DEMONSTRATIO MATHEMATICA
Vol. XXII No 3 1989

Zdzisław Grodzki

DETERMINISTIC CONTROLLED SHIFT-REGISTERS

1. Introduction

k-shift-registers are the technical arrangements which generate binary pseudoperiodic sequences with period length less or equal to 2^k. Such arrangements have been used in such areas as automatic control, criptology [4], coding theory [3], electrotechnics [1] and many others.

The aim of this paper is to introduce a new class C_k of the controlled k-registers. Such registers are equipped with a memory of k cells where symbols of a nonempty alphabet A can be inserted, of a feedback function $f : A^k \longrightarrow A$ and of a control $h : A^k x\ N \longrightarrow \{r, l\}$ which assings a state $t_2 \ldots t_k f(t_1 \ldots t_k)$ when $h(t_1 \ldots t_k, i) = r$, or $f(t_1 \ldots t_k) t_1 \ldots t_{k-1}$ when $h(t_1 \ldots t_k, i) = l$ to a state $t_1 \ldots t_k \in A^k$ and a moment $i \geq 1$.

Two subclasses $C_{k,i}$ (i = 1, 2) of C_k when a control h is constant with respect to the i-th argument will be distinguished.

The necessary and sufficient condition for a nonempty set $E \subseteq (A^k)^\infty$ to be a set of all sequences generable by the registers of the classes C_k, $C_{k,1}$ and $C_{k,2}$ will be given. The periodicity problem of such sets will be investigaed.

2. Preliminaries

Nonempty sets will be denoted always by upper case letters. The empty set and the set of all positive integers will be denoted by $\emptyset$ and N, respectively.

Elements of N will be denoed by lower case Latin letters i, j, k, m, n, p, q.

Let A be an alphabet of cardinality n, for some $n > 1$, and A^k - the k-th Cartesian product of A. Elements of A^k will be denoted by lower case Latin letters x, y, z (possibly with subscripts).

$(A^k)^\infty$ will denote the set of all infinite sequences, over A^k. The element of $(A^k)^\infty$ will be denoted by upper case Latin letters X, Y, Z (possibly with subscripts) and nonempty subsets of $(A^k)^\infty$ - by upper case letter H (possibly with subscripts).

For $X = x_1, x_2, \ldots \in (A^k)^\infty$, $H \subseteq (A^k)^\infty$ and $1 \leq i \leq j$, X(i, j) and H(i, j) will denote a restricted sequence $x_i, \ldots, x_j$ and a set $\{ X(i,j) : X \in H \}$, respectively.

E will denote the cardinality of a set E and the sign $\subset$ -the proper inclision of the sets.

The functions of A^k into A will be denoted by lower case Latin letters f, g and of A^k onto A^k - by upper case ones F^r, F^l, F^s. R_h will denote the range of the function h.

The relations will be denoted by upper case boldface Latin letter **S** with subscripts.

3. Basic definitions

Let us introduce at the beginning the auxiliary notion of a pseudoperiodic sequence

A sequence $X = x_1, x_2, \dots \in (A^k)^\infty$ is said to be pseudoperiodic if and only if the following condition is satisfied:

(1) $$(\exists i \geq 1)\ (\exists j \geq 1)\ (\forall p \geq i)\ (x_{p+j} = x_p).$$

Let i_0 be the minimal number of all numbers i for which the condition (1) is satisfied.

By a threshold segment of X (th(X)) we mean a sequence $X(1, i_0-1)$, if $i_0 > 1$, or the empty sequence ε - otherwise.

For i_0 as above, by the period of X (p(X)) we mean a sequence $X(i_0, i_0+j-1)$ with the minimal j.

A pseudoperiodic sequence with the empty threshold segment is said to be periodic.

$(A^k)^\infty_{pd}$ will denote the subset of $(A^k)^\infty$ of all periodic sequences.

Now the notion of a controlled k-register will be introduced.

