DEMONSTRATIO MATHEMATICA
Vol. XXXIII No 1 2000

Zdzisław Grodzki

RELATIONSHIP BETWEEN SOME CLASSES OF NONDETERMINISTIC $\vec{k}$-NETS OF PARALLEL CONTROLLED SHIFT-REGISTERS

Abstract. The classes $NNPCR^{I}_{\vec{k}}$ and $NNPCR^{II}_{\vec{k}}$ of nondeterministic parallel controlled $\vec{k}$-nets of shift-registers are introduced. These classes are generalizations of the majority of shift-register nets that have been considered before. It is proved that the finiteness problem for sets definable by the $\vec{k}$-nets of some subclasses of both classes is decidable. Then it is shown that the class of sets definable by $\vec{k}$-nets of $NNPCR^{I}_{\vec{k}}$ is a subclass of the class of sets definable by $\vec{k}$-nets of $NNPCR^{II}_{\vec{k}}$ but the converse relation is not true. On the other hand the classes of all state sequences of the $\vec{k}$-nets of both classes are identical.

At the very end a few open problems are put forward.

1. Introduction

The theory of deterministic shift-registers has been intensively explored for more than forty years. Several monographs related to this topic have been published [1], [2], [9]. Many interesting applications of shift-registers (automatic regulation, coding theory, cryptology, computer technology, integrated circuits, radar and many others) have been completed in [2], [15], [18]. The majority of papers which have been published before are devoted to maximal shift-registers (the sequences generated by them have maximal period lengths). An algebraic method introduced by Zierler [19] has been primarily used to the study of linear shift-registers (the sequences generated by them are called pseudorandom ones). Mykkelweit, Siu and Tong [11] have extended this method to study the nonlinear shift-registers. Furthermore let us mention two dissertations [10], [20] conducted by the author which were devoted to construction of some classes of maximal shift-registers.

An algebraic method has been adopted by Ronse [16] to study the sequential nets of shift-registers (see also [17]). The author has also studied the class of sequential nets of shift-registers [3], [5] (deterministic and nondeterministic). But so far the uniform theory of sequential nets of shift-registers has not been elaborated, many problems remain open.

The theory of parallel and parallel-sequential nets of shift-registers is in initial stage of development. Only few papers related to separate classes of such nets have been published [4], [6]–[8]. The class $DNPCR_{\vec{k}}$ of deterministic $\vec{k}$-nets of parallel controlled shift-registers which has been studied in [6] is a subclass of the classes of nondeterministic $\vec{k}$-nets which are considered here.

The paper [7] is related to the class $\mathcal{GBG}_{\vec{k}}$ of generalized de Bruijn graphs of rank $\vec{k}$. It has been proved that $\mathcal{GBG}_{\vec{k}}$ is connected, Hamiltonian and Eulerian. A simple algorithm, with linear space and time complexities, for the construction of Hamiltonian circuits has been also given in [7]. The paper [8] deals with the class $\overline{DNPCR}_{\vec{k}}$ of the deterministic $\vec{k}$-nets realizing the factors of $\mathcal{GBG}_{\vec{k}}$ (*i.e.* the subgraphs whose all the connected components form the cycles).

The problem of generation of vector pseudorandom sequences has been explored lately by many authors, especially Niederreiter. Wider use of parallelized simulations methods makes the above problem an increasingly important subject. The reader is referred to [12]–[14], where a few methods (multiple matrix-recursive method, inversive one) and references related to this topic are presented.

The aim of this paper is to introduce two classes $NNPCR^{I}_{\vec{k}}$ and $NNPCR^{II}_{\vec{k}}$ of nondeterministic $\vec{k}$-nets of parallel controlled shift-registers (briefly $\vec{k}$-nets), where $\vec{k} = (k_1, \ldots, k_m) \in \mathcal{N}^m$. The classes $NNPCR^{I}_{\vec{k}}$ and $NNPCR^{II}_{\vec{k}}$ can be briefly characterized in such a way that for the first class the controls are single-valued functions while the feedback functions are many-valued but for the second one the controls are many-valued functions while the feedback functions are single-valued.

It is shown that the class of sets definable by the $\vec{k}$-nets of $NNPCR^{I}_{\vec{k}}$ is a subclass of the class of set definable by the $\vec{k}$-nets of $NNPCR^{II}_{\vec{k}}$ but the converse inclusion does not hold.

Finally it is proved that the classes of all state sequences of the $\vec{k}$-nets of both classes $NNPCR^{I}_{\vec{k}}$ and $NNPCR^{II}_{\vec{k}}$ are equal to $(A^{\omega})^m$.

For the $\vec{k}$-nets of both classes mentioned above an essential problem $FD_{\vec{k}}$ is to determine whether the sets definable by them are finite. In this case nondeterminism is inessential. It is shown that the problem $FD_{\vec{k}}$ is decidable for some subclasses of $NNPCR^{I}_{\vec{k}}$ and of $NNPCR^{II}_{\vec{k}}$.

The following reasons motivate introduction of the above classes of the $\vec{k}$-nets:

(1) The majority of technical devices work nondeterministically and it is not possible to eliminate nondeterminism entirely. The problem is to limit them in such a way that devices work almost deterministically;
(2) Every class mentioned above covers over the majority of shift-registers nets which have been considered before;
(3) In majority of applications of shift-registers in technics (especially in production of integrated circuits) they do not occur as self-reliant devices but rather as nets (parallel or parallel-sequential);
(4) A great use of vector pseudorandom sequences in cryptology and during parallel simulation of real processes implies a need to define different kinds of technical devices generating such sequences;
(5) The great interest of vector pseudorandom sequences [12], [13] substantiates direction of the studies on parallel $\vec{k}$-nets.

2. The class $NNPCR^I_{\vec{k}}$ of nondeterministic $\vec{k}$-nets of parallel controlled shift-registers

For an alphabet A ($|A| \geq 2$) and positive integers $k_1, \ldots, k_m$ (not necessarily different) let $V = A^{k_1} \times \ldots \times A^{k_m}$ and $\vec{k} = (k_1, \ldots, k_m)$. V^ω denotes the set of all infinite sequences over V.

Every nondeterministic $\vec{k}$-net $N_{\vec{k}}$ of parallel controlled shift-registers of $NNPCR^I_{\vec{k}}$ (briefly $\vec{k}$-net) is defined as a tuple $(A, \Phi_1^{k_1} \times \cdots \times \Phi_m^{k_m}, \Psi)$, where every $\Phi_j^{k_j}$, $(j = 1, 2, \ldots, m)$ is a set of total functions of A^{k_j} into $2^A \setminus \{\emptyset\}$ and Ψ is a total function of $V \times \mathcal{N}$ into $\Phi = \Phi_1^{k_1} \times \ldots \times \Phi_m^{k_m}$ ($\mathcal{N}$ is the set of all positive integers). Every element of $\Phi_j^{k_j}$ $(j = 1, 2, \ldots, m)$ is called *a feedback function* and Ψ – *the control* of $N_{\vec{k}}$.

If every feedback function of $\Phi_j^{k_j}$ $(j = 1, 2, \ldots, m)$ is a mapping of A^{k_j} into A then the above $\vec{k}$-net $N_{\vec{k}}$ is said to be *deterministic*, otherwise a *strictly nondeterministic* one. For brevity strictly nondeterministic $\vec{k}$-nets will be called *nondeterministic.*

Every vector $x \in V$ is said to be *a state* of $N_{\vec{k}}$.

