DEMONSTRATIO MATHEMATICA
Vol XXII No 1 1989

Zdzisław Grodzki, Marek Łatko

THE CONJUGATED SHIFT-REGISTERS

Introduction

The k-shift-registers are technical arrangements which generate binary pseudoperiodic sequences. Let us quote a few sentences from the preface to Golomb's monograph [5].

"The theory of shift-registers has found major applications in a wide variety of technological situations, including secure, reliable and efficient communications, digital ranging and tracking systems, deterministic simulation of random processes and computer sequencing and timing schemes".

With respect to easy technical realization the linear k-registers have been used most frequently. The theory of these ones has been elaborated for the practice in a satisfactory way. Namely, to every linear k-register R_k a unique polynomial $f_k(x)$ of degree k is assigned. The properties of these polynomials allow to obtain the length of the output sequences of respective k-registers. The Ronse's monograph [11] describes an uniform algebraical method which is useful for solving the above problems for arbitrary k-registers.

The most problems which have been published before are related to the construction of a whole class of the k-registers for which the output sequences are periodic with period length of 2^k (or of 2^k-1 in the linear case). Such k-registers are said to be maximal and their output sequences - pseudorandom. We do not recall here the directions of the studies on this problem. The reader is referred to the Fredricksen's paper [4] where almost whole bibliography has been completed.

On the other hand the studies on shift-registers go in the different directions. Namely, in the monographs [2,10,11] the pure algebraical results related to the shift-registers have been described.

The period of 30 years which passed since the appearence of Golomb's monograph [5] didn't make the scientists lose the interest in the shift-registers, on the contrary, it increased the field of applications in the technology of integrated circuits. In modern electronics shift-registers are used rather as nets (sequential or parallel) than as singular ones.

The theory of nets of shift-registers is still in the initial stage of development, however there are several papers which are related to the singular classes [6,8,9,11].

This paper is related to the nets of parallel conjugated k-registers which "work" synchronously. The basic properties of the sets of all output sequences, in particular a periodicity problem of such sets, will be studied.

At the very end a more general class of parallel shift-registers will be introduced and a few properties of the output sets will be given.

1. Preliminaries and basic definitions

Nonempty sets will be denoted by upper case letters. In particular, the empty set and the set of all nonnegative integers will be denoted by $\emptyset$ and N, respectively.

Let A be an alphabet of cardinality n ($n > 1$) and A^k ($k \geq 2$) - the k-th Cartesian product of A. The elements of A^k will be denoted by lower case Latin letters x, y, z (possibly with subscripts).

Let A^∞, $A_{-\infty}$, $A^\infty_{-\infty}$ denote the sets of all righthand side, lefthand side and bothhand side infinite sequences, over A. The elements and the subsets of the above sets will be denoted by upper case Latin letters T, U, V, V and E, F, respectively.

To uniform the considerations later on a sequence $T = t_1, t_2, \ldots$ will denote a sequence $t_1, t_2, \ldots$ of A^∞ or a sequence $t_{-1}, t_{-2}, \ldots \in A_{-\infty}$.

For $T = t_1, t_2, \ldots \in A^{\infty} \cup A_{-\infty}$, $E \subseteq A^{\infty} \cup A_{-\infty}$ and $1 \leqslant i \leqslant j$ $T(i,j)$ and $E(i,j)$ will denote a sequence $t_i \ldots t_j$ and a set $\{T(i,j) : T \in E\}$.

The analogical notations can be introduced for the elements and the subsets of $A^{\infty}_{-\infty}$.

Let $(A^k)^{\infty}$ denote the set of all right-hand side infinite sequences, over A^k. The elements and the subsets of $(A^k)^{\infty}$ will be denoted by upper case Latin letters X, Y, Z and G, H, respectively.

Let $(A^k \times A^k)^{\infty}$ denote the set of all right-hand side infinite sequences, over $A^k \times A^k$. The elements and the subsets of $(A^k \times A^k)^{\infty}$ will be denoted by upper case boldface letters $\underline{X}$, $\underline{Y}$, $\underline{Z}$ and $\underline{G}$, $\underline{H}$, respectively.

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

The analogical notations can be introduced for the elements and the subsets of $(A^k \times A^k)^{\infty}$.