By a controlled k-register CR_k $(k \geq 2)$ in the alphabet A (briefly k-register) we mean a triple $(A, f, h, \{r, l\})$, where $f : A^k \longrightarrow A$ is its feedback function, $h : A^k \times N \longrightarrow \{r, l\}$ - a control.

Both the above functions are total, r and l are the abbreviations for "righthand side" and "lefthand side" movement.

Every $x \in A^k$ is said to be a state of CR_k.

If $R_h = \{r\}$ $(R_h = \{l\})$ then CR_k is said to be a righthand side (a lefthand side) k-register.

An infinite sequence $X = x_1, x_2, \dots \in (A^k)^\infty$ is said to be generable by a controlled k-register $CR_k = (A, f, h, \{r, l\})$ if and only if the following condition is satisfied :

(2) for every $i \geq 1$, if $h(x_i, i) = r$ $(h(x_i, i) = l)$ then we have

$$x_{i+1} = x_i(2,k)\ f(x_i) \qquad (x_{i+1} = f(x_i)\ x_i(1,k-1)).$$

The set of all sequences generable by CR_k is called its definable set and will be denoted by $D(CR_k)$.

For $i = 1,2$ let $C_{k,i}$ denote a subclass of all controlled k-registers the controls of which are constant with respect to the i-th argument [1]. In both the cases the controls can be written as the one argument functions.

Let us consider a class $C_{k,2}$. We are able to associate to every k-register $CR_k = (A, f, h, \{r, l\}) \in C_{k,2}$ unique digraph G_k with labelled edges as follows :

(4) the nodes of G_k are all the elements of A^k ;

(5) if x, y are two nodes (not necessarily different) then there is an edge in G_k going from x to y and labelled r (l) if and only if $y = x(2,k)f(x)$ (or $y - f(x)x(1,k-1)$).

If we remove the labels from G_k then we obtain a transition graph of CR_k.

[1] A function $h : A^k \times N \longrightarrow \{r, l\}$ is said to be constant with respect to the first argument if and only if for all $x, y \in A^k$ and $i \in N$ we have : $h(x, i = h(y, i)$. Analogously, h is said to be constant with respect to the secnd argument if and only if for all $x \in A^k$ and $i, j \in N$ we have : $h(x, i) = h(x, j)$.

Example 3.1. Define a controlled 3-register $CR_3 = (\{0,1\}, f, h, \{r,l\})$ as follows :
$f(x) = 1$ for $x \in \{000, 010, 110\}$ and $f(y) = 0$ for the remaining $y \in \{0,1\}^3$, $h(x) = r$ if and only if the decimal value of x is an even number.

Then the digraph G_3 of CR_3 has the form :

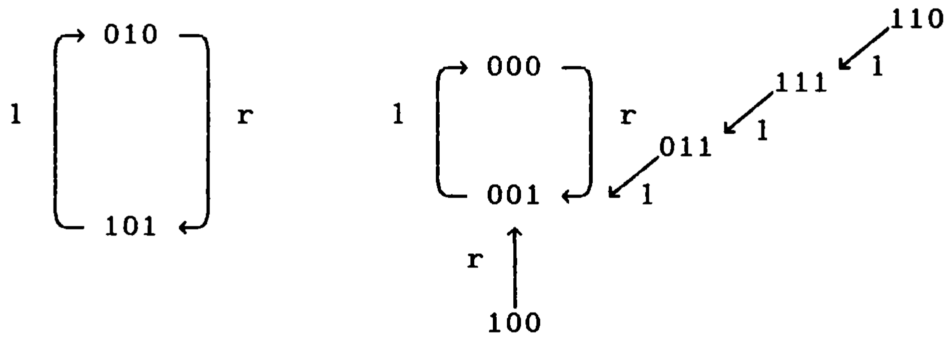

Fig. 3.1

Remark 3.1. Every k-register CR_k of $C_{k,2}$ can be defined immediately by some digraph G_k with labelled edges. The nodes of G_k are all the elements of A^k and the node x is joined with a node y and labelled r (or l) if and only if $x(2,k) = y(1,k-1)$ (or $x(1,k-1) = y(2,k)$).

