \varphi_4), (\varphi_4, \varphi_4)\}, \quad \Psi_2(4p+2) = \{(\varphi_1, \varphi_2), (\varphi_2, \varphi_1)\},$$
$$\Psi_2(4p+3) = \{(\varphi_4, \varphi_3), (\varphi_3, \varphi_3)\}, \quad \Psi_2(4p+4) = \{(\varphi_2, \varphi_1), (\varphi_1, \varphi_2)\},$$

for all $p \geq 0$. One can easily verify that $\mathrm{C}(N_{2,(2,3)})$ is infinite.

4. Synthesis problem of the $(n, \vec{k})$-nets

At the beginning a necessary and sufficient condition for a nonempty set $\mathbf{E} \subseteq (A^\omega)^n$ to be the computation set of any $(n, \vec{k})$-net of $\mathcal{NSR}^n_{\vec{k}}$ will be given.

Then three aspects of the synthesis problem will be considered.

THEOREM 4.1. *A nonempty set $\mathbf{E} \subseteq (A^\omega)^n$ is the computation set of any $(n, \vec{k})$-net of $\mathcal{NSR}^n_{\vec{k}}$ iff there exists a sequence $k_{i_1}, k_{i_2}, \ldots \in \{k_1, \ldots k_m\}^\omega$ satisfying the power condition* (1) *of Section* 3 *such that*

(1) *For every* $\mathbf{y} \in (A^{k_{i_1}})^n$ *there exists a sequence* $\mathbf{X} \in \mathbf{E}$ *such that* $\mathbf{y} = \mathbf{X}[1, k_{i_1}]$;

(2) $(\forall \mathbf{X} \in \mathbf{E})(\forall \mathbf{Y} \in \mathbf{E})(\forall j \geq 1)(\mathbf{X}[j, j + k_{i_j} - 1] = \mathbf{Y}[j, j + k_{i_j} - 1] \Rightarrow$
$\Rightarrow Suc_{\mathbf{E}}\mathbf{X}[j, j + k_{i_j} - 1] = Suc_{\mathbf{E}}\mathbf{Y}[j, j + k_{i_j} - 1])$
where $Suc_{\mathbf{E}}\mathbf{X}[p, q] = \{\mathbf{Z}[q + 1] : \mathbf{Z} \in \mathbf{E} \ \& \ \mathbf{Z}[p, q] = \mathbf{X}[p, q]\}$;

(3) $(\forall \mathbf{X} \in \mathbf{E})(\forall \mathbf{Y} \in \mathbf{E})(\forall j \geq 1)(\mathbf{X}[j, j + k_{i_j} - 1] = \mathbf{Y}[j, j + k_{i_j} - 1] \Rightarrow$
$\Rightarrow \mathbf{X}[1, j + k_{i_j} - 1]\mathbf{Y}[j + k_{i_j}, \infty] \in \mathbf{E})$.

THEOREM 4.2. *A nonempty set* $\mathbf{E} \subseteq (A^\omega)^n$ *is the computation set of any* $(n, \vec{k})$*-net of* $\overline{\mathcal{NSR}}^n_{\vec{k}}$ *iff there exists a sequence* $k_{i_1}, k_{i_2}, \ldots \in \{k_1, \ldots k_m\}^\omega$ *satisfying the power condition* (1) *of Section* 3 *such that the conditions* (1) *and* (2) *of Theorem* 4.1 *and the following one are satisfied*:

(4) $(\forall \mathbf{X} \in \mathbf{E})(\forall \mathbf{Y} \in \mathbf{E})(\forall j \geq 1)(\mathbf{X}[j, j + k_{i_j} - 1] = \mathbf{Y}[j, j + k_{i_j} - 1] \Rightarrow$
$(|Suc_{\mathbf{E}}(\mathbf{X}[j, j + k_{i_j} - 1]| = |Suc_{\mathbf{E}}\mathbf{Y}[j, j + k_{i_j} - 1]|)$,

where $|\mathbf{F}|$ *denotes the cardinality of* $\mathbf{F}$.