The sign $\subset$ denotes the proper inclusion for the sets and $|A^p|$ - the cardinality of A^p.

The functions of A^k into A will be denoted by lower case letters f, g and of A^k into A^k - by upper case ones F^r, F^l, F^s.

The symbols $\neg$, $\&$, $\Rightarrow$, $\Leftrightarrow$ denote the logical connectives and $\forall$, $\exists$ - the quantifiers.

Let us introduce at the end the notions of a pseudoperiodic sequence and a k-homogeneous set.

A sequence $T = t_1, t_2, \ldots \in A^{\infty} \cup A_{-\infty}$ is said to be pseudoperiodic if and only if the following condition is satisfied:

$$(1) \qquad (\exists i \geqslant 1)(\exists\, j \geqslant 1)\ (\forall p \geqslant i)\ (t_p = t_{p+j}).$$

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

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

For i_0 as above, by the period of T (p(T)) we mean a sequence $t_{\underline{i_0}} \ldots t_{\underline{i_0+j-1}}$ with the minimal number j.

A pseudoperiodic sequence with the empty threshold segment is said to be periodic. A periodic sequence T with the period $t_{\underline{i}} \ldots t_{\underline{j}}$ will be denoted as $(t_{\underline{1}} \ldots t_{\underline{j}})_\infty$.

A nonempty set $E \subseteq A^\infty$ is said to be k-homogeneous ($k \geq 1$) if and only if the following condition is satisfied:

$$(2) \quad (\forall T \in E)(\forall U \in E)\forall i \geq 1(\forall j \geq 1)(T(i,i+k-1) = U(j,j+k-1) \Longrightarrow T(i+k,i+k) = U(j+k,j+k))$$

The same notions can be introduced for the elements and the subsets of $(A^k)^\infty$ as well as of $(A^k \times A^k)^\infty$.

2. Nets of the conjugated k-registers

Nets of the conjugated k-registers, right-hand side and left-hand side, with the same feedback function will be considered. The characteristics of these nets by means of their transition graphs will be given. In particular, a necessary and sufficient condition for all the connected components of their transition graphs to be the cycles will be given.

Let us introduce at the beginning some necessary definitions.

Given total function $f : A^k \longrightarrow A$ ($k \geq 2$) let us define two functions F^r and F^l of A^k into A^k as follows:

$$(1) \quad F^r(t_1 \ldots t_k) = t_2 \ldots t_k f(t_1 \ldots t_k),$$

$$(2) \quad F^l(t_1 \ldots t_k) = f(t_1 \ldots t_k) t_1 \ldots t_{k-1}$$

for all $t_1 \ldots t_k \in A^k$.

R e m a r k 2.1. It is possible to define immediately the functions F^r and F^l as follows:

$$(3) \quad \text{if } F^r(t_1 \ldots t_k) = u_1 \ldots u_k \text{ then } u_i = t_{i+1},$$

(4) if $F^l(t_1 \ldots t_k) = u_1 \ldots u_k$ then $u_{i+1} = t_i$

for all $1 \leqslant i \leqslant k-1$ and $t_1 \ldots t_k$, $u_1 \ldots u_k$ A^k.

Obviously, each of the functions F^r and F^l which is defined by means of (3) or (4) univocally determines the function f.

The pairs (A^k, F^r), (A^k, F^l) and $(A^k, (F^r, F^l))$ are said to be a right-hand side, a left-hand side k-register and a net of the conjugated k-registers (briefly k-net), respectively.

A^k, $(A^k)^2$ and F^s, (F^r, F^l) are said to be the sets of states and the transition functions of R_k^s and N_k, respectively. A function $f : A^k \to A$, which is connected with F^r and F^l by means of (1) and (2) is said to be the feedback function of R_k^s as well as of N_k.

A state $y \in A^k$ is said to be a successor of a state $x \in A^k$ in a k-register $R_k^s = (A^k, F^s)$ if and only if there is $i \geqslant 1$ such that $y = (F^s)^i(x)$, where $(F^s)^i$ denotes the i-th iteration of F^s. Analogously, a state (x_1, y_1) is said to be a successor of a state (x,y) in a k-net $N_k = (A^k, (F^r, F^l))$ if and only if $(x_1, y_1) = ((F^r)^i(x), (F^l)^i(y))$ for some $i \geqslant 1$.