For arbitrary states $x, y \in V$, $x = (x^1, \ldots, x^m)$, $y = (y^1, \ldots, y^m)$, y is said to be *an immediate successor* of x of $N_{\vec{k}}$ iff $y^j[1, k_j - 1] = x^j[2, k_j]$ for all $j \leq m$ with $k_j > 1$, and there exist $i \geq 1$ as well as $(\varphi_1, \ldots, \varphi_m) \in \Phi$ such that $(\varphi_1, \ldots, \varphi_m) = \Psi(x, i)$ and $y^j[k_j, k_j] = z$ for some $z \in \varphi_j(x^j)$; if $k_j = 1$ then we put $y^j = z \in \varphi_j(x^j)$. [1]

For arbitrary states $x, y \in V$, y is said to be *a successor* of x of $N_{\vec{k}}$ iff

[1] For every $t = t_1 \ldots t_k \in A^k$ and $1 \leq j \leq k$, $t[i, j]$ denotes a restricted sequence $t_i \ldots t_j$.

there exists a sequence $x_1, \ldots, x_n$, $n > 1$, of states such that $x_1 = x, x_n = y$ and x_{i+1} is an immediate successor of x_i of $N_{\vec{k}}$ for $1 \leq i < n$.

An infinite sequence $x = x_1, x_2, \ldots \in V^\omega$ is said to be *a state sequence* of a $\vec{k}$-net $N_{\vec{k}}$ iff every x_{i+1}, $i \geq 1$, is an immediate successor of x_i of $N_{\vec{k}}$.

The set of all state sequences of $N_{\vec{k}}$ is called its *definable set* and denoted by $D(N_{\vec{k}})$.

Let $NNPCR^{I,1}_{\vec{k}}$ and $NNPCR^{I,2}_{\vec{k}}$ be the subclasses of $NNPCR^{I}_{\vec{k}}$ of all $\vec{k}$-nets such that their controls are total functions of V and of $\mathcal{N}$ into Φ, respectively.

Hence the $\vec{k}$-nets of $NNPCR^{I,1}_{\vec{k}}$ are constructed in such a way that the immediate successors of their all states are only determined by these states and are independent of the time moments. The consequence of this fact is that for the identical states occurring in different moments their immediate successors are identical if the vectors of feedback functions assigned to these states by the controls contain only single-valued functions or possible different immediate successors if at least one feedback function is many-valued.

But for the class $NNPCR^{I,2}_{\vec{k}}$ the situation is quite different. In every time-moment a control of a $\vec{k}$-net assigns unique feedback functions vector which will be used to compute the immediate successor of all actual states. The consequence of this fact is that the sets of immediate successors of identical states occurring at the same moment are equal.

REMARK 2.1. One can associate to every $\vec{k}$-net $N_{\vec{k}} = (A, \Phi_1^{k_1} \times \cdots \times \Phi_m^{k_m}, \Psi)$ of $NNPCR^{I,1}_{\vec{k}}$ a digraph $G_{\vec{k}}$ with labelled edges, called *the labelled transition graph* of $N_{\vec{k}}$, as follows:

(1) The nodes of $G_{\vec{k}}$ are all elements of V;
(2) If x and y are arbitrary nodes (not necessarily different) then there exists an edge in $G_{\vec{k}}$ going from x to y and labelled $(i_1, \ldots, i_m)$ iff $\Psi(x) = (\varphi_{i_1}, \ldots, \varphi_{i_m})$ and $y^j = x^j[2, k_j]z^j$ if $k_j > 1$, or $y^j = z^j$ if $k_j = 1$, for all $1 \leq j \leq m$ and some $z^j \in \varphi_{i_j}(x^j)$.

If we remove the labels from $G_{\vec{k}}$ then we obtain *the transition graph* of $N_{\vec{k}}$.

For an illustration of the previous definition let us see two examples.

EXAMPLE 2.2. Let us define nondeterministic $(2,2)$-net $N_{(2,2)} = (\{0,1\}, \{\varphi_1, \varphi_2\} \times \{\pi_1, \pi_2\}, \Psi) \in NNPCR^{I,1}_{(2,2)}$ as follows:

t	$\varphi_1(t)$	$\varphi_2(t)$	$\pi_1(t)$	$\pi_2(t)$
00	$\{0\}$	$\{1\}$	$\{0\}$	$\{1\}$
01	$\{1\}$	$\{0,1\}$	$\{0\}$	$\{1\}$
10	$\{0\}$	$\{1\}$	$\{0\}$	$\{1\}$
11	$\{0\}$	$\{1\}$	$\{0\}$	$\{1\}$

$$\Psi(x) = \begin{cases} (\varphi_1, \pi_1) & \text{if the last elements of all sequences of } x \text{ are equal to } 0 \\ (\varphi_2, \pi_2) & \text{if the last elements of all sequences of } x \text{ are equal to } 1 \\ (\varphi_1, \pi_2) & \text{for the remaining cases.} \end{cases}$$

The labelled transition digraph $G_{(2,2)}$ of $N_{(2,2)}$ has the form presented in Figure 2.1.

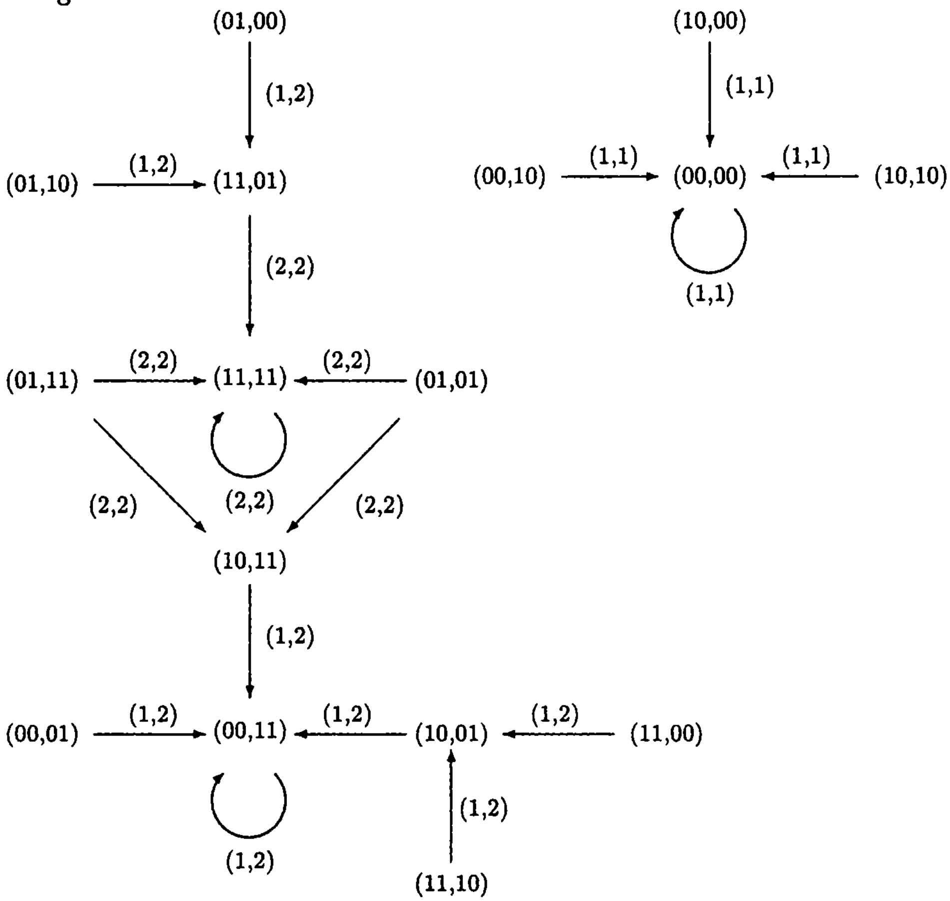

Fig. 2.1. The labelled transition graph $G_{(2,2)}$ of $N_{(2,2)}$.