COROLLARY 4.1. *For arbitrary vector* $\vec{k}$ *and* $n \in N$ *the following inclusion holds*:

$$C(\overline{\mathcal{NSR}}^n_{\vec{k}}) \subseteq C(\mathcal{NSR}^n_{\vec{k}}),$$

where $C(\overline{\mathcal{NSR}}^n_{\vec{k}})$ *and* $C(\mathcal{NSR}^n_{\vec{k}})$ *denote the classes of the computation sets of all the* $(n, \vec{k})$*-nets of* $\overline{\mathcal{NSR}}^n_{\vec{k}}$ *and* $\mathcal{NSR}^n_{\vec{k}}$, *respectively.*

Remark 4.1. The proofs of necessity of both above theorems are obvious. For the proof of sufficiency we have to verify if the conditions (1)–(3) of Theorem 4.1 (or the condition (1), (2), (4) of Theorem 4.2) are satisfied. But this verification is ineffective even in the case when all components of the sequences of $\mathbf{E}$ are defined by means of recursive functions. In the majority of cases a construction of respective $(n, \vec{k})$-nets is also ineffective. Therefore we omit the proofs of both theorems. The solution of the synthesis problems which will be formulated below allows to construct (effectively) the $(n, \vec{k})$-nets with the prescribed properties.

Let us state three synthesis problems $SP^n_{\vec{k}}$ and $SP^{n;i}_{\vec{k}}$ for i=1,2, as follows:

$SP^n_{\vec{k}}$: For a finite set $\mathbf{E} \subseteq (A^\omega_{pd})^n$ whose elements are defined by means of their periods we have to decide if there exists a $(n, \vec{k})$-net $N_{n,\vec{k}} \in \overline{\mathcal{DNSR}}^n_{\vec{k}}$ such that $\mathbf{E}$=C($N_{n,\vec{k}}$).

$SP^{n;1}_{\vec{k}}$: For a finite set $\mathbf{E} \subseteq (A^\omega_{pd})^n$ whose elements are defined by means of their periods and a set $\Phi = \{\Phi_1^{k_1}, \ldots, \Phi_m^{k_m}\}$ we have to decide if there exists a $(n, \vec{k})$-net $N_{n,\vec{k}} = (A, \Phi, \Psi) \in \overline{\mathcal{DNSR}}^n_{\vec{k}}$ such that $\mathbf{E} = C(N_{n,\vec{k}})$.

$SP^{n;2}_{\vec{k}}$: For a finite set $\mathbf{E} \subseteq (A^{\omega}_{pd})^n$ whose elements are defined by means of their periods and a function

$$\Psi : N \to (\Phi_1^{k_1})^n \cup \ldots, \cup (\Phi_m^{k_m})^n$$

we have to decide if there exists a $(n, \vec{k})$-net $N_{n,\vec{k}} = (A, \{\Phi_1^{k_1}, \ldots, \Phi_m^{k_m}\}, \Psi) \in \overline{\mathcal{DNSR}}^n_{\vec{k}}$ such that $\mathbf{E} = C(N_{n,\vec{k}})$.

If the answer on the above problems is positive then a construction of respective $(n, \vec{k})$ – nets should be done.

To prove the decidability of the problems $SP^n_{\vec{k}}$ and $SP^{n;i}_{\vec{k}}$ $(i = 1, 2)$ we have to verify if the conditions **(1)**, **(2)**, **(3)** of the Theorem 4.1 (or the conditions **(1)**, **(2)**, **(4)** of Theorem 4.2) are satisfied. The effectiveness of this verification follows from the fact that $\mathbf{E} \subseteq (A^{\omega}_{pd})^n$ is finite and its elements are defined by means of their periods.

The same synthesis problems for the class of sequential nets of shift-registers have been solved by the author [5]. Therefore we omit the solution of the above problems.