Each k-register $R_k^s = (A^k, F^s)$ as well as a k-net $N_k = (A^k, (F^r, F^l))$ determines unique directed graph $G(R_k^s)$ and $G(N_k)$ - their transition graphs. The nodes of $G(R_k^s)$ (of $G(N_k)$) are all the elements of A^k (of $A^k \times A^k$) and an edge goes from a state x to a state y (from a state (x,y) to a state (x_1, y_1)) if and only if $y = F^s(x)$ ($x_1 = F^r(x)$ and $y_1 = F^l(y)$).

E x a m p l e 2.1. Define a function $f : \{0,1\}^3 \to \{0,1\}$ as follows: $f(x) = 1$ for all $x \in \{000, 101, 110, 011\}$ and $f(y) = 0$ for the remaining elements of $\{0,1\}^3$.

The transition graphs of the right-hand side and left-hand side 3-registers, for which f is a feedback function, have a form:

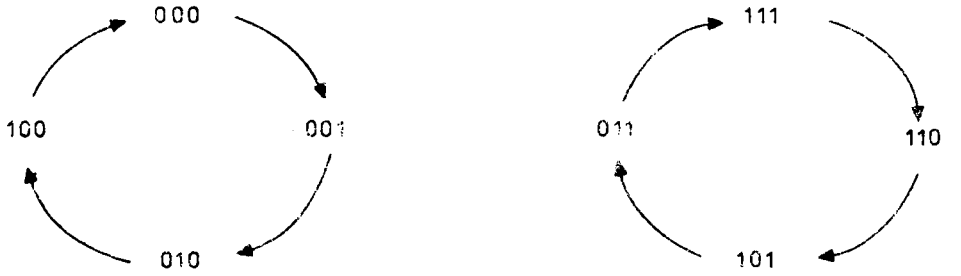

Fig.2.1

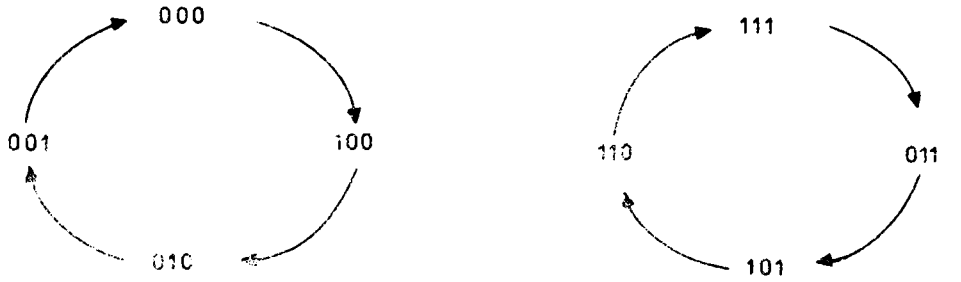

Fig.2.2

The transition graph $G(N_3)$ of the 3-net N_3, for which f is the feedback function, consists of 16 connected components which are the cycles. Every such a component consists of 4 states.

Now a necessary and sufficient condition for all the connected components of the transition graphs of a k-register R_k^s as well as of a k-net N_k to be the cycles will be formulated.

Let $R_k^s = (A^k, F^s)$ $(k \geq 2)$, $s \in \{r,l\}$) be a k-register and $N_k = (A^k, (F^r, F^l))$ - a k-net. Let $G(R_k^s)$ and $G(N_k)$ be their transition graphs.

L e m m a 2.1. For R_k^s the following conditions are equivalent:

(5) every connected component of the transition graph $G(R_k^s)$ of R_k^s forms a cycle;

(6) the transition function F^s of R_k^s is a mapping of A^k onto A^k;

(7) for the feedback function f of R_k^s the following conditions are satisfied for all $t_2 \ldots t_k \in A^{k-1}$ and $a, b \in A$ $(a \neq b)$:

(7.1) if $s = r$ then $f(at_2 \ldots t_k) \neq f(bt_2 \ldots t_k)$;

(7.2) if $s = l$ then $f(t_2 \ldots t_k a) \neq f(t_2 \ldots t_k b)$.

Proof in [5] has been given.