Looking at the graph $G_{(2,2)}$ one can see that all states, excluding $(01, 11)$ and $(01, 01)$, have unique immediate successors. But the successors of $(01, 11)$ and of $(01, 01)$ form the cycles with cycle lengths equal to 1. The conclusion is that all state sequences of $N_{(2,2)}$ are almost periodic[2] and $|D(N_{(2,2)})| < \aleph_0$.

[2] A sequence $x_1, x_2, \ldots \in V^\omega$ is said to be *almost periodic* iff there are j and p of $\mathcal{N}$ such that $x_i = x_{i+j}$ for all $i \geq p$. If $p = 1$ then above sequence is said to be *periodic* and $x_1, \ldots, x_j$, with minimal j, is said to be its *period*. A sequence $y \in V^\omega$ is said to be *aperiodic* iff it is not almost periodic.

THEOREM 2.3. *For arbitrary $\vec{k}$-net $N_{\vec{k}}$ of $NNPCR^{I,1}_{\vec{k}}$ we are able to decide (effectively) if $|D(N_k)| < \aleph_0$, or not.*

Proof. Let $N_{\vec{k}} = (A, \Phi, \Psi)$ be an arbitrary $\vec{k}$-net of $NNPCR^{I,1}_{\vec{k}}$. Let W be a subset of V of all states $x = (x^1, \cdots, x^m)$ of $N_{\vec{k}}$ with the property: if $\Psi(x) = (\varphi_1, \ldots, \varphi_m)$ for some $(\varphi_1, \ldots, \varphi_m) \in \Phi$ then there exists at least one function φ_i, $1 \le i \le m$, such that $|\varphi_i(x^i)| > 1$. If $E = \emptyset$ then obviously we have $|D(N_k)| < \aleph_0$. Let us suppose that $E \neq \emptyset$ and $x \in E$. To decide if $|D(N_k)| < \aleph_0$ we have to verify if every immediate successor of x has a successor being a node of any cycle C whose every node has unique immediate successor. As V and E are finite then the above verification is effective. □

EXAMPLE 2.4. Let us define nondeterministic $(2,2)$-net $N^1_{(2,2)} = (\{0,1\}, \{\varphi_1, \varphi_2\} \times \{\pi_1, \pi_2\}, \Psi_1)$ of $NNPCR^{I,2}_{(2,2)}$, as follows:

φ_n, π_n, $n = 1, 2$, are the same as in Example 2.2 and

$$\Psi_1(i) = \begin{cases} (\varphi_1, \pi_1) & \text{if } i \text{ is odd;} \\ (\varphi_2, \pi_2) & \text{if } i \text{ is even,} \end{cases}$$

for all $i \ge 1$.

Observe that for a unique feedback function φ_2 and a state 01 we have $\varphi_2(01) = \{0,1\}$ (for the remaining cases the value of every function $\lambda \in \{\varphi_1, \varphi_2, \pi_1, \pi_2\}$ is a unique element of $\{0,1\}$). Let us see that a functions (φ_2, π_2) is only used in even moments but every state $(x, y) \in \{0,1\}^2 \times \{0,1\}^2$ of $N^1_{(2,2)}$ can be transformed by means of (φ_1, π_1) in odd moments into any state (x_1, y_1) such that $x_1 \in \{0,1\}^2 \setminus \{(01)\}$ and $y \in \{0,1\}^2$. The conclusion is that any state $(01, y)$, $y \in \{0,1\}^2$ do not occurs in even moments when the function (φ_2, π_2) would be applied. Hence $N^1_{(2,2)}$ is equivalent to a deterministic $(2,2)$-net $N^2_{(2,2)}$ which is defined analogously as $N^1_{(2,2)}$ with such only difference that $\varphi_2(01) = a$ for some $a \in \{0,1\}$.

The conclusion is that all state sequences of $N^1_{(2,2)}$ are almost periodic with the period length less than or equal to 2^q, $q = k_1 + \cdots + k_m$ and we have $|D(N^1_{(2,2)})| < \aleph_0$.

REMARK 2.5. The situation illustrated in Example 2.4 is the best one for the technical realization of the $\vec{k}$-nets (the nondeterminism is inessential). But it is possible a case that all state sequences generable by the $\vec{k}$-nets are aperiodic (or some of them). This shows the following example.

EXAMPLE 2.6. Let us define a nondeterministic $(2,2)$-net

$N^2_{(2,2)} = (\{0,1\}, \{\varphi_1, \varphi_2\} \times \{\pi_1, \pi_2\}, \Psi_2)$ of $NNPCR^{I,2}_{\vec{k}}$, where $\varphi_n, \pi_n, n = 1, 2$ are the same as in Example 2.2, but a control Ψ_2 is an aperiodic sequence (for instance $(\varphi_1, \pi_1), (\varphi_2, \pi_2), (\varphi_1, \pi_1), (\varphi_2, \pi_2), (\varphi_2, \pi_2), (\varphi_1, \pi_1), (\varphi_2, \pi_2), (\varphi_2, \pi_2), (\varphi_2, \pi_2) \ldots)$

Then $N^2_{(2,2)}$ has surely the aperiodic sequences (possibly all).

REMARK 2.7. For arbitrary feedback function set $\Phi = \Phi_1^{k_1} \times \cdots \times \Phi_m^{k_m}$ one is able to construct an infinite set of the $\vec{k}$-nets of $NNPCR^{I,2}_{\vec{k}}$ having aperiodic state sequences.

Obviously, the definable sets by all such $\vec{k}$-nets are infinite.

Taking into account the above examples we are able to formulate a necessary and sufficient condition for definable by a $\vec{k}$-net set to be finite.

THEOREM 2.8. *For arbitrary $\vec{k}$-net $N_{\vec{k}} = (A, \Phi, \Psi)$ of $NNPCR^{I,2}_{\vec{k}}$, $|D(N_{\vec{k}})| < \aleph_0$ iff the set*

$$(3)\qquad B_{N_{\vec{k}}} = \{(x, j) \in V \times N : (\exists(\varphi_1, \ldots, \varphi_n) \in \Phi)(\exists p \leq m)[\Psi(x, j) = (\varphi_1, \ldots, \varphi_m) \wedge |\varphi_p(x^p)| > 1\}$$

is empty.

Proof is obvious. □

Let $\overline{NNPCR}^{I,2}_{\vec{k}}$ be a subclass of $NNPCR^{I,2}_{\vec{k}}$ such that for all its $\vec{k}$-nets the following condition holds: the set $B_{N_{\vec{k}}}$ assigned to a $\vec{k}$-net $N_{\vec{k}}$ by means of (3) is finite and it is effectively computable.