4. The controlled k-registers of the class $C_{k,2}$

The periodicity problem of the definable sets by the registers of the class $C_{k,2}$ will be investigated.

Let $CR_k = (A, f, h, \{r,l\})$ $(k \geq 2)$ be an arbitrary k-register of the class $C_{k,2}$.

Lemma 4.1. For arbitrary sequences $X, Y \in D(CR_k)$ and $i, j \in N$ the following implication holds :

if $X(i,i)=Y(j,j)$ then $X(i+m,i+m)=Y(j+m,j+m)$ for all $m \geq 0$.

Proof can be done by mathematical induction with respect to m.

Corollary 4.1. All sequences generable by an arbitrary k-register of the class $C_{k,2}$ are pseudoperiodic with period length less or equal to $|A^k|$, where $|A^k|$ denotes the cardinality of A^k.

Now the following problem will be considered : what should the feedback functions be like so that all sequences generable by respective k-registers were periodic.

Lemma 4.2. Let $CR_k = (A,f,h,\{r,l\})$ be a controlled k-register of the class $C_{k,2}$ such that $|R_h| = 1$.

The following conditions are equivalent :

(1) all connected components of the transition graph of CR_k form the cycles ;

(2) all sequences generable by CR_k are periodic ;

(3) for all $x \in A^{k-1}$ and $a,b \in A$ $(a \neq b)$ the following conditions are satisfied :

(3.1) if $R_h = \{r\}$ then $f(ax) \neq f(bx)$;

(3.2) if $R_h = \{l\}$ then $f(xa) \neq f(xb)$.

Proof has been given in [4].

Remark 4.1. For a controlled k-register $CR_k = (A, f,h,\{r,l\})$ $(k > 2)$ such that $R_h= \{r,l\}$ both the conditions

(4) $f(ax) \neq f(bx)$

and

(5) $f(xa) \neq f(xb)$

for all $x \in .A^{k-1}$ and $a \neq b$ are neither necessary nor sufficient for all sequences generable by CR_k to be periodic.

This show the following examples.

Example 4.1. Define a controlled 3-register $CR_3=(\{0,1\},f,h,\{r,1\})$ as follows :

$f(x) = 1$ for all $x \in \{000,011,101,110\}$ and $f(y) = 0$ for the remaining $y \in \{0,1\}^3$, $h(z) = 1$ for all $z \in \{000,010,011,100,101,110,111\}$ and $h(001) = r$.

However for f both the conditions (4) and (5) are satisfied but there is a sequence with an initial state 000 generable by CR_3 which is not periodic.

Example 4.2. Define a controlled 3-register $CR'_3=(\{0,1\},f_1,h_1,\{r,1\})$ as follows :

$f_1(x) = 1$ for $x \in \{011,100,101,111\}$ and $f(y) = 0$ for the remaining $y \in \{0,1\}^3$, $h_1(z) = r$ for $z \in \{000,001,010,100\}$ and $h_1(z) = 1$ for the remaining $z \in \{0,1\}^3$.

However there are the states 010, 110, 100, 101 such that $f_1(010) = f_1(110)$ and $f_1(100) = f_1(101)$ but all the sequences generable by CR'_3 are periodic.

Theorem 4.1. For an arbitrary function $f\colon A^k \longrightarrow A$ $(k \geq 2)$ satisfying at least one of the onditions (4) or (5) there exists a controlled k-register $CR_k \in C_{k,2}$ with f as the feedback function generating periodic sequences only.

The proof is obvious, because there is a k-register with the feedback function f generating periodic sequences only.

5. The controlled k-registers of the class $C_{k,1}$

The properties of the definable sets by the controlled k-registers of the class C will be investigated. In particular, a periodicity problem of such sets will be studied.

For the further considerations let $CR_k = (A,f,h,\{r,l\})$ $(k \geq 2)$ e a controlled k-register of the class $C_{k,1}$ and $H = D(CR_k)$.