T h e o r e m 2.1. For the k-net N_k the following conditions are equivalent:

(8) all the connected components of the transition graph $G(N_k)$ of N_k form the cycles;

(9) both functions F^r and F^l are the mapping of A^k onto A^k;

(10) both the conditions (7.1) and (7.2) are satisfied.

Proof immediately follows from Lemma 2.1.

3. The output sequences of the k-nets

A necessary and sufficient condition for a nonempty set E of $A_{-\infty}^{\infty}$ to be the set of all output sequences of any k-net N_k will be given.

Let us introduce at the beginning the necessary definitions.

Let $R_k^s = (A^k, F^s)$ $(k \geq 2)$ be a k-register and $N_k = (A^k, (F^r, F^l))$ - a k-net. Let f be their feedback function.

An infinite sequence $T = t_1, t_2, \ldots \in A^{\infty} \cup A_{-\infty}$ is said to be an output sequence of R_k^s if and only if the following conditions are satisfied for all $i \geq 1$:

(1) if $s = r$ then $t_{i+k} = f(t_i \ldots t_{i+k-1})$;

(2) if $s = l$ then $t_{-i-k} = f(t_{-i-k+1} \ldots t_{-i})$.

A both-hand side infinite sequence $U \in A_{-\infty}^{\infty}$ is said to be an output sequence of a k-net N_k if and only if the following conditions are satisfied:

(3) if $i \geq 0$ then $U(i+k,i+k) = f(U(i,i+k-1))$;

(4) if $i < 0$ then $U(i-k,i-k) = f(U(i-k+1,i))$.

L e m m a 3.1. A nonempty set $E \subseteq A^{\infty}$ or $E \subseteq A_{-\infty}$ is a set of all output sequences of some k-register R_k^s if and only if the following conditions are satisfied:

(5) for each $x \in A^k$ there is unique sequence $T \in E$ such that $x = T(1,k)$;

(6) E is k-homogeneous.

Proof in [7] has been given.

T h e o r e m 3.1. A nonempty set $E \subseteq A_{-\infty}^{\infty}$ is the set of all output sequences of some k-net N_k ($k \geq 2$) if and only if the following conditions are satisfied:

(7) for each $x \in A^k$ there is unique sequence $T \in E$ such that $x = T(0,k-1)$;

(8) E is both-hand side k-homogeneous; this means that for all sequences $T,U \in E$ and the integers i,j we have:

(8.1) if $i \geq 0$, $j \geq 0$ and $T(i,i+k-1) = U(j,j+k-1)$ then $T(i+k,i+k) = U(j+k,j+k)$;

(8.2) if $i < 0$, $j < 0$ and $T(i-k+1,i) = U(j-k+1,j)$ then $T(i-k,i-k) = U(j-k,j-k)$;

(8.3) if $i \geq 0$, $j < 0$ and $T(i,i+k-1) = U(j-k+1,j)$ then $T(i-k,i-k) = U(j-k,j-k)$.

Proof immediately follows from Lemma 3.1.

4. Definable sets by the k-nets

A characteristics of the k-nets by means of the finite sets of right-hand side infinite sequences of successive their states will be given.

Let us introduce at the beginning the necessary definitions.

Let $R_k^s = (A^k, F^s)$ be a k-register and $N_k = (A^k, (F^r, F^l))$ - a k-net.

An infinite sequence $\underline{X} = x_1, x_2, \ldots \in (A^k)^\infty$ is said to be generable by R_k^s if and only if $x_{i+1} = F^s(x_i)$ for all $i \geq 1$.

The set of all sequences generable by R_k^s will be called a definable set by it and will be denoted by $D(R_k^s)$.

An infinite double sequence $\underline{X} = (x_1,y_1),(x_2,y_2),\ldots \in (A^k \times A^k)^\infty$ is said to be generable by N_k if and only if $x_{i+1} = F^r(x_i)$ and $y_{i+1} = F^l(x_i)$ for all $i \geq 1$.

The set of all sequences generable by N_k will be called a definable set by it and denoted by $D(N_k)$.

R e m a r k 4.1. $D(N_k)$ consists of only periodic sequences if and only if $D(R_k^r)$ and $D(R_k^l)$ have the same property. Theorem 2.1 formulates the respective conditions for periodicity of $D(N_k)$.

