DEMONSTRATIO MATHEMATICA
Vol. XII No 4 1979

Zdzisław Grodzki, Marian Sagan

CONSTRUCTION OF (k, m)-REGISTERS GENERATING SEQUENCES WITH LONG CYCLES

1. Introduction

This paper is related to deterministic (k,m)-registers. The basic notions as well as the fundamental properties of the sets of all sequences generated by the registers of this class have been given in [3], [4], [5]. The (k,m)-registers generate only cyclic sequences.

With respect to eventual use of (k,m)-registers in practice, the most useful ones are those which generate sequences with long cycles.

The subclass of (k,m)-registers generating sequences with the maximal cycle length, equal $2^k m$, has not been sufficiently investigated. For example, till now, there has not been given an algorithm for constructing at least one such (k,m)-register. Necessary and sufficient conditions on feedback functions of a (k,m)-register $R_{k,m}$, such that sequences generable by it are of maximal cycles, have not been formulated, either.

We are not going to solve the above problems but we shall construct some (k,m)-registers generating sequences with long cycles. Such a (k,m)-register is obtained from the given one by changing its transition function for some states. The idea of this construction is based on Yoeli's method [8] which has been used in [6], [7], [8] for the case m =1. In most cases the

above method allows us to obtain as a final result sequences with the maximal cycles.

In the opinion of the authors the considerations of this paper allow one to solve easily at least one of the previous open problems.

2. Basic definitions

Let N denote the set of all nonnegative integers (called here numbers). Elements of N will be denoted by lower case Latin letters i,j,k,m,n,p,q,r,s.

Let $M = \{0,1\}$ and let M^k for $k \geq 1$ denote the set of all sequences of the length k, over M.

The elements of M^k will be denoted by upper case Latin letters A,B,C,D (possibly with subscripts).

M^∞ denotes the set of all infinite sequences over M. The elements of M^∞ will be denoted by upper case Latin letters T,U,V,W,X,Y,Z (possibly with subscripts).

If $T = t_1,t_2,\ldots \in M^\infty$, then $T|_{i,j}$ for $1 \leq i \leq j$ denotes a restricted sequence $t_i,\ldots,t_j$ and $T|_i$ - an infinite sequence $t_i,t_{i+1},\ldots$.

The nonempty subsets of M^∞ will be denoted by upper case Latin letters E,F,G,H.

Now we shall recall basic definitions from [3].

Let $k \geq 1$ and $m \geq 1$ be arbitrary (fixed) numbers.

D e f i n i t i o n 2.1. By a (k,m)-register $R_{k,m}$ we mean an ordered $(m+1)$ - tuple $< M, \varphi_1,\ldots,\varphi_m >$ where every φ_i for $1 \leq i \leq m$ is a Boolean function from M^k into M.

Each φ_i $(1 \leq i \leq m)$ will be called a feedback function of $R_{k,m}$ and the function $\Phi_i : M^k \to M^k$ defined as follows:

$$(1) \qquad \Phi_i(t_1,\ldots,t_k) = (t_2,\ldots,t_k, \varphi_i(t_1,\ldots,t_k))$$

will be called the transition function of $R_{k,m}$.

Only (k,m) - registers with injective transition functions will be considered here.

L e m m a 2.1. For an arbitrary (k,m)-register $R_{k,m} = \langle M, \varphi_1, \ldots, \varphi_m \rangle$ each transition function Φ_i $(1 \leq i \leq m)$ is injective if and only if the following condition is satisfied:

$$(2) \qquad \varphi_i(\bar{x}_1, x_2, \ldots, x_k) = \overline{\varphi_i(x_1, \ldots, x_k)}$$

for all $(x_1, \ldots, x_k) \in M^k$ where $\bar{y} = 1$ when $y = 0$ and $\bar{y} = 0$ - otherwise.

The proof of Lemma 2.1 has been given in [6].

D e f i n i t i o n 2.2. An infinite sequence $T = t_1, t_2, \ldots \in M^\infty$ is said to be generable by a (k,m)-register $R_{k,m} = \langle M, \varphi_1, \ldots, \varphi_m \rangle$ if and only if the following condition is satisfied:

$$(3) \qquad \bigvee_{n \geq 0} \bigvee_{p \leq m} (t_{k+mn+p} = \varphi_p(t_{mn+p}, \ldots, t_{k+mn+p-1})).$$

The set of all sequences generable by $R_{k,m}$ will be denoted by $G(R_{k,m})$.