Lemma 5.1. For CR_k we have :

(1) if H consists of an aperiodic sequence then the control h of CR_k is an aperiodic sequence too.

Proof iś obvious.

Remark 5.1. The inverse statement to (1) is false.
This shows the following example.

Example 5.1. We shall define a subclass $C^f_{k,1}$ of $C_{k,1}$ of the controlled k-registers with the common feedback function f and aperiodic controls which generate of only pseudoperiodic sequences.

Define the functions $f:\{0,1\}^k \longrightarrow \{0,1\}$ and $h: N \longrightarrow \{r,l\}$ as follows :

$f(x) = 1$ if and only if $x(k,k) = 1$ and $f(y) = 0$ for the remaining $y \in \{0,1\}^k$, the controls h can be arbitrary aperiodic sequences with unique restriction : $h(i) = r$ for $i = 1,2, \dots ,k$.

It follows immediately from the above construction that all sequences generable by an arbitrary k-register $CR_k \in C^f_{k,1}$ are pseudoperiodic.

Lemma 5.2. For CR_k we have :

(2) if the control h of CR_k is periodic then all the sequences generable by CR_k are pseudoperiodic.

Proof is obvious.

Theorem 5.1. Let $CR_k = (A, f, h, \{r, l\})$ $(k \geq 2)$ be a k-register of the class $C_{k,1}$ such that $R_h = \{r, l\}$ and $H = D(CR_k)$.

H consists of only periodic sequences $(H \subseteq (A^k)^{\infty}_{pd})$ if and only if the following conditions are satisfied [2] :

(3) h is periodic ;

(4) both the conditions (4) and (5) of Remark 4.1. are satisfied.

Proof of sufficiency is obvious.

For the proof of necessity suppose that at least one of the conditions (3) or (4) is not satisfied. If h is not periodic then H consists of an pseudoperiodic sequence with a nonempty threshold segment or an aperiodic one. If at least one of the conditions (4) or (5) of Remark 4.1. is not satisfied then from the assumption that $R_h = \{r, l\}$ it follows that there is $i \geq 1$ such that $H(i,i) \subset A^k$ and therefore $\neg(H \subseteq (A^k)^{\infty}_{pd})$.

Corollary 5.1. Let for CR_k the assumptions (3) and (4) of Theorem 5.1 are satisfied and let $q > 1$ be the period length of h.

[2] If we omit in Theorem 5.1 the assumption $R_h = \{r, l\}$ then the obtained sentence is false.

Then the period length of arbitrary sequence of H is less or equal to $q|A^k|$.

The following example shows the mehodology of a construction of the k-registers of the class $C_{k,1}$ generating of only periodic sequences with the given periods lenths.

Example 5.2. Define a function $f : \{0,1\}^3 \longrightarrow \{0,1\}$ and $h : N \longrightarrow \{r,l\}$ as follows :

$f(x) = 1$ for $x \in \{000,011,101,110\}$ and $f(y) = 0$ for the remaining $y \in \{0,1\}^3$,

$$h(m) = \begin{cases} r \text{ (or } l) & \text{for } 8i+1 \le m \le 8i+4 \\ l \text{ (or } r) & \text{for } 8i+5 \le m \le 8(i+1) \end{cases}$$

where $i = 0,1,2,\ldots$.

As all the connected components of both the conjugated 3-registers R_3^r and R_3^l with the feedback function f form the cycles of length 4 therefore it is obvious that all sequences generable by a controlled 3-register $CR_3 = (\{0,1\}, f, h, \{r,l\})$ are periodic with period length equal to 8.