The necessary and sufficient condition for a nonempty set $G \subseteq (A^k)^\infty$ ($\underline{G} \subseteq (A^k \times A^k)^\infty$) to be definable by some k-register R_k^s (a k-net N_k) will be formulated.

L e m m a 4.1. A nonempty set $G \subseteq (A^k)^\infty$ is definable by some k-register R_k^s if and only if the following conditions are satisfied:

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

(2) G is 1-homogeneous;

(3) for arbitrary segments $G(i,i) = \{x_1,\ldots,x_{n^k}\}$ and $G(i+1,i+1) = \{y_1,\ldots,y_{n^k}\}$ $(i \geq 1)$ the following conditions are satisfied:

(3.1) if $s = r$ then $y_j(1,k-1) = x_j(2,k)$;

(3.2) if $s = l$ then $y_j(2,k) = x_j(1,k-1)$

for all $1 \leq j \leq n^k$.

The proof immediately follows from Lemma 3.1.

C o r o l l a r y 4.1. For arbitrary k-register R_k^s its definable set G consists of only pseudoperiodic sequences with the period of length less or equal to $|A^k|$.

T h e o r e m 4.1. A nonempty set $\underline{G} \subseteq (A^k \times A^k)^\infty$ is definable by some k-net N_k if and only if the following conditions are satisfied:

(4) for each $(x,y) \in A^k \times A^k$ there is unique sequence $(x_1,y_1),(x_2,y_2),\ldots \in \underline{G}$ such that $(x,y) = (x_1,y_1)$;

(5) if we denote by $\underline{G}^i$, $i = 1,2$ the sets:
$\underline{G}^1 = \{x_1,x_2,\ldots \in (A^k)^\infty : (\exists (x_1,y_1),(x_2,y_2),\ldots \in \underline{G})\}$;
$\underline{G}^2 = \{y_1,y_2,\ldots \in (A^k)^\infty : (\exists (x_1,y_1),(x_2,y_2),\ldots \in \underline{G})\}$
then $\underline{G}^1$ and $\underline{G}^2$ are 1-homogeneous;

(6) for each $i \geq 1$ and a sequence $(x_1,y_1),(x_2,y_2),\ldots \in \underline{G}$ we have:
$x_{i+1}(1,k-1) = x_i(2,k)$ and $y_{i+1}(2,k) = y_i(1,k-1)$.

Proof is obvious.

C o r o l l a r y 4.2. For arbitrary k-net N_k all sequences generable by it are pseudoperiodic with the period of length less or equal to $|A^{2k}|$.

5. Relational k-nets

A notion of an relational k-net will be introduced. A relational k-net is an immediate generalization of a k-net.

Formal definition and the basic properties of the sets which are definable by such nets will be given.

By a relational k-net RN_k $(k \geq 2)$ we mean a quadruple (A^k,F^r,F^l,R), where F^r and F^l are the transition functions which in section 2 have been defined and $R \subseteq A^k \times A^k$ is an arbitrary relation.

A sequence $X = (x_1,y_1),(x_2,y_2),\ldots \in (A^k \times A^k)^\infty$ is said to be generable by a relational k-net $N_k = (A^k,F^r,F^l,R)$ if and only if the following conditions are satisfied:

(1) $$(x_{i+1},y_{i+1}) = \begin{cases} (F^r(x_i),F^l(y_i)) & \text{if } (x_i,y_i) \in R \\ (F^l(x_i),F^r(y_i)) & \text{otherwise.} \end{cases}$$

The set of all sequences generable by RN_k is said to be definable by it and denoted by $D(RN_k)$.

It follows immediately from the above definition the following corollary.

C o r o l l a r y 5.1. For arbitrary relational k-net $N_k = (A^k, F^r, F^l, R)$ we have:

(2) if $R = A^k \times A^k$ then $D(RN_n) = D(N_k)$ where $N_k = (A^k, (F^r, F^l))$ is a k-net;

(3) if $R = \emptyset$ then $D(RN_k) = D(N_k')$, where $N_k' = (A^k, (F^l, F^r))$ is a k-net.

The transition graph of a relational k-net can be defined analogously as for a k-net.

T h e o r e m 5.1. Let $RN_k = (A^k, F^r, F^l, R)$ $(k \geq 2)$ be a relational k-net and f - its feedback function.