5. Periodicity problems for the $(n, \vec{k})$-nets

The following periodicity problems $PP^n_{\vec{k}}$ and $\overline{PP}^n_{\vec{k}}$ for the class $\overline{\mathcal{PDNSR}}^n_{\vec{k}}$ of the deterministic $(n, \vec{k})$-nets with the periodic controls will be considered:

$PP^n_{\vec{k}}$: How can the feedback functions of a $(n, \vec{k})$-net $N_{n,\vec{k}} \in \overline{\mathcal{PDNSR}}^n_{\vec{k}}$ be like for all its computations to be periodic;

$\overline{PP}^n_{\vec{k}}$: We have to decide if for arbitrary $(n, \vec{k})$-net $N_{n,\vec{k}} \in \overline{\mathcal{PDNSR}}^n_{\vec{k}}$ all its computations are periodic.

Only the problem $PP^n_{\vec{k}}$, with $\vec{k} = (k_1)$, will be solved. The general problem $PP^n_{\vec{k}}$ we leave as open. On the other hand it will be shown that $\overline{PP}^n_{\vec{k}}$ is decidable.

LEMMA 5.1. *Let $N_{n,\vec{k}} = (A, \{\Phi_1^{k_1}, \ldots, \Phi_m^{k_m}\}, \Psi)$ be an arbitrary $(n, \vec{k})$-net of $\overline{\mathcal{PDNSR}}^n_{\vec{k}}$. Then all its computations are almost periodic with the period length less than or equal to*

$$q = \sum_{i=1}^{n} |\Phi_i^{k_i}|^n \cdot |A^{k_i}|^n.$$

Proof is obvious.

Remark 5.1. If the controls of the $(n, \vec{k})$-nets are aperiodic then in majority of casses their computations are aperiodic as well. But there are the $(n, \vec{k})$-nets of $\overline{\mathcal{DNSR}}^n_{\vec{k}}$ with aperiodic controls such that all their computations are almost periodic.

EXAMPLE 5.1. Let us define a $(3,(2))$-net $N_{3,(2)} = (\{0,1\}, \Phi^2, \Psi)$ with $\Phi^2 = \{\varphi_1, \varphi_2\}$ where

x	φ_1(x)	φ_2(x)
0 0	0	0
0 1	1	0
1 0	0	0
1 1	1	1

and with the control Ψ which is an aperiodic sequence of the form:

$$(\varphi_1,\varphi_2,\varphi_1),(\varphi_2,\varphi_1,\varphi_2),(\varphi_1,\varphi_2,\varphi_1),$$
$$(\varphi_1,\varphi_2,\varphi_1),(\varphi_2,\varphi_1,\varphi_2),(\varphi_2,\varphi_1,\varphi_2),\ldots$$

One can easily verify that all computations of $N_{3,(2)}$ are almost periodic with the period length of 1.

LEMMA 5.2. *Let $N_{n,(k)} = (A, \Phi^k, \Psi)$ be a $(n,(k))$-net of $\overline{\mathcal{DNSR}}^n_{(k)}$, with a periodic control. Then all computations of $N_{n,(k)}$ are periodic iff the following condition is satisfied*:

(1) *For every function $\varphi \in \Phi^k$ we have*:

$$(*) \qquad \varphi(at_2\ldots t_k) \neq \varphi(bt_2\ldots t_k)$$

for all $t_2\ldots t_k \in A^{k-1}$, $a,b \in A$ and $a \neq b$.

Proof. Let $N_{n,(k)} = (A, \Phi^k, \Psi)$ be a $(n,(k))$-net with the periodic control and $\mathbf{E} = \mathrm{C}(N_{n,(k)})$. Then $N_{n,(k)}$ determines an existence of a unique sequence $N^j_{1,(k)} = (A, \Phi^k_j, \Psi_j)$ $(j = 1,2,\ldots,n)$ of the sequential $(1,(k))$-nets such that

$$\Psi_j(p) = \{\varphi_j : (\exists\varphi_1,\ldots,\varphi_n \in \Phi^k)((\varphi_1,\ldots,\varphi_n) \in \Psi(p))\}, p \geq 1,$$
$$\Phi^k_j = \{\varphi \in \Phi^k : \varphi \in Rg(\Psi_j)\}, \text{ where } Rg(\Psi_j) \text{ denotes the range of } \Psi_j.$$

Obviously we have

$$\Phi^k = \bigcup_{j=1}^{n} \Phi^k_j.$$

and $\mathbf{E} = E_1 \times \ldots \times E_n$, where $E_j = \mathrm{C}(N^j_{1,(k)})$ for $1 \leq j \leq n$.