Lemma 5.3. Let $CR_k = (A,f,h,\{r,l\})$ $(k \ge 2)$ be a controlled k-register with the properties :

(5) all the connected components of the transition graphs of the conjugated k-registers R_k^r and R_k^l with f as the feedback function form the cycles of the same length q, for some $q \ge 1$ (it is possible a case that a constant states form the cycles of length 1) ;

(6) the control h is periodic with period length of 2mq, for some $m \ge 1$, and such that

$$h(p) = \begin{cases} r \text{ (or } l) & \text{for } \quad 2imq + 1 \le p \le (2i+1)mq \\ l \text{ (or } r) & \text{for } (2i+1)mq + 1 \le p \le 2mq(i+1) \end{cases}$$

where $i = 0, 1, \ldots$;

(7) the conjugated k-registers R_k^r and R_k^l are similar in such a sense that there is one-to-one correspondence between their transition graphs such that the cycles corresponding to each other consist of the same states (possibly with another ordering).

Then all sequences generable by CR_k are periodic with period length of 2mq.

Proof. It follows from the assumption that all the sequences generable by both the k-registers R_k^r and R_k^l are periodic with the period length of q. Then all the sequences generable by CR_k are also periodic with the period length of 2mq.

Remark 5.2. The following example comprise a more general class of shift-registers.

Example 5.3. Define a function $f : \{0,1\}^3 \longrightarrow \{0,1\}$ and $h : N \longrightarrow \{r, l\}$ as follows :

$f(x) = 1$ for $x \in \{001, 010, 100, 111\}$ and $f(y) = 0$ for the remaining $y \in \{0,1\}^3$,

$$h(p) = \begin{cases} r \text{ (or } l) & \text{for } \quad 8i + 1 \le p \le 8i + 4m \\ l \text{ (or } r) & \text{for } \quad 4(2i+m)+1 \le p \le 4(2i+2m+1) \ , \end{cases}$$

for $i = 0, 1, a..$ and some $m \ge 1$.

All the connected components of the conjugated r-registers R_3^r and R_3^l with the feedback function f form four cycles of lengths 1,2 and 4. It follows from the construction that all the sequences generable by the controlled 3-register $CR_3 = (\{0,1\}, f, h, \{r,l\})$ are periodic with the period lengths of 1 (two constant sequences), of length 2 (two sequences consisting the initial states 010 and 101) and of length 4 (the remaining sequences).

6. The definable sets

A necessary and sufficient condition for a nonempty set $H \subseteq (A^k)^\infty$ to be definable by the controlled k-registers of the classes C_k, $C_{k,1}$ and $C_{k,2}$ will be given.

Theorem 6.1. A nonempty set $H \subseteq (A^k)^\infty$ is definable by any controlled k-register $CR_k \in C_k$ if and only if the following conditions are satisfied :

(1) for every $x \in A^k$ there is an unique $X \in H$ such that $x = X(1,k)$;

(2) for every sequence $X = x_1, x_2, \ldots \in H$ and $i \geq 1$ we have :

$$x_{i+1}(1,k-1) = x_i(2,k) \quad \text{or} \quad x_{i+1}(2,k) = x_i(1,k-1) \ ;$$

(3) for all two sequences $X, Y \in H$ and $i \geq 1$, if $X(i,i) = Y(i,i)$ then $X(i+1,i+1) = Y(i+1,i+1)$.

Proof. Let $CR_k = (A, f, h, \{r,l\})$ be a controlled k-register of the class C_k and $H = D(CR_k)$.

The condition (2) follows from the assumption that f is a total function of A^k into A and therefore each sequence $x \in A^k$ is an initial state of any sequence X generable by CR_k. As CR_k is deterministic therefore the condition (3) holds.

The condition (2) means that a righthand side or a lefthand side realization of a k-register is possible.

Sufficiency. Suppose that for H the conditions (1)-(3) of Theorem 6.1 are satisfied. We shall construct the functions $f : A^k \longrightarrow A$ and $h : A^k x N \longrightarrow \{r, l\}$ on the basis of H. Let $H(1,1) = \{x_1, \dots, x_{n^k}\}$ and $H(2,2) = \{y_1, \dots\dots, y_{n^k}\}$. Then we verify for all $1 \le j \le n^k$, if $y_j(1,k-1) = x_j(2,k)$ or $y_j(2,k) = x_j(1,k-1)$. In the first case we put $f(x_j) = y_j(k,k)$ and $h(x_j, 1) = r$, otherwise $f(x_j) = y_j(1,1)$ and $h(x_j, 1) = l$.