For the subclass $\overline{NNPCR}^{I,2}_{\vec{k}}$ let us state the *finiteness problem* $F_{\vec{k}}$ as follows:

$F_{\vec{k}}$: For arbitrary $\vec{k}$-net $N_{\vec{k}} \in \overline{NNPCR}^{I,2}_{\vec{k}}$ we have to decide if $|D(N_{\vec{k}})| < \aleph_0$.

COROLLARY 2.9. For the class $\overline{NNPCR}^{I,2}_{\vec{k}}$ the problem $F_{\vec{k}}$ is decidable.

Proof. Let $N_{\vec{k}} = (A, \Phi, \Psi)$ be an arbitrary $\vec{k}$-net of $NNPCR^{I,2}_{\vec{k}}$ and let q be the maximal number of all j such that $(x, j) \in B_{N_{\vec{k}}} (x \in V)$. To solve the problem $F_{\vec{k}}$ it is sufficient to construct the initial segments of all state sequences of $N_{\vec{k}}$ of the length q and verify if there is a state $x \in V$ and a moment $j \leq q$ such that $\Psi(x, j) = (\varphi_1, \ldots, \varphi_m) \in \Phi$ and $|\varphi_p(x^p)| > 1$ for any $p \leq m$. If so then $D(N_{\vec{k}})$ is infinite otherwise a finite one. □

Finally let us state a few properties constituting the relations between the class $\mathcal{D}^I_{\vec{k}}$ and its subclasses.

COROLLARY 2.10. *For every vector $\vec{k} \in \mathcal{N}^m$ and every different $p, q \in \{1,2\}$ the following relations hold:*

$$\mathcal{D}^{I,p}_{\vec{k}} \subseteq \mathcal{D}^{I}_{\vec{k}}, \tag{4}$$

$$\mathcal{D}^{I,1}_{\vec{k}} \cap \mathcal{D}^{I,2}_{\vec{k}} \neq \emptyset, \tag{5}$$

$$\neg(\mathcal{D}^{I,p}_{\vec{k}} \subseteq \mathcal{D}^{I,q}_{\vec{k}}), \tag{6}$$

where $\mathcal{D}^{I}_{\vec{k}}$ and $\mathcal{D}^{I,p}_{\vec{k}}$, $p = 1,2$, denote the classes of sets definable by the $\vec{k}$-nets of $NNPCR^{I}_{\vec{k}}$ and of $NNPCR^{I,p}_{\vec{k}}$, respectively. The sign $\neg$ denotes the negation connective.

3. The class $NNPCR^{II}_{\vec{k}}$ of nondeterministic $\vec{k}$-nets of parallel controlled shift-registers

A new class $NNPCR^{II}_{\vec{k}}$ of $\vec{k}$-nets for which the controls are many-valued functions while the feedback functions are single-valued ones will be introduced. The subclassses $NNPCR^{II,n}_{\vec{k}}$ $(n = 1,2)$ of $NNPCR^{II}_{\vec{k}}$ can be analogously defined as for $NNPCR^{I}_{\vec{k}}$.

Let us introduce the basic definitions.

Every element $N_{\vec{k}}$ of $NNPCR^{II}_{\vec{k}}$, which will be also called *a nondeterministic $\vec{k}$-net of parallel controlled shift-registers* (or shortly a *$\vec{k}$-net*), is defined as a tuple $(A, \Phi_1^{k_1} \times \cdots \times \Phi_m^{k_m}, \Psi)$, where every $\Phi_j^{k_j}$, $(j = 1,2,\ldots,m)$, is a set of total functions of A^{k_j} into A (*the feedback functions* of $N_{\vec{k}}$) and *the control* Ψ is a total function of $V \times \mathcal{N}$ into $2^{\Phi} \setminus \{\emptyset\}$, respectively.

For arbitrary states $x, y \in V$, $x = (x^1,\ldots,x^m)$, $y = (y^1,\ldots,y^m)$, y is said to be *an immediate successor* of x of $N_{\vec{k}}$ iff $y^j[1, kj-1] = x^j[2,k_j]$ for all $j \leq m$ with $k_j > 1$, and there exist $i \geq 1$ as well as $(\varphi_1,\ldots,\varphi_m) \in \Phi$ such that $(\varphi_1,\ldots,\varphi_m) \in \Psi(x,i)$ and $y^j[k_j,k_j] = \varphi_j(x^j)$; if $k_j = 1$ then we put $y^j = \varphi_j(x^j)$.

For arbitrary states $x, y \in V$, y is said to be a *successor* of x of $N_{\vec{k}}$ iff there exists a sequence $x_1,\cdots,x_n$, $n > 1$, of states such that $x_1 = x$, $x_n = y$ and x_{i+1} is an immediate successor of x_i of $N_{\vec{k}}$ for every $1 \leq \mathrm{i} < n$.

An infinite sequence $x = x_1, x_2, \ldots \in V^{\omega}$ is said to be *a state sequence* of $N_{\vec{k}}$ iff every x_{i+1}, $i \geq 1$, is an immediate successor of x_i of $N_{\vec{k}}$.

The set of all state sequences of a $\vec{k}$-net $N_{\vec{k}}$ of $NNPCR^{II}_{\vec{k}}$ is called its *definable set* and denoted by $D(N_{\vec{k}})$.

A $\vec{k}$-net $N_{\vec{k}} = (A,\Phi,\Psi)$ of $NNPCR^{II}_{\vec{k}}$ is said to be *deterministic* iff $|\Psi(x,i)| = 1$ for every $x \in V$ and every $i \in N$, otherwise if $\Psi(y,j) = \{(\varphi_1^i,\ldots,\varphi_m^i)\colon 1 \leq i \leq r\}$ for some $y = (y^1,\ldots,y^m) \in V$ and some $j \in N$

then we have

$$\varphi_p^m(y^p) = \varphi_p^n(y^p) \quad \text{for every } 1 \le m \le n \le r \text{ and every } 1 \le p \le m.$$

Let $NNPCR_{\vec{k}}^{II,1}$ and $NNPCR_{\vec{k}}^{II,2}$ denote the subclasses of $NNPCR_{\vec{k}}^{II}$ of all the $\vec{k}$-nets whose the controls are the total functions of V and of N into $2^{\Phi} \setminus \{\phi\}$, respectively ($\Phi$ denotes as previously $\Phi_1^{k_1} \times \cdots \times \Phi_m^{k_m}$).

For an illustration of the previous definitions let us see a few examples.