D e f i n i t i o n 2.3. An infinite sequence $T = t_1, t_2, \ldots \in M^\infty$ is said to be cyclic if and only if the following condition is satisfied:

$$(4) \qquad \bigexists_{i \geq 1} \bigexists_{j \geq 1} \bigvee_{p \geq i} (t_p = t_{p+j}).$$

Let M^0 denote the set of all cyclic sequences $T = t_1, t_2, \ldots$ with the pure cycle i.e. such that $t_p = t_{p+j}$ for all $p \geq 1$ and some $j \geq 1$.

D e f i n i t i o n 2.4. Let $T \in M^\infty$ be a cyclic sequence and p the minimal number of all numbers i for which the condition (4) is satisfied.

By a tail of T we mean the sequence $T|_{1,p}$, if $p > 0$, or the empty sequence ε if $p = 0$.

D e f i n i t i o n 2.5. A sequence $t_{p+1}, \ldots, t_{p+q}$ is said to be a cycle of T if and only if q is the least number j for which the condition (4) holds.

L e m m a 2.2. Let $R_{k,m} = \langle M, \varphi_1, \ldots, \varphi_m \rangle$ be a (k,m)-register and Φ_i for $1 \leq i \leq m$ its transition functions.

$G(R_{k,m}) \subset M^0$ if and only if each Φ_i is injective.

The proof of Lemma 2.2 has been given in [2].

3. Complexity degree of (k,m)-registers

We shall introduce a notion of complexity degree of a (k,m)-register which will be useful for the further discussion.

At the beginning we shall introduce some auxiliary notions.

D e f i n i t i o n 3.1. Let $\psi : M^k \longrightarrow M^k$ be a total injective function.

Let us define a relation $R_\psi \subseteq M^k \times M^k$ as follows:

$$(1) \qquad \bigwedge_{A \in M^k} \bigwedge_{B \in M^k} \left((A,B) \in R_\psi \Leftrightarrow \bigvee_{p \geq 1} (\psi^p(A) = B) \right).$$

We shall write $A \, R_\psi \, B$ instead of $(A,B) \in R_\psi$.

T h e o r e m 3.1. For each total injective function $\psi : M^k \longrightarrow M^k$, R_ψ is the equivalence relation of M^k.

The proof of Theorem 3.1 results from Lemma 2.2.

Let $R_{k,m} = \langle M, \varphi_1, \ldots, \varphi_m \rangle$ be a (k,m)-register and Φ_i for $1 \leq i \leq m$ its transition function.

A new function $\psi_i : M^k \longrightarrow M^k$ is defined as follows:

$$(2) \qquad \psi_i = \Phi_i \circ \Phi_{i+1} \circ \cdots \circ \Phi_{i-1} \quad \text{when} \quad 1 \leq i \leq m,$$

where the composition $\pi_1 \circ \pi_2$ is understood as $\pi_2(\pi_1(A))$.

It follows from Theorem 3.1 that the relation R_{ψ_i} which has been defined in Definition 3.1 is the equivalence relation of M^k.

The set $\left\{ B \in M^k : A \, R_{\psi_i} \, B \right\}$ is denoted by $\left[A\right]_{R_{\psi_i}}$.

The set of all equivalence classes of R_{ψ_i} will be denoted by $\left[\, \right]_{R_{\psi_i}}$.

L e m m a 3.1. For each (k,m)-register $R_{k,m} = \langle M, \varphi_1, \ldots, \varphi_m \rangle$ we have

$$(3) \qquad \bigvee_{1 \leq i \leq m} \bigvee_{A \in M^k} \bigvee_{B \in M^k} \left(A \, R_{\psi_i} \, B \leftrightarrow \phi_i(A) R_{\psi_{i \oplus 1}} \phi_i(B) \right),$$

where $i \oplus 1 = i + 1$ for $1 \leq i \leq m-1$ and $i \oplus 1 = 1$ for $i = m$.

The proof of Lemma 3.1 is obvious and immediately follows from the definition of the relation R_{ψ_i}.

L e m m a 3.2. For every (k,m)-register $R_{k,m} = \langle M, \varphi_1, \ldots, \varphi_m \rangle$ we have

$$(4) \qquad \bigvee_{i \leq m} \bigvee_{j \leq m} \left(\operatorname{card} [\,]_{R_{\psi_i}} = \operatorname{card} [\,]_{R_{\psi_j}} \right).$$

The proof of Lemma 3.2 immediately follows from Lemma 3.1.

D e f i n i t i o n 3.2. By the complexity degree of a (k,m)-register $R_{k,m} = \langle M, \varphi_1, \ldots, \varphi_m \rangle$ (denoted by $\deg(R_{k,m})$) we mean the cardinality of $[\,]_{R_{\psi_1}}$.