The following conditions are equivalent:

(1) all the connected components of the transition graph $G(RN_k)$ form a cycle;

(2) $D(RN_k)$ consists of only periodic sequences;

(3) both the transition functions F^r and F^l are the mappings of A^k onto A^k;

(4) for all $t_1 \ldots t_{k-1} \in A^{k-1}$ and $a, b \in A$ $(a \neq b)$ we have:

(4.1) $f(at_1 \ldots t_{k-1}) \neq f(bt_1 \ldots t_{k-1})$

(4.2) $f(t_1 \ldots t_{k-1}a) \neq f(t_1 \ldots t_{k-1}b)$.

P r o o f . The equivalence of the conditions (1) and (2) as well as (3) and (4) is obvious. It is sufficient to prove the equivalence of the conditions (2) and (3). Let us see that the condition (2) implies (3) because otherwise it would be $E(i,i) \subset (A^k)^2$ for some $i \geq 1$, where $E = D(RN_k)$. The inverse implication is obvious.

C o r o l l a r y 5.1. For arbitrary relational k-net RN_k all sequences generable by it are pseudoperiodic with the period length less or equal to $|A^{2k}|$.

If there is a periodic sequence $X \in D(RN_k)$ with the period length of $|A^{2k}|$ then all sequences generable by RN_k have the same property.

T h e o r e m 5.2. A nonempty set $\underline{G} \subseteq (A^k \times A^k)^\infty$ $(k \geq 2)$ is definable by some relational k-net if and only if the following conditions are satisfied:

(5) for arbitrary $(x,y) \in A^k \times A^k$ there is unique sequence $\underline{X} \in \underline{G}$ such that $(x,y) = \underline{X}(1,1)$;

(6) $\underline{G}$ is 1-homogeneous;

(7) for each $i \geq 1$ and a sequence $(x_1,y_1),(x_2,y_2),\ldots \in \underline{G}$ exactly one of the following conditions is satisfied:

(7.1) $x_{i+1}(1,k-1) = x_i(2,k)$ and $y_{i+1}(2,k) = y_i(1,k-1)$,

(7.2) $x_{i+1}(2,k) = x_i(1,k-1)$ and $y_{i+1}(1,k-1) = y_i(2,k)$.

Proof is obvious.

For the class of relational k-nets many problems are open. We will put forward the following three problems:

(8) give an algorithm for the construction of a whole class of the relational k-nets generating only periodic sequences with period length of $|A^{2k}|$;

(9) solve the synthesis problem for the class of the relational k-nets as have been stated in [8] for another class of the controlled shift-registers;

(10) introduce a few kinds of homomorphisms for the class of the relational k-nets.

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, Dusseldorf, 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] H. F r e d r i c k s e n : A survey of full length non-linear shift-register algorithm, SIAM Rev. 24 (1982), 195-221.

[5] S.W. G o l o m b : Shift-register sequences. Holden Day, San Francisco, Cambridge, London, Amsterdam 1967.

[6] Ju.V. G o l u n k o v : Microprogram bases on shift--registers with four feedbacks, Vierojatnostnyje Metody i Kibernetika, N 12-13 (1976), 33-39.

[7] Z. G r o d z k i : The theory of shift-registers. Information and Control, Vol. 21, N 3 (1972), 196-205.

[8] Z. G r o d z k i : Synthesis problem for deterministic controlled (k-m)-shift-registers, Demonstratio Math. 20 (1987) 547-559.

[9] Z. G r o d z k i , M. Ł a t k o : The nets of conjugated shift-registers. Problems of Control and Information Theory 17 (3) (1988), 159-170.

[10] R. L i d l , H. N i e d e r r e i t e r : Finite fields, Encyclopedia of Math. and Applications, Vol. 20 (1983), Addison-Wesley Reading, Mass. 1983.

[11] Ch. R o n s e : Feedback shift-registers, Lecture Notes in Computer Science, ed. G.Goss, J.Hartmanis, Springer Verlag, Berlin, Heidelberg, New York, Tokyo 1984.

DEPARTMENT OF MATHEMATICS, TECHNICAL UNIVERSITY,
20-618 LUBLIN, POLAND
Received March 25, 1987.