EXAMPLE 3.1. Let us define two nondeterministic $(2,3)$-nets $N_{(2,3)}^1 = (\{0,1\}, \Phi^2 \times \Pi^3, \Psi_1)$ of $NNPCR_{(2,3)}^{II,1}$ and $N_{(2,3)}^2 = (\{0,1\}, \Phi^2 \times \Pi^3, \Psi_2)$ of $NNPCR_{(2,3)}^{II,2}$ as follows

$\Phi^2 = \{\varphi_1, \varphi_2, \varphi_3\}$ and $\Pi^3 = \{\pi_1, \pi_2, \pi_3\}$, where

t	$\varphi_1(t)$	$\varphi_2(t)$	$\varphi_3(t)$
00	0	1	1
01	0	1	1
10	0	1	0
11	0	1	0

u	$\pi_1(u)$	$\pi_2(u)$	$\pi_3(u)$
000	0	1	1
001	0	1	1
010	0	1	0
011	0	1	1
100	0	1	0
101	0	1	0
110	0	1	1
111	0	1	0

and

$$\Psi_1(x) = \begin{cases} \{(\varphi_1, \pi_1), (\varphi_2, \pi_2)\} & \text{if all sequences of } x \text{ are constant} \\ \{(\varphi_3, \pi_3)\} & \text{for the remaining cases} \end{cases}$$

$$\Psi_2(i) = \begin{cases} \{(\varphi_1, \pi_1), (\varphi_2, \pi_2)\} & \text{if } i \text{ is odd} \\ \{(\varphi_3, \pi_3)\} & \text{if } i \text{ is even} \end{cases}$$

for every $x \in V = \{0,1\}^2 \times \{0,1\}^3$ and every $i \in N$.

The transition graph $G_{2,3}$ of $N_{(2,3)}^1$ is illustrated in Figure 3.1.

Looking on $G_{(2,3)}$ one can see that the state sequences of $N_{(2,3)}^1$ are almost periodic as well as aperiodic ones. As for the states $x = (00, 000)$ and $y = (11, 111)$ the same states are their immediate successors so long as we only wish (if we use the functions (φ_1, π_1) to x and (φ_2, π_2) to y) therefore we have: $|D(N_{(2,3)}^1)| = \aleph_0$. But for $N_{(2,3)}^2$ the situation is quite different. As $\Psi_2(i) = \{(\varphi_1, \pi_1), (\varphi_2, \pi_2)\}$ for every odd moments and $\varphi_1(x) \neq \varphi_2(x)$, $\pi_1(y) \neq \pi_2(y)$ for every $x \in \{0,1\}^2$ and $y \in \{0,1\}^3$ then one can choose an aperiodic or almost periodic sequence of feedback functions as a control

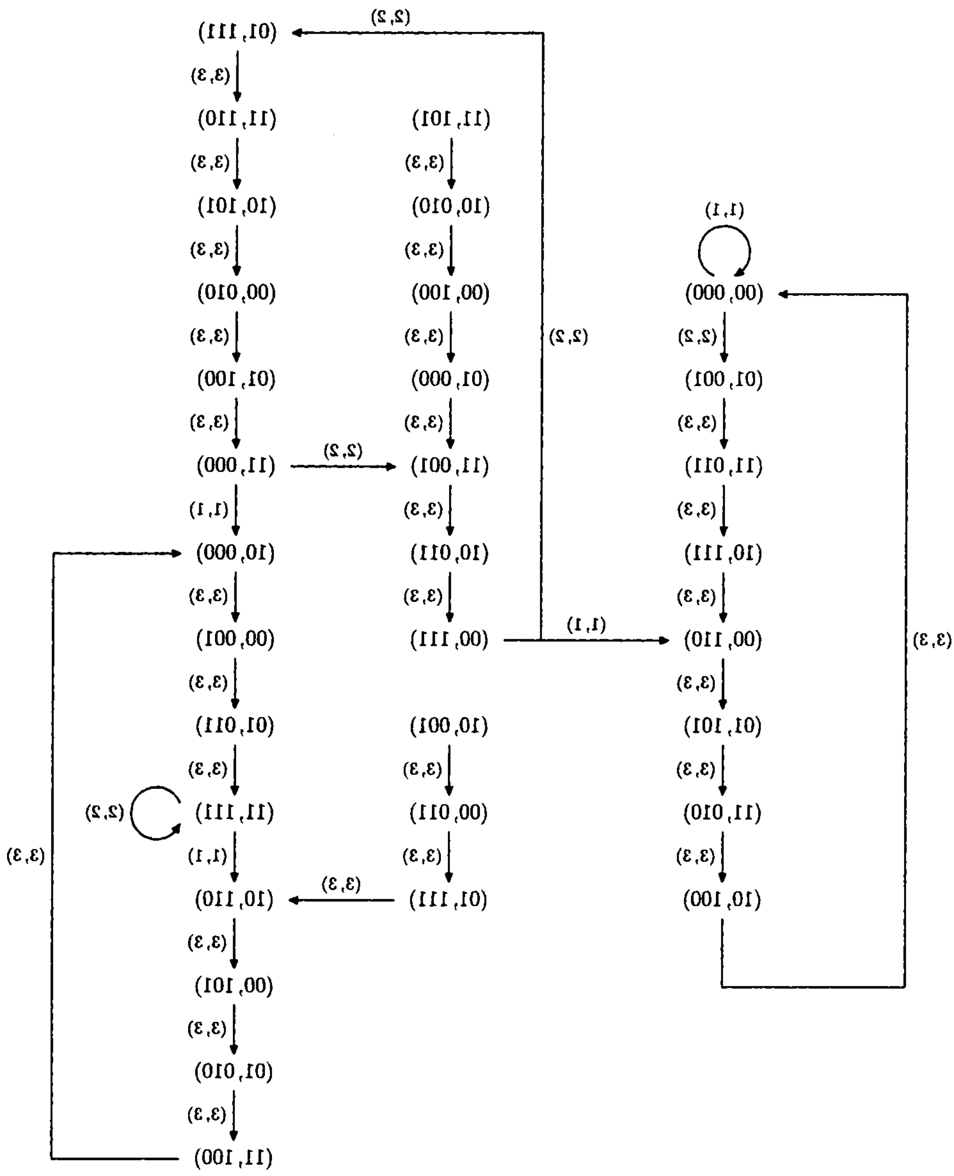

Fig. 3.1. The transiton graph $G_{2,3)}$ of $N^1_{(2,3)}$

sequence. The consequence of this fact is that the state sequences of $N^2_{(2,3)}$ can be almost periodic or aperiodic ones, what implies that $|D(N^2_{(2,3)})| = \aleph_0$.

THEOREM 3.2. *For arbitrary $\vec{k}$-net $N_{\vec{k}}$ of $NNPCR^{II,1}_{\vec{k}}$ we are able to decide (effectively) if $|D(N_k)| < \aleph_0$, or not.*

Proof is similar to the proof of Theorem 2.3 and therefore will be omitted.

One can easily cheek that for a class $\mathcal{D}^{II}_{\vec{k}}$ of definable sets by the $\vec{k}$-nets of $NNPCR^{II}_{\vec{k}}$ and its subclasses $\mathcal{D}^{II,p}_{\vec{k}}$, $p \in \{1,2\}$, the following results are valid.

COROLLARY 3.3. *For every* $\vec{k} \in \mathcal{N}^m$ *and every* $p,q \in \{1,2\}$, $p \neq q$, *the following relations hold*:

$$\mathcal{D}^{II,p}_{\vec{k}} \subseteq \mathcal{D}^{II}_{\vec{k}}, \tag{1}$$

$$\mathcal{D}^{II,1}_{\vec{k}} \cap \mathcal{D}^{II,2}_{\vec{k}} \neq \emptyset, \tag{2}$$

$$\neg(\mathcal{D}^{II,p}_{\vec{k}} \subseteq \mathcal{D}^{II,q}_{\vec{k}}), \tag{3}$$

4. Relationship between the classes $\mathcal{D}^{I}_{\vec{k}}$ and $\mathcal{D}^{II}_{\vec{k}}$ and their subclasses

It will be shown that $\mathcal{D}^{I}_{\vec{k}}$ (resp. $\mathcal{D}^{I,i}_{\vec{k}}$ for $i = 1,2$) is a subclass of $\mathcal{D}^{II}_{\vec{k}}$ (resp.of $\mathcal{D}^{II,i}_{\vec{k}}$) but the converse inclusion does not hold.