R e m a r k 3.1. The condition $\deg(R_{k,m}) = 1$ is equivalent to the following one:

$$(5) \qquad \bigvee_{T \in G(R_{k,m})} \bigvee_{i \geq 1} \left(\left\{ T \middle| _{i+jm, i+jm+k-1} : j = 0, 1, \ldots, 2^k - 1 \right\} = M^k \right).$$

4. Reduction of complexity degree of (k,m)-registers

In order to obtain a (k,m)-register with less complexity degree than the given one, a method taken from [6], [8] will be used here. Repeating this method we are able to obtain a maximal (k,m)-register.

Let $R_{k,m} = \langle M, \varphi_1, \ldots, \varphi_m \rangle$ be a (k,m)-register and $A = (x_1, \ldots, x_k)$, $B = (y_1, \ldots, y_k)$ - the arbitrary states.

D e f i n i t i o n 4.1. A and B are said to be conjugated in j-th coordinate ($1 \leq j \leq k$) if and only if $x_j = \bar{y}_j$ and $x_i = y_i$ for all $i \neq j$.

D e f i n i t i o n 4.2. A pair (A,B) is said to be a switching over for the function ϕ_i (or in the class $[A]_{R_{\psi_i}}$ if and only if A and B are conjugated in the first coordinate and the equivalence classes $[A]_{R_{\psi_i}}$, $[B]_{R_{\psi_i}}$ are disjoint.

E x a m p l e 4.1. Let $\deg(R_{k,m}) = 2$, $[A]_{R_{\psi_i}} \cap [B]_{R_{\psi_i}} = \phi$ for $1 \leq i \leq m$ and let A, B be the conjugated states in the first coordinate.

Let us define a (k,m)-register $S_{k,m} = \langle M, \pi_1, \ldots, \pi_m \rangle$ as follows:

$$\pi_i(t_1,\ldots t_k) = \begin{cases} \overline{\phi_i(t_1,\ldots t_k)} \text{ when } (t_2,\ldots t_k) = (x_2,\ldots x_k) \\ \phi_i(t_1,\ldots t_k) \text{ - for the other cases.} \end{cases}$$

Table 1 illustrates the above definition

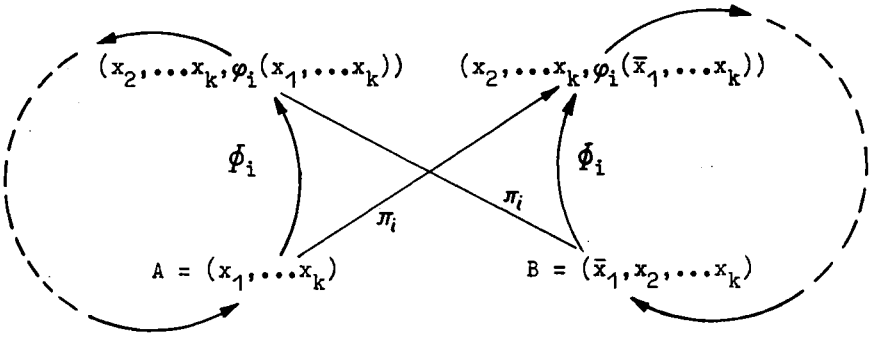

Table 1

It follows immediately from the definition of π_i that $\deg(S_{k,m}) = 1$.

R e m a r k 4.1. A similar argument leads to the conclusion that changing 0 into 1, and conversely, in the value

of some feedback function φ_i of a (k,m)-register $R_{k,m}$ (analogously as before), for each two states A and B which are conjugated in the first coordinate, results in obtaining a new (k,m)-register $S_{k,m}$ generating cycles of which at least one is longer than any cycle of the (k,m)-register $R_{k,m}$. Additionally it should be observed that if (A,B) is not a switching over pair, one of the cycles of the (k,m)-register $R_{k,m}$ is dissected into two smaller cycles. These cycles are obtained by dissection of some cycle of the sequence generated by $R_{k,m}$.

R e m a r k 4.2. The analogical consideration as in Example 4.1 is for the case of $\deg(R_{k,m}) = p > 2$. Using the above construction we obtain a (k,m)-register $S_{k,m}$ such that $\deg(S_{k,m}) = p-1$.