As it has been shown in [3] $E_j \subseteq A^{\omega}_{pd}$ iff the condition $(*)$ holds for all functions $\varphi \in \Phi^k_j$. Then $\mathbf{E} \subseteq (A^{\omega}_{pd})^n$ iff the condition $(*)$ is satisfied for the whole set Φ^k. ■

Remark 5.2. For arbitrary $(n,\vec{k})$-net $N_{n,\vec{k}} = (A, \{\Phi^{k_1}_1,\ldots,\Phi^{k_m}_m\}, \Psi) \in \overline{\mathcal{PDNSR}}^n_{\vec{k}}$ the previous condition (1) has the form:

(2) For every $1 \leq j \leq m$ and a function $\varphi \in \Phi_j^{k_j}$ the following condition holds

$$(**) \qquad \varphi(a\mathbf{x}) \neq \varphi(b\mathbf{x})$$

for all $\mathbf{x} \in A^{k_j - 1}$, $a, b \in A$ and $a \neq b$.

The condition (2) does not imply the periodicity of all computations of the $(n, \vec{k})$-nets (see Example 3.1). On the other hand there are the $(n, \vec{k})$-nets having only periodic computations for which the condition (2) is not satisfied.

EXAMPLE 5.2. Let us define a sequential (2,4)-net

$$N_{1,(2,4)} = (\{0,1\}, \{\Phi_1^2, \Phi_2^4\}, \Psi) \in \overline{\mathcal{DNSR}}_{(2,4)},$$

as follows:

$$\Phi_1^2 = \{\varphi_1, \varphi_2\} \quad \text{and} \quad \Phi_2^4 = \{\varphi_3, \varphi_4\},$$

$$\varphi_1(\mathbf{x}) = 0, \ \varphi_2(\mathbf{x}) = 1 \text{ for all } \mathbf{x} \in \{0,1\}^2,$$

$$\varphi_3(\mathbf{y}) = 0, \ \varphi_4(\mathbf{y}) = 1$$

$$\text{for } \mathbf{y} \in \{0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111\},$$

$$\varphi_3(\mathbf{z}) = 1, \ \varphi_4(\mathbf{z}) = 0 \text{ for the remaining } \mathbf{z} \in \{0,1\}^4$$

$$\Psi(1) = \varphi_1, \Psi(2) = \varphi_2, \Psi(3p+3) = \varphi_3, \Psi(3p+4) = \varphi_4, \Psi(3p+5) = \varphi_3,$$

for all $p \geq 0$. It is easy to see that there exists a $(1,(4))$-net $N_{1,(4)} = (\{0,1\}, \Phi_2^4, \Psi_1)$ with $\Psi_1(3p+i) = \Psi(3p+i+3)$, $p \geq 0$ and $i = 1,2,3$, such that $\mathbf{E} = \mathrm{C}(N_{1,(2,4)}) \subseteq \mathrm{C}(N_{1,(4)}) = \mathbf{E}_1$. As Ψ_1 is periodic and for all functions of Φ_2^4 the condition (2) holds then $\mathbf{E}_1$ consists of only periodic sequences. Although the control Ψ is almost periodic with the nonempty tail and for the functions φ_1, φ_2 the condition (2) is not satisfied but all computations of $N_{1,(2,4)}$ are periodic, because $\mathbf{E} \subseteq \mathbf{E}_1$.

Remark 5.3. Example 5.2 inspires a method of construction of a $\overline{\mathcal{DNSR}}_{\vec{k}}^n$ subclass of the $(n, \vec{k})$-nets with almost periodic controls and for which the condition (2) of Remark 5.2 is not satisfied but having only periodic computations.

Let us solve at the end the problem $\overline{PP}_{\vec{k}}^n$.