Before we formulate the respective theorems let us consider at the beginning two examples.

EXAMPLE 4.1. Let us reconsider the nondeterministic $(2,2)$-net $N_{(2,2)}$ of $NNPCR^{I,1}_{(2,2)}$ of Example 2.2. Let us construct a $(2,2)$-net

$$N^1_{(2,2)} = (\{0,1\}, \{\varphi_1', \varphi_2', \varphi_2''\} \times \{\pi_1', \pi_2'\}, \Psi_1) \in NNPCR^{II,1}_{(2,2)}$$

by means of $N_{(2,2)}$ as follows:

t	$\varphi_1'(t)$	$\varphi_2'(t)$	$\varphi_2''(t)$	$\pi_1'(t)$	$\pi_2'(t)$
00	0	1	1	0	1
01	1	0	1	0	1
10	0	1	1	0	1
11	0	1	1	0	1

$$\Psi_2(x) = \begin{cases} \{(\varphi_1', \pi_1')\} & \text{if the last elements of all sequences of } x \text{ are equal to } 0 \\ \{(\varphi_2', \pi_2'), (\varphi_2'', \pi_2')\} & \text{if the last elements of all sequences of } x \text{ are equal to } 1 \\ \{(\varphi_1', \pi_2')\} & \text{for the remaining cases,} \end{cases}$$

for every $x \in V$. Let us observe that $\varphi_1(x) = \{\varphi_1'(x)\}$, $\pi_1(x) = \{\pi_1'(x)\}$, $\pi_2(x) = \{\pi_2'(x)\}$ and $\varphi_2(x) = \{\varphi_2'(x), \varphi_2''(x)\}$ for every $x \in \{0,1\}^2$.

One can easily verify that the transition graph of $N^1_{(2,2)}$ is the same as in Example 2.2.

EXAMPLE 4.2. Let us define a $(2,2)$-net $N^2_{(2,2)} = (\{0,1\}, \{\varphi'_1, \varphi'_2, \varphi''_2\} \times \{\pi'_1, \pi'_2\}, \Psi_1)$ of $NNPCR^{II,2}_{(2,2)}$, as follows:

$\varphi'_1, \varphi'_2, \varphi''_2, \pi'_1, \pi'_2$ are the same as in Example 4.1, and

$$\Psi_1(i) = \begin{cases} (\varphi'_1, \pi'_1) & \text{if } i \text{ is odd,} \\ \{(\varphi'_2, \pi'_2), (\varphi''_2, \pi'_2)\} & \text{if } i \text{ is even,} \end{cases}$$

for all $i \geq 1$.

It is easy to observe that $(2,2)$-nets of Examples 2.4 and 4.2 are equivalent. □

EXAMPLE 4.3. Let us reconsider the $(2,3)$-nets $N^1_{(2,3)}$ and $N^2_{(2,3)}$ of Example 3.1. We would like to construct $(2,3)$-nets $N^3_{(2,3)} = (\{0,1\}, \bar{\Phi}^2_1 \times \bar{\Pi}^3_1, \Psi_3) \in NNPCR^{I,2}_{(2,3)}$ and $N^4_{(2,3)} = (\{0,1\}, \bar{\Phi}^2_1 \times \bar{\Pi}^3_1, \Psi_4) \in NNPCR^{I,2}_{(2,3)}$ which would be equivalent to $N^1_{(2,3)}$ and to $N^2_{(2,3)}$, respectively.

Looking at the controls Ψ_1 and Ψ_2 of $N^1_{(2,3)}$ and of $N^2_{(2,3)}$ we conclude that $\bar{\Phi}^2_1$ and $\bar{\Pi}^3_1$ would have the following form

$\bar{\Phi}^2_1 = \{\varphi'_1, \varphi'_2\}$, $\bar{\Pi}^3_1 = \{\pi'_1, \pi'_2\}$, where

t	$\varphi'_1(t)$	$\varphi'_2(t)$
00	$\{0,1\}$	1
01	a	1
10	a	0
11	$\{0,1\}$	0

u	$\pi'_1(u)$	$\pi'_2(u)$
000	$\{0,1\}$	1
001	b	1
010	b	0
011	b	1
100	b	0
101	b	0
110	b	1
111	$\{0,1\}$	0

for some $a, b \in A$.

The controls should be defined as follows:

$$\Psi_3(x) = \begin{cases} (\varphi'_1, \pi'_1) & \text{if all sequences of } x \text{ are constant} \\ (\varphi'_2, \pi'_2) & \text{for the remaining cases,} \end{cases}$$

$$\Psi_4(i) = \begin{cases} (\varphi'_1, \pi'_1) & \text{if } i \text{ is odd} \\ \\ (\varphi'_2, \pi'_2) & \text{if } i \text{ is even.} \end{cases}$$

Let us see that every state $x \in V$ of $N^1_{(2,3)}$ as well as of $N^2_{(2,3)}$ has at most two immediate successors. But a state y consisting of only constant sequences has axactly 2^5 immediate successors of $N^3_{(2,3)}$. Analogously every state z occurring in odd moments has exactly 2^5 immediate successors of $N^4_{(2,3)}$.

The conclusion is such that we are not able to construct the $(2,3)$-nets of $NNPCR^{I,i}_{\vec{k}}$, $i = 1, 2$, which would be equivalent to $N^3_{(2,3)}$ and to $N^4_{(2,3)}$.

THEOREM 4.4. *For every vector $\vec{k} \in \mathcal{N}^m$ and every number $i \in \{1,2\}$ the following inclusions hold*

$$\mathcal{D}^{I,i}_{\vec{k}} \subseteq \mathcal{D}^{II,i}_{\vec{k}}, \tag{1}$$

The converse inclusions do not hold.

Proof. Let us consider the arbitrary $\vec{k}$-nets $N^1_{\vec{k}} = (A, \Phi, \Psi_1)$ of $NNPCR^{I,1}_{\vec{k}}$ and $N^2_{\vec{k}} = (A, \Phi, \Psi_2)$ of $NNPCR^{I,2}_{\vec{k}}$, where $A = \{a_1, \cdots, a_n\}$ and $\Phi^{k_1}_1 \times \cdots \times \Phi^{k_m}_m$. For any function $\varphi : A^{k_j} \to 2^A \setminus \{\emptyset\}$ of $\Phi^{k_j}_j\,(j = 1, 2 \cdots m)$ let us define a set

$$C_\varphi = \{\xi : \xi : A^{k_j} \to A \;\text{ and }\; \xi(x) \in \varphi(x) \;\text{ for all } x \in A\}.$$