The question arises whether a switching over pair exists for each (k,m)-register $R_{k,m} = \langle M,\varphi_1,\ldots,\varphi_m\rangle$ such that $\deg(R_{k,m}) > 1$. The answer is positive. We are going to prove that if for all feedback functions φ_i $(1 \leq i \leq m)$ and each $A \in [\ ]_{R_{\psi_i}}$ there is a state $B \in [A]_{R_{\psi_I}}$ which is conjugated with A in the first coordinate, (i.e. there is not a switching over pair for ψ_i in $[\ ]_{R_{\psi_i}}$) then we have $\deg(R_{k,m})=1$.

At the beginning we are going to prove two auxiliary lemmas.

Let $R_{k,m} = \langle M,\varphi_1,\ldots,\varphi_m\rangle$ be a (k,m)-register and $A \in M^k$ - an arbitrary state.

L e m m a 4.1. If for each $B \in [A]_{R_{\psi_i}}$ there is an element in this class which is conjugated with B in the first coordinate, then for each $B_1 \in [\phi_i(A)]_{R_{\psi_{i\oplus 1}}}$ there is an element in this class which is conjugated with B_1 in k-th coordinate.

P r o o f . Let $B = (y_1,\ldots,y_k) \in [\phi_i(A)]_{R_{\psi_{i\oplus 1}}}$. Let $\phi_i(B_1) = B$ where $B_1 = (y_o,\ldots,y_{k-1}) \in [A]_{R_{\psi_i}}$. Then for the state B_1 there is a state $B_2 = (\bar{y}_o,y_1,\ldots,y_{k-1}) \in [A]_{R_{\psi_i}}$

which is conjugated with B_1 in the first coordinate. Let $B_3 = \phi_i(B_2) \in [\phi_i(A)]_{R_{\psi_{i\oplus 1}}}$. Because ϕ_i is injective, $B_3 = (y_1,\ldots,y_{k-1},\bar{y}_k)$. Q.E.D.

L e m m a 4.2. It has been assumed that for each element B_1 in any class $[A]_{R_{\psi_i}}$ there is an element in this class which is conjugated with B_1 in $(r+1)$-th coordinate $(r < k)$ and that for each element B_2 of the class $[\phi_i(A)]_{R_{\psi_{i\oplus 1}}}$ there is an element B_3 in this class conjugated with B_2 in k-th coordinate. Then for each $B \in [\phi_i(A)]_{R_{\psi_{i\oplus 1}}}$ there is $D \in [\phi_i(A)]_{R_{\psi_{i\oplus 1}}}$ which is conjugated with B in r-th coordinate.

P r o o f . Let $B = (y_1,\ldots y_r,\ldots y_k) \in [\phi_i(A)]_{R_{\psi_{i\oplus 1}}}$. Let $\phi_i(B_1) = B$, (i.e. $B_1 = (y_0,y_1,\ldots y_r,\ldots y_{k-1}) \in [A]_{R_{\psi_i}}$). It follows from the assumption that $B_2 = (y_0,\ldots\bar{y}_r,\ldots y_{k-1}) \in [A]_{R_{\psi_i}}$. Let $B_3 = \phi_i(B_2)$. Then we have $B_3=(y_1,\ldots\bar{y}_r,\ldots\tilde{y}_k) \in [\phi_i(A)]_{R_{\psi_{i\oplus 1}}}$. If $\tilde{y}_k = y_k$ then B_3 is conjugated with B in the r-th coordinate. If $\tilde{y}_k = \bar{y}_k$, then it follows from the assumption that for B_3 there is $B_4 \in [\phi_i(A)]_{R_{\psi_{i\oplus 1}}}$, which is conjugated with it in the k-th coordinate. This element has the form $B_4 = (y_1,\ldots,\bar{y}_r,\ldots,y_k)$ and it is conjugated with B in the r-th coordinate. Q.E.D.

T h e o r e m 4.1. If for every equivalence class $[A]_{R_{\psi_1}}$, $[\phi_1(A)]_{R_{\psi_2}}$, $[\phi_1\circ\phi_2(A)]_{R_{\psi_3}}$ $\ldots$ $[\phi_1\circ\ldots\circ\phi_{m-1}(A)]_{R_{\psi_m}}$ for each element $B \in [\phi_1\circ\ldots\circ\phi_i(A)]_{R_{\psi_{i\oplus 1}}}$ there is an element in this class which is conjugated with B in the first coordinate, then we have $\deg(R_{k,m}) = 1$.

P r o o f . It follows from Lemmas 4.1 and 4.2 that there is equivalence class $[D]_{R_{\psi_i}}$ $(i \leq m)$ belonging to

the classes which in Theorem 4.1 have been defined so that for each $B \in [D]_{R_{\psi_i}}$ there is $C \in [D]_{R_{\psi_i}}$ which is conjugated with B in arbitrary coordinate. This means that $[D]_{R_{\psi_i}} = M^k$. It follows from Theorem 3.2 that $\deg(R_{k,m}) = 1$. Q.E.D.