Suppose that f and h have been defined on the segment $H(1, i-1)$ for $i \ge 2$. Let $H(i, i) = \{z_1, \dots, z_{n^k}\}$ and $H(i+1,i+1) = \{z'_1, \dots, z'_{n^k}\}$. Then we follow analogously as in the fist step. The conditions (1)-(3) guarantee that f and h have been defined correctly. It follows immediately from the construction that $H = D(CR_k)$, where $CR_k = (A, f, h, \{r, l\})$.

Now the analogical theorems for the cases when respective registers are elements of $C_{k,1}$ or of $C_{k,2}$ will be formulated.

Theorem 6.2. A nonempty set $H \subseteq (A^k)^\infty$ is definable by any controlled k-register $CR_k \in C_{k,2}$ if and only if the conditions (1), (2) and the following one are satisfied :

(4) H is 1-homogeneous, i.e. for each two sequences $X, Y \in H$ and $i, j \in N$, if $X(i,i) = Y(j,j)$ then $X(i+1,i+1) = = Y(j+1,j+1)$.

Theorem 6.3. A nonempty set $H \subseteq (A^k)^\infty$ is definable by any controlled k-register $CR_k \in C_{k,1}$ if and only if the conditions (1), (3) and the following one are satisfied :

(5) each H(i+1,i+1) (i ≥ 1) results from H(i,i) by a righthand side (or a lefthand side) movement ; more precisely, if E(i,i) = $\{x_1,\ldots,x_{n^k}\}$ and H(i+1.i+1) = = $\{y_1,\ldots\ldots,y_{n^k}\}$ then for all $1 \le j \le n^k$ the following condition holds :

$$y_j(1,k-1) = x_1(2,k) \text{ (or } y_j(2,k) = x_j(1,k-1)).$$

Proofs of Theorems 6.2 and 6.3 are similar to the proof of Theorem 6.1 and will be omitted.

7. Some decidable problems related to the synthesis of the class of the controlled k-registers

Generally speaking in the synthesis problem we have to construct a singular controlled k-register or whole class of such registers with the given properties, if such a class is nonempty.

The solution of the synthesis problem consists of two steps :

(1) we have to decide if the desired class is nonempty ;

(2) if the answer to (1) is positive we have to construct effectively this class.

We restrict our considerations to the first step only.

Let us state at the beginning two auxiliary problems. Let Ω^k denote the class of all functions of A^k into A.

Define two problems $S^k \subseteq \Omega^k$ and $S_1^k \subseteq (\Omega^k)^2$ as follows :

(3) for arbitrary function $f : A^k \longrightarrow A$, $S^k(f)$ if and only if there is a controlled k-register $CR_k \in C_{k,2}$ with the feedback function f such that all sequences generable by CR_k are periodic

(4) for arbitrary functions f and g of A^k into A, $S_1^k(f,g)$ if and only if there are two controlled k-registers CR_k and CR_k' of $C_{k,2}$ with the feedback functions f and g such that all the connected components of their transition graphs form the cycles and there is one-to-one correspondence between transition graphs such that corresponding to each others cycles consists of the same states.

Theorem 7.1. For each $k \geq 2$, S^k is decidable.

Proof. Given function $f : A^k \longrightarrow A$ we construct a digraph G(f) with labelled edges as follows :

(5) the nodes of G(f) are all the elements of A^k ;

(6) from an arbitrary node $x \in A^k$ there goes two edges with labels r and l to the nodes $x(2,k)f(x)$ and $f(x)x(1,k-1)$.

Then we verify, if there is a subgraph G'(f) of G(f) with n^k nodes consisting of all the elements of A^k and such that all the connected components form the cycles.

As the cardinality of Ω^k is finite and for each function $f \in \Omega^k$ the verification as above is effective therefore S^k is decidable.