Elements of C_φ are called *components* of φ. For every $1 \le j \le m$ let

$$C^{k_j}_{\Phi_j} = \{C_\varphi : \varphi \in \Phi^{k_j}_j\}.$$

Let us define two $\vec{k}$-nets $N^3_{\vec{k}} = \left(A, C_{\Phi^{k_1}_1} \times \cdots \times C_{\Phi^{k_m}_m}, \Psi_3\right)$ of $NNPCR^{II,1}_{\vec{k}}$ and $N^4_{\vec{k}} = \left(A, C_{\Phi^{k_1}_1} \times \cdots \times C_{\Phi^{k_m}_m}, \Psi_4\right)$ of $NNPCR^{II,2}_{\vec{k}}$ as follows:

For every $x \in V$, $i \in N$ and every $(\varphi_1, \cdots, \varphi_m) \in \Phi^{k_1}_1 \times \cdots \times \Phi^{k_m}_m$, if $\Psi_1(x) = (\varphi_1, \cdots, \varphi_m)$ (resp. if $\Psi_2(i) = (\varphi_1, \ldots, \varphi_m)$) then we put $\Psi_3(x) = C_{\varphi_1} \times \cdots \times C_{\varphi_m}$ (resp. $\Psi_4(i) = C_{\varphi_1} \times \ldots \times C_{\varphi_m}$). The above construction implies that $D(N^1_{\vec{k}}) = D(N^3_{\vec{k}})$ and $D(N^2_{\vec{k}}) = D(N^4_{\vec{k}})$, hence the inclusion (1) holds.

The relations

$$\neg(\mathcal{D}^{II,i}_{\vec{k}} \subseteq \mathcal{D}^{I,i}_{\vec{k}}) \text{ for } i = 1, 2, \tag{2}$$

are still to be proved.

For this purpose let us define two $\vec{k}$-nets $N^5_{\vec{k}} = (A, \bar{\Phi}, \Psi_5)$ of $NNPCR^{II,1}_{\vec{k}}$ and $N^6_{\vec{k}} = (A, \bar{\Phi}, \Psi_6)$ of $NNPCR^{II,2}_{\vec{k}}$ as follows: $\bar{\Phi} = \bar{\Phi}^{k_1}_1 \times \cdots \times \bar{\Phi}^{k_m}_m$ and $\bar{\Phi}^{k_i}_i = \{\varphi^i_1, \ldots, \varphi^i_n, \varphi^i_{n+1}\}$ for $1 \le i \le m$, where $\varphi^i_j(t) = a_j$, $\varphi^i_{n+1}(t) = a_p$

for every $t \in A^{k_i}$, every $1 \le j \le n$, and some $a_p \in A$,

$$\Psi_5(x) = \begin{cases} \{(\varphi_1^1, \varphi_1^2, \dots \varphi_1^m), \dots, (\varphi_n^1, \dots \varphi_n^m)\} & \text{if all sequences of } x \\ & \text{are constant} \\ \{(\varphi_{n+1}^1, \dots, \varphi_{n+1}^m)\} & \text{for the remaining cases,} \end{cases}$$

$$\Psi_6(i) = \begin{cases} \{(\varphi_1^1, \varphi_1^2, \dots, \varphi_1^m), \dots (\varphi_n^1, \dots, \varphi_n^m)\} & \text{if } i \text{ is odd} \\ \{(\varphi_{n+1}^1, \dots, \varphi_{n+1}^m)\} & \text{if } i \text{ is even} \end{cases}$$

We would like to construct two $\vec{k}$-nets $N_{\vec{k}}^7 = (A, \Pi, \Psi_7)$ of $NNPCR_{\vec{k}}^{I,1}$ and $N_{\vec{k}}^8 = (A, \Pi, \Psi_8)$ of $NNPCR_{\vec{k}}^{I,2}$ which would be equivalent to $N_{\vec{k}}^5$ and $N_{\vec{k}}^6$, respectively.

Looking at Ψ_5 and at Ψ_6 we conclude that $\Pi = \Pi_1^{k_1} \times \dots \times \Pi_m^{k_m}$, where $\Pi_i^{k_i} = \{\pi_1^i, \pi_2^i\}$ for $1 \le i \le m$, $\pi_1^i(t) = \{a_1, \dots, a_n\}$, $\pi_2^i(t) = \varphi_{n+1}^i(t)$ for every $t \in A^{k_i}$, every $1 \le i \le m$, and the controls Ψ_7 and Ψ_8 have the form:

$$\Psi_7(x) = \begin{cases} (\pi_1^1, \dots \pi_1^m) & \text{if every sequence of } x \text{ is constant} \\ (\pi_2^1, \dots, \pi_2^m) & \text{for the remaining cases} \end{cases}$$

$$\Psi_8(i) = \begin{cases} (\pi_1^1, \dots, \pi_1^m) & \text{if } i \text{ is odd} \\ (\pi_2^1, \dots, \pi_2^m) & \text{if } i \text{ is even} \end{cases}$$

for every $x \in A^{k_1} \times \dots \times A^{k_m}$ and every $i \in N$.

Let use see that every state $x \in V$ consisting of only constant sequences has exactly n immediate successors of $N_{\vec{k}}^5$ whereas the same state x has n^n immediate ones of $N_{\vec{k}}^7$ Analogously every state y occurring in odd moments has exactly n immediate successors of $N_{\vec{k}}^6$ while n^n immediate ones of $N_{\vec{k}}^8$. The conclusion is such that the $\vec{k}$-nets of $NNPCR_{\vec{k}}^{I,1}$, $i = 1, 2$, which would be equivalent to $N_{\vec{k}}^5$ and to $N_{\vec{k}}^6$ do not exist. □

THEOREM 4.5. For every vector $\vec{k} \in \mathcal{N}^m$ the following inclusion holds:

$$\mathcal{D}_{\vec{k}}^I \subseteq \mathcal{D}_{\vec{k}}^{II}. \tag{3}$$

The converse inclusion does not hold.

Proof is analogous to the proof of Theorem 4.4. and therefore will be omitted.

5. Properties of the classes of state sequences of the $\vec{k}$-nets

Let $S_{\vec{k}}^I$ (resp. $S_{\vec{k}}^{I,i}$ for $i = 1, 2$) and $S_{\vec{k}}^{II}$ (resp. $S_{\vec{k}}^{II,i}$ for $i = 1, 2$) denote the classes of the state sequences of all $\vec{k}$-nets of $NNPCR_{\vec{k}}^I$ (resp. of $NNPCR_{\vec{k}}^{I,i}$) and of $NNPCR_{\vec{k}}^{II}$ (resp. of $NNPCR_{\vec{k}}^{II,i}$), respectively.

If the above symbols are preceeded by the letter $\mathcal{D}$ then new symbols denote the classes of the state sequences of all deterministic $\vec{k}$-nets of respective classes.

The following lemmas constitute the relations between the mentional above classes.