LEMMA 5.3. *The problem $\overline{PP}_{\vec{k}}^n$ is decidable for the class $\overline{\mathcal{PDNSR}}_{\vec{k}}^n$*

Proof. Let $N_{n,\vec{k}} = (A, \{\Phi_1^{k_1}, \ldots, \Phi_m^{k_m}\}, \Psi)$ be an arbitrary $(n, \vec{k})$-net of $\overline{\mathcal{PDNSR}}_{\vec{k}}^n$. As all computations of $N_{n,\vec{k}}$ are almost periodic with the period length less than or equal to q, where

$$q = \sum_{i=1}^{m} |A^{k_i}|^n \cdot |\Phi_i^{k_i}|^n,$$

then we are able to define a q-register $R_q = (A^q, \pi)$ such that $C(N_{n,\vec{k}}) \subseteq C(R_q)$. We define a function $\pi : (A^q)^n \to A^n$ as follows:

$$\pi(\mathbf{X}[i, i+q-1] = \mathbf{X}[i+q] \text{ for all } \mathbf{X} \in \mathbf{E} \text{ and } i \geq 1.$$

Then we verify if for all $\mathbf{x} \in (A^{q-1})^n$, $\mathbf{a}, \mathbf{b} \in A^n$ $(\mathbf{a} \neq \mathbf{b})$ such that $(\mathbf{ax}) \in D_\pi$, $(\mathbf{bx}) \in D_\pi$ we have

$$\pi(\mathbf{ax}) \neq \pi(\mathbf{bx})$$

As the above verification is effective therefore $\overline{PP}^n_{\vec{k}}$ is decidable. ■

6. The graph controlled $(n, \vec{k})$-nets of shift registers

By *a graph controlled* $(n, \vec{k})$-net of shift registers (briefly $(n, \vec{k})$-gnet) we mean a triple $GN_{n,\vec{k}} = (A, \Phi, G^n_{\vec{k}})$ where

(1) $\Phi = \{\Phi_1^{k_1}, \ldots, \Phi_m^{k_m}\}$ is the set of functions as previously;

(2) $G^n_{\vec{k}}$ is a directed labelled graph such that

(2.1) the set $\mathbf{V}$ of its vertices is equal to Φ;

(2.2) an edge going from a vertex $\Phi_i^{k_i}$ to a vertex $\Phi_j^{k_j}$ is labelled by an n – tuple of the indexes of feedback functions of $\Phi_i^{k_i}$.

$G^n_{\vec{k}}$ is said to be a transition graph of $GN_{n,\vec{k}}$. Sometimes the transition graphs will be identified with $(n, \vec{k})$-gnets.

To obtain the infinite computations of such nets we restrict ourselves to the cases when the transition graphs are the cycles or the rooted infinite trees. Additionally for such graphs the following power condition must be satisfied:

PC': for every walk of $G^n_{\vec{k}}$ of the form

(3) $\Phi_{i_1}^{k_{i_1}}, (j_1^1, \ldots, j_n^1), \Phi_{i_2}^{k_{i_2}}, (j_1^2, \ldots, j_n^2), \ldots$ $(k_{i_j} \in \{k_1, \ldots, k_m\}$ for all $j \geq 1)$ the following conditions hold:

(3.1) if $G^n_{\vec{k}}$ is a rooted infinite tree then we have: $k_{i_p} \leq k_{i_1} + p$ for all $p \geq 1$;

(3.2) if $G^n_{\vec{k}}$ is a cycle then we have: $k_{i_{p+1}} = k_{i_p} + 1$ or $k_{i_p} = k_{i_{p+1}} + 1$ or $k_{i_{p+1}} = k_{i_p}$ for all $p \geq 1$.

An $(n, \vec{k})$-gnet $GN_{n,\vec{k}}$ is said to be *deterministic* iff every vertex of its transition graph has a unique outcoming edge. Otherwise $GN_{n,\vec{k}}$ is said to be *nondeterministic*.