Theorem 7.2. For all $k \geq 2$, S_1^k is decidable.

We shall give only a short outline of the proof.

Let f and g be the arbitrary elements of Ω^k. We shall construct at the beginning the digraphs G(f) and G(g) and we verify, if $S^k(f)$ and $S^k(g)$, or not. If the answer to the above question is positve then we verify, if $S^k_1(f,g)$, or not. As the cardinality of the class Ω^k is finite and the verification as above is effective therefore S^k_1 is decidable.

Let Ψ^k denote the class of all total functions of A^k into $\{r,l\}$ and Π - the class of all periodic functions of N into $\{r.l\}$. which are defines by means of their periods. Let $\mathcal{F}^k$ denote the class of all finite sets $H \subseteq A^k$ consisting of all periodic sequences which are defined by means of their periods.

Let us state the following synthesis problems :

(7) for arbitrary functions $h, h_1 \in \Psi^k$, $S_2(h,h_1)$ if and only if there are two controlled k-registers $CR_k = (A,f,h, \{r,l\})$ and $CR'_k = (A,g,h_1,\{r,l\})$ of $C_{k,2}$ such that $S_1(f,g)$;

(8) for arbitrary functions h, $h_1 \in \Pi$ and $k \in N$, $S_3(h,h_1,k)$ if and only if there are the controlled k-registers CR_k and CR'_k of $C_{k,1}$ with the controls h and h_1 and such that $D(CR_k)= D(CR'_k)$;

(9) for arbitrary $H \subseteq (A^k)^\infty \in \mathcal{F}^k$, $S_4(H)$ if and only if there is a controlled k-regiser $CR_k \in C_{k,2}$ (or of $C_{k,1}$ such that $H = D(CR_k)$;

(10) for arbitrary set $H \subseteq (A^k)^\infty \in \mathcal{F}^k$ and a function $f \in \Omega^k$, $S_5(H,f)$ if and only if there is a k-register $CR_k \in C_{k,2}$ (or $CR_k \in C_{k,1}$) with the feedback function f and such that H = $D(CR_k)$;

(11) for arbitrary set $H \in \mathcal{F}^k$ and $h \in \Pi$, $S_6(H,h)$ if and only if there is a controlled k-register $CR_k \in C_{k,1}$ with the

control h such that $H = D(CR_k)$.

All problems (7)-(11) are decidable. These problems have been solved by the author [6] for a slightly different class of the controlled shift-registers. We do not repeat here the considerations of [6].

REFERENCES

[1] A.I. Aleksiejev, A. G. Szeremietiev, G. I. Tuzov, B. I. Glazov : Theory and application of pseudorandom signals (In Russian), Izd. Nauka, Moskwa (1969).

[2] G. Birkhoff, T. Bartee : Modern applied algebra, Mc-Graw-Hill Book Company, New York, St Louis, San Francisco, Dťsseldorf, London, Mexico, Panama, Sydney, Toronto (1970).

[3] R. E. Blahut : Theory and practice of error-correcting codes, Addison-Wesley Publishing Company, Menlo Park, California, London, Amsterdam, Don Mills, Ontario, Sydney, Reprinted from correction (1984).

[4] S. W. Golomb : Shift-register sequences, Holden Day, San Francisco, Cambridge, London, Amsterdam (1967).

[5] Z. Grodzki : The theory of shift-registers, Information and Control 3(1972), 196-205.

[6] Z. Grodzki : Synthesis problem for deterministic controlled (k,m) - shift-registers (to appear in Demonstratio Math.).

[7] Z. Grodzki, M. Łatko : The nets of conjugated

shift-registers (to appear in Problems of Control and Information Theory).

[8] Z. Grodzki, M. Łatko : The conjugated shift-registers (to appear in Demonstratio Math.).

INSTITUTE OF MATHEMATICS, TECHNICAL UNIVERSITY OF LUBLIN,
20-618 LUBLIN, POLAND

Received August 17, 1987.