LEMMA 5.1. *For every vector $\vec{k} \in N^m$, $m \geq 1$, the following relations hold:*

$$\mathcal{DS}_{\vec{k}}^{I,i} = \mathcal{DS}_{\vec{k}}^{II,i}, \quad \text{for } i = 1,2, \tag{1}$$

$$\mathcal{DS}_{\vec{k}}^{I} = \mathcal{DS}_{\vec{k}}^{II}, \tag{2}$$

$$\mathcal{DS}_{\vec{k}}^{I,1} \subset \mathcal{DS}_{\vec{k}}^{I,2} , \tag{3}$$

$$\mathcal{DS}_{\vec{k}}^{II,1} \subset \mathcal{DS}_{\vec{k}}^{II,2} . \tag{4}$$

Proof. The equalities (1) and (2) immediately follow from the definitions of respective classes of deterministic $\vec{k}$-nets. The strong inclusions (3) and (4) follow from the facts that $\mathcal{DS}_{\vec{k}}^{I,1}$ and $\mathcal{DS}_{\vec{k}}^{II,1}$ consist of only almost periodic sequences whereas $\mathcal{DS}_{\vec{k}}^{I,2}$ and $\mathcal{DS}_{\vec{k}}^{II,2}$ the larger classes of almost periodic sequences and additionally aperiodic ones. □

LEMMA 5.2. *For every vector $\vec{k} = (k_1 \dots k_m) \in N^m$ the following relations hold:*

$$\mathcal{S}_{\vec{k}}^{0,i} = V^\omega \text{ for } 0 \in \{I, II\} \text{ and } i = 1,2, \tag{5}$$

$$S_{\vec{k}}^{I} = S_{\vec{k}}^{II} = V^\omega. \tag{6}$$

Proof. To prove (5) for $0 = I$ let us define two $\vec{k}$-nets $N_{\vec{k}}^1 = (A, \Phi, \Psi_1)$ of $NNPCR_{\vec{k}}^{I,1}$ and $N_{\vec{k}}^2 = (A, \Phi, \Psi_2)$ of $NNPCR_{\vec{k}}^{II,2}$ as follows:

$\Phi = \{\varphi_1\} \times \cdots \times \{\varphi_m\}$ where $\varphi_i(x) = A$ for $i = 1,2,\dots m$, $\Psi_1(x) = (\varphi_1, \cdots, \varphi_m)$ and $\Psi_2(i) = (\varphi_1, \cdots, \varphi_m)$ for every $x \in A^k$ and every $i \in N$.

It is obvious that $D(N_{\vec{k}}^1) = D(N_k^2) = V^\omega$.

Proof of (6) can be similarly conducted with a slight modification. □

6. Final remarks

This paper provides only a mathematical background on two classes $NNPCR_{\vec{k}}^{I}$ and $NNPCR_{\vec{k}}^{II}$ of nondeterministic parallel controlled $\vec{k}$-nets of shift-registers and constitutes the relationship between them. Further studies should be continued in a few directions. Let us list some of them:

(1) It would be interesting to distinguish the subclasses $\overline{NNPCR_{\vec{k}}^{I}}$ and $\overline{NNPCR_{\vec{k}}^{II}}$ (resp. $\overline{NNPCR_{\vec{k}}^{I,i}}$ and $\overline{NNPCR_{\vec{k}}^{II,i}}$, $i = 1,2$) of $NNPCR_{\vec{k}}^{I}$ and of $NNPCR_{\vec{k}}^{II}$ (resp. of $NNPCR_{\vec{k}}^{I,i}$ and of $NNPCR_{\vec{k}}^{II,i}$) with the property:

For every $\vec{k}$-net $N_{\vec{k}}$ of $\overline{NNPCR_{\vec{k}}^{0}}$ (resp. of $\overline{NNPCR_{\vec{k}}^{0,i}}$, $i = 1,2$), $0 \in \{I, II\}$, there exists an equivalent deterministic $\vec{k}$-net $\vec{N}_k$ of $NNPCR_{\vec{k}}^{0}$ (resp. of $NNPCR_{\vec{k}}^{0,i}$);

(2) There is a need to consider different aspect of nondeterministicity of the considered above $\vec{k}$-nets;

(3) There is a need to consider different kinds of complexity problems of the $\vec{k}$-nets of both classes as well as of their state sequences;

(4) There is a need to study the pseudorandomness of the state sequences of deterministic $\vec{k}$-nets;

(5) One can also consider the probabilistic $\vec{k}$-nets;

(6) One can introduce a new class $NNPCR_{\vec{k}}$ of the $\vec{k}$-nets such that their controls and the feedback functions can be many-valued.

References

[1] G. Birkhoff, T. Bartee, *Modern Applied Algebra*, Mc Graw-Hill Book Company, New York, St. Louis, San Francisco, Düsseldorf, London, Mexico, Panama, Sydney, Toronto, 1970.

[2] S. W. Golomb, *Shift-Register Sequences*, Acean Park Press, Laguna Hills, California (1982) (Revised edition).

[3] Z. Grodzki, *The controlled iterative systems (deterministic and nondeterministic)* [In Polish], Prace Instytutu Mat-Fiz-Chem, Ser A, No 2, Wyd. Uczelniane 1981.

[4] Z. Grodzki, I. Meznik, *Nets of time variant parallel controlled shift-registers*, Knižnice Odbornych a Vedeckych Spisu Vysokeho Učeni Techničkeho v Brnie, Ročnik 1988, B-119, 205–210.

[5] Z. Grodzki, *The nondeterministic controlled iterative (k, m)-systems*, Bull. Polish Acad. Sci., Ser. Technica, Vol. 39, 1(1991), 139–144.

[6] Z. Grodzki, *The deterministic $(k_1, \ldots, k_m)$-nets of parallel controlled shift-registers*, Demonstratio Math. 27 (1994), 379–389.

[7] Z. Grodzki, A. Wroński, *Generalized de Bruijn multigraphs of rank $\vec{k}$*, Ars Combinatoria (submitted).

[8] Z. Grodzki, *Cascade parallel $\vec{k}$-nets of shift-registers* (submitted for publication in Discrete Applied Mathematics).

[9] R. Lidl, H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge University Press, Cambridge 1986.

[10] M. Łatko, *Synthesis of the maximal factors of the de Bruijn graphs* [In Polish], Ph.D. Dissertation, University of Maria Skłodowska-Curie, Lublin 1987.

[11] J. Mykkelweit, M. Siu, P. Tong, *On the cycle structure of some nonlinear shift-register sequences*, Inform. Contr. 43 (1979), 202–215.

[12] H. Niederreiter, *Statistical independence properties of pseudorandom vectors produced by matrix generators*, J. Comput. Appl. Math. 31 (1990), 139–151.

[13] H. Niederreiter, *Pseudorandom vector generation by the inverse method*, ACM Trans. on Modelling and Computer Simulation, Vol. 4, No 2 (1994), 191–212.

[14] H. Niederreiter, *The multiple-recursive matrix method for pseudorandom number generator*, Finite Fields and Their Applications 1(1995), 3–30.

[15] W. Patterson, *Mathematical Cryptology for Computer Scientists and Mathematicians*, Rowman & Littlefield Publishers 1987.

[16] Ch. Ronse, *Feedback Shift-Registers*, Lecture Notes in Computer Science, 169, Springer Verlang, Berlin, Heidelberg, New York, Tokyo, 1984.

[17] J. Szuster, *Analysis of the controlled iterative systems*, Ph. D. Disseration, University of Maria Skłodowska-Curie, Lublin 1990.

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

[19] N. Zierler, *Linear recurring sequences*, J. Soc. Indust. Appl. Math. 7,(1959), 31–48.

[20] J. Żurawiecki, *Boolean k-machines* [In Polish], Ph D. Dissertation, University of Maria Skłodowska-Curie, Lublin, 1979.

INSTITUTE OF MATHEMATICS
TECHNICAL UNIVERSITY OF LUBLIN
ul. Okopowa 8
20-022 LUBLIN, POLAND

Received January 20, 1999.