An infinite sequence $\mathbf{X} = (T_1, \ldots, T_n) \in (A^\omega)^n$ is said to be *a computation* of an $(n, \vec{k})$-gnet $GN_{n,\vec{k}} = (A, \Phi, G^n_{\vec{k}})$ iff there exists a walk of the form (3) such that for every $p \geq 1$ and $1 \leq q \leq n$ we have:

$$T_q[p + k_{j_q^p}] = \varphi_{j_q^p}(T_q(p, p + k_{j_q^p} - 1]).$$

The set of all computations of $GN_{n,\vec{k}}$ will be denoted, as previously, by $C(GN_{n,\vec{k}})$.

EXAMPLE 6.1. Let us consider a $(3,(2,3))$-gnet $GN_{3,(2,3)}$ which is defined by means of its transition graph $G^3_{(2,3)}$ which is shown in Figure 1, where Φ^2_1 and Φ^2_1 in Example 3.1 have been defined. It is obvious that all computations of $GN_{3,(2,3)}$ are almost periodic.

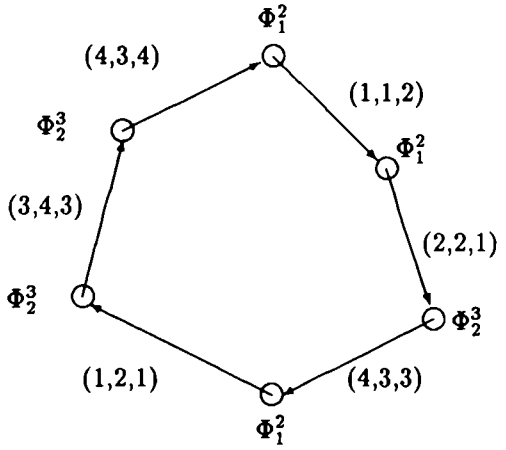

Fig. 1. Transition graph of Example 6.1

EXAMPLE 6.2. Let $GN_{2,(3)}$ be a deterministic $(2,(3))$-gnet such that its transition graph $G^2_{(3)}$ which is a binary infinite tree of the form:

(4) The set of vertices of $G^2_{(3)}$ is equal to $\Phi^3 = \{\varphi_1, \varphi_2, \varphi_3, \varphi_4\}$ where φ_3 and φ_4 are the same as in Example 3.1 and φ_1, φ_2 are defined as follows:

$$\varphi_i(\mathbf{x}) = i - 1 \text{ for all } \mathbf{x} \in \{0,1\}^3 \text{ and } i = 1,2;$$

(5) The edges going to the left and right sons of the root are labelled by (1,3) and (2,4);

(6) If an edge incoming to an arbitrary vertex is labelled by (p,q) then the eges outcoming to the left and right sons are labelled by $(p \oplus 1, q)$ and $(p, q \oplus 1)$, respectively where $\oplus$ is an addition modulo 4.

One can easily show that for $GN_{2,(3)}$ there exists an equivalent $(n,\vec{k})$-net $N_{2,(3)}$ of $\overline{\mathcal{NSR}}^2_3$.

Let $\mathcal{GNSR}^n_{\vec{k}}$ denote the class of all graph controlled $(n,\vec{k})$-gnets and $\mathcal{TNSR}^n_{\vec{k}}$, $\mathcal{CNSR}^n_{\vec{k}}$–the subclasses of $\mathcal{GNSR}^n_{\vec{k}}$ of the $(n,\vec{k})$-nets such that their transition graphs are the rooted trees and the cycles. $C(\mathcal{GNSR}^n_{\vec{k}})$,

$\mathcal{C}(\mathcal{TNSR}_{\vec{k}}^n), \mathcal{C}(\mathcal{CNSR}_{\vec{k}}^n)$ denote the classes of the computation sets of $(n, \vec{k})$-gnets of $\mathcal{GNSR}_{\vec{k}}^n$, $\mathcal{TNSR}_{\vec{k}}^n$ and $\mathcal{CNSR}_{\vec{k}}^n$, respectively.

The following theorem shows the relationship between the classes of computation sets.