C o r o l l a r y 4.1. If for a (k,m)-register $R_{k,m}$ with $k < m$ for successive equivalence classes $[A]_{R_{\psi_1}}$ ... $[\phi_1 \circ \ldots \circ \phi_{k-1}(A)]_{R_{\psi_k}}$ there are no conjugated pairs in the first coordinate then $\deg(R_{k,m}) = 1$.

R e m a r k 4.1. If we have a (k,m)-register $R_{k,m}$ with $k < m$ it is sufficient to change the value of k successive feedback functions for switching over pairs in order to obtain a (k,m)-register $R_{k,m}$ such that $\deg(R_{k,m}) = 1$. The question is whether it is possible to obtain the above result by changing less than k feedback functions. The answer is negative.

E x a m p l e 4.1. Let us define a (2,4)-register $R_{2,4} = \langle M, \varphi_1, \varphi_2, \varphi_3, \varphi_4 \rangle$ as follows:

$\varphi_i(00) = 1$ for $1 \leq i \leq 3$ and $\varphi_4(00) = 0$,
$\varphi_i(01) = 1$ for $1 \leq i \leq 4$,
$\varphi_i(10) = 0$ for $1 \leq i \leq 3$ and $\varphi_4(10) = 1$,
$\varphi_i(11) = 0$ for $1 \leq i \leq 4$.

A sequence $T = t_1, t_2, \ldots$ generable by a (2,4)-register $R_{2,4}$ with initial state 00 has the cycle 00110110.

It is easy to verify that (10) is an element of $[00]_{R_{\psi_4}}$ and (00,10) is not a switching over pair. But for the functions ϕ_3 and ϕ_1 there are switching over pairs (for ϕ_3 - (11,01),(10,00) and for ϕ_1 - (00,10),(01,11)). The functions ϕ_2 and ϕ_4 have not switching over pairs, but each two successive functions $\phi_1 \circ \phi_2$, $\phi_2 \circ \phi_3$, $\phi_3 \circ \phi_4$, $\phi_4 \circ \phi_1$ have ones.

Therefore we are not able to reduce the complexity degree by changing the value of individual feedback function.

T h e o r e m 4.2. For all $k \geq 1$ and $m \geq 1$ there is a (k,m)-register $R_{k,m}$ such that $\deg(R_{k,m}) = 1$.

P r o o f . Taking into consideration an arbitrary (k,m)-register $S_{k,m}$ with $\deg(S_{k,m}) > 1$, we are able to construct (using method of Example 1.4) a (k,m)-register $R_{k,m}$ such that $\deg(R_{k,m}) = \deg(S_{k,m}) - 1$ and so on. Q.E.D.

Open problems:

1) What is the maximal complexity degree of (k,m)-registers?
2) Find a construction of at least one (k,m)-register with the maximal complexity degree.
3) The condition $\deg(R_{k,m}) = 1$ does not always imply that $R_{k,m}$ generates only sequences with maximal cycle length. Give reasons for this fact.

REFERENCES

[1] H. F r e d r i c k s e n : Generation of the Ford sequences of length 2^n, J.Comb.Theory 12(1972) 153-154.

[2] S.W. G o l o m b : Shift-register sequences, San Francisco 1976.

[3] Z. G r o d z k i : The controlled shift-registers, Elektron. Informationsverarbeit. Kybernetik 3(1975) 143-150.

[4] Z. G r o d z k i : The Boolean controlled shift-registers, ibid 7/8 (1975) 459-467.

[5] Z. G r o d z k i , J. Ż u r a w i e c k i : Equivalence problem for deterministic (k,m) shift-registers, Demonstratio Math. 10(1977) 629-636.

[6] W. S k a r b e k , K. Z e m b r z u s k i : On maximal cycles of the Boolean k-registers In Polish Prace COPAN 245, Warszawa 1976.

[7] J. Ż u r a w i e c k i : Boolean shift-registers, Demonstratio Math. 10(1977) 405-415.

[8] M. Y o e l i : Couting with nonlinear binary feedback shift-registers, I.E.E.E. Transactions on Electronic Computers (1963) 357-361.

INSTITUTE OF MATHEMATICS, TECHNICAL UNIVERSITY, LUBLIN
INSTITUTE OF MATHEMATICS, HIGHER SCHOOL OF ENGINEERING, RADOM
Received June 24, 1978.