THEOREM 6.1. *For arbitrary numbers* $k_1, \ldots, k_m, n \in \mathbf{N}$ *the following relations hold*:

$$\mathcal{C}(\mathcal{TNSR}_{\vec{k}}^n) \subseteq \mathcal{C}(\mathcal{NSR}_{\vec{k}}^n)$$

$$\neg(\mathcal{C}(\mathcal{CNSR}_{\vec{k}}^n) \subseteq \mathcal{C}(\overline{\mathcal{NSR}}_{\vec{k}}^n)).$$

Proof. The first inclusion is obvious. To prove the second one let us observe that the controls of the $(n, \vec{k})$-gnets of $\mathcal{CNSR}_{\vec{k}}^n$ are the finite sets of periodic sequences (because the computations can start from an arbitrary vertex of a transition graph) whereas the controls of $(n, \vec{k})$-nets of $\overline{\mathcal{NSR}}_{\vec{k}}^n$ are the unique sequences, which can be even aperiodic. ∎

Final remarks

This paper is the initial stage of developments on the class $\mathcal{NSR}_{\vec{k}}^n$ of the $(n, \vec{k})$-nets. Only basic properties of the computation sets of such nets have been given. Many problems, such as equivalence and complexity, remain open. It would be also interesting to study a subclass of the binary $(n, \vec{k})$-nets with the linear feedback functions.

The next author's paper will be devoted to a slightly different class of the nets. Adding the identity functions, it is easy to design the nets of this class which realize the Hamiltonian circuits.

References

[1] S. W. Golomb, *Shift-register sequences*, Aecean Park Press, Laguna Hills, California 1982 (Revised edition).

[2] W. A. Golunkov Ju. V., *Shift-register realization of microprogram basses* (In Russian), Kybernetica No 12–13 (1976), 33–39.

[3] Z. Grodzki, *The controlled shift-registers*, Elektron. Informationsverarbeit. Kybernetik 11 (1975), 142–150.

[4] Z. Grodzki, *The controlled iterative systems (deterministic and nondeterministic,)* (In Polish), Prace Inst. Mat-Fiz-Chem, Ser. A, 2 (1981), 1–142.

[5] Z. Grodzki, *Synthesis problem for deterministic controlled* (k, m)*-shift-registers*, Demonstratio Math. 20 (1987), 547–559.

[6] Z. Grodzki and J. Meznik, *Nets of time variant parallel controlled shift-registers*, Knižnice Odborn. Věd. Spisu Vysoké. Učeni Tech. v Brně B–119 (1988), 205–209.

[7] Z. Grodzki, Mikulašek, *Nets of parallel controlled shift-registers*, ibid., 219–226.

[8] Z. Grodzki and P. Siwak, *Relational nets of parallel shift-registers*. Found. Control Engrg. 2 (1981), 61–75.

[9] R. Lidl and H. Niederreiter, *Introduction to finite fields an their applications*, Cambridge Univ. Press, Cambridge 1986.

[10] D. G. Martitas, A. C. Arvilias and A. C. Boanas, *Phase shift-analysis of linear feedback shift-registers structures generating pseudorandom sequences*, IEEE Trans. Computers vol. C-27, No 7 (1978), 660–669.

[11] H. Niederreiter, *Cryptology — The mathematical theory of data security*, Proc. Internat. Symp. on Prospect of Mathematical Science (Tokyo 1986).

[12] W. Paterson, *Cryptology (for mathematicians and computer scientists)*, Rowman and Littefield, Savage, Maryland, 1987

[13] Ch. Ronse, *Feedback shift-registers*, Lecture Notes in Computer Science, 169, Springer Verlag, Berlin 1986.

[14] R. A. Ruppel, *Analysis and Design of Stream Ciphers*, Springer Verlag, Berlin 1986.

[15] J. Szuster, *Analysis of the controlled iterative systems*, (In Polish), Ph.D. thesis, Lublin 1990.

DEPARTMENT OF APPLIED MATHEMATICS
TECHNICAL UNIVERSITY OF LUBLIN
Bernardyńska 13
20-950 LUBLIN, POLAND

Received April 13, 1994.