DEMONSTRATIO MATHEMATICA
Vol. X No 3-4 1977

Z. Grodzki, J. Żurawiecki

EQUIVALENCE PROBLEM FOR DETERMINISTIC (k, m)-SHIFT-REGISTERS

1. Introduction

The great use of shift-registers in practice is well known and will not be recalled here the reader is referred to Golomb's monograph [1]). For all these applications the general desire is to have the sequences with a large cycle length. With respect to this practical need a class of controlled (k,m)-shift-registers has been introduced in [2]. Every such (k,m)-register consists of a memory with k cells and of m transition functions $\varphi_1,\ldots,\varphi_m$, where every φ_i is a partial function from M^k into M (M is a finite alphabet). Given an initial state $t_1,\ldots,t_k$ a (k,m)-register generates an infinite sequence $T = t_1,t_2,\ldots$ as follows: $t_{k+1} = \varphi_1(t_1,\ldots,t_k),\ldots,t_{k+m} = \varphi_m(t_m,\ldots,t_{k+m-1})$ and so on. If $T = t_1,\ldots,t_n$ $(n > k)$ then $t_{n-k+1},\ldots,t_n$ does not belong to the domain of respective transition function φ_i [1]. The (k,m)-registers generating only of infinite sequences will be considered. For such registers the following questions arise.

Is the (k,m)-register $R_{k,m}$ uniquely generating the set E? Is m the least number of all numbers q such that E is generable by any (k,q)-register?

---

[1] Only (k,m)-registers with total transition functions have been considered in [2].

Several classes of registers are indicated for which the first problem has a unique solution. As an application of the second problem the possibility of reduction of transition functions is shown. This is of great importance in practice. This one is similar to minimization problem for Boolean functions.

2. Notations and definitions

Let $M = \{a_1,\dots,a_n\}(n > 1)$ be a fixed alphabet and M^* - the set of all sequences (finite and infinite) over M. M^∞ denotes the subset of all infinite sequences of M^* and $M^0 \subset M^\infty$ - the subset of all cyclic sequences $T = t_1,t_2,\dots$ such that $t_i = t_{i+j}$ for all $i \geqslant 1$ and some $j \geqslant 1$.

If $T = t_1,t_2,\dots$ is an element of M^*, then $T|_{i,j}$ for $1 \leqslant i \leqslant j \leqslant l(T)$ denotes a sequence $t_i,\dots,t_j$, where $l(T)$ is the length of T. $T|_i$ denotes a sequence $t_i,\dots,t_j$, if $l(T) = j$ or an infinite sequence $t_i,t_{i+1},\dots$, if $l(T)=\infty$.

For every nonempty set $E \subseteq M^*$ consisting only of sequences of the length greater or equal to j, $E|_{i,j}$ $(i \leqslant j)$ denotes the restriction of the set E to the interval $\langle i,j\rangle$ i.e.

$$E|_{i,j} = \left\{ T \in M^* : \exists_{U \in E}\ T = U|_{i,j} \right\}.$$

Analogously, $E|_i$ denotes the set $\left\{T \in M^* : \exists_{U \in E} T=U|_i\right\}$.

The functions are denoted by lower case Greek letters $\pi, \varphi, \psi, \omega$. D_π and R_π denote the domain and the range of the function π.

Now we shall give some necessary definitions.

Let $k \geqslant 1$ and $m \geqslant 1$ be two arbitrary but fixed positive integers.

D e f i n i t i o n 1. By a (k,m)- register $R_{k,m}$ we mean an ordered $(m+1)$- tuple $\langle M, \varphi_1,\dots\varphi_m\rangle$, where every φ_i for $1 \leqslant i \leqslant m$ is a partial function from M^k into M.

we shall assume that $D_{\varphi_i} \neq \emptyset$ for all i, $1 \leqslant i \leqslant m$.

D e f i n i t i o n 2. A sequence $T = t_1, t_2, \ldots$ (finite and of the length greater that k or infinite) is said to be generable by a (k,m)-register $R_{k,m} = \langle M, \varphi_1, \ldots, \varphi_m \rangle$ iff the following conditions are satisfied:

$$(1) \qquad \bigwedge_{n \geq 0} \bigwedge_{p \leq m} \left[k+mn+p \leq l(T) \Rightarrow t_{k+mn+p} = \varphi_p(t_{mn+p}, \ldots, t_{k+mn+p-1}) \right];$$

$$(2) \qquad \bigwedge_{n \geq 0} \bigwedge_{p \leq m} \left[l(T) = k+mn+p-1 \Rightarrow (t_{mn+p}, \ldots, t_{k+mn+p-1}) \notin D_{\varphi_p} \right].$$

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

The class of all (k,m)-registers $R_{k,m}$ such that $GR_{k,m} \subseteq M^0$ will be denoted by $D^{k,m}$.

D e f i n i t i o n 3. A nonempty set $E \subseteq M^*$ is said to be a (k,m)-definable set iff there is a (k,m)-register $R_{k,m}$ such that $E = GR_{k,m}$.

D e f i n i t i o n 4. A nonempty $E \subseteq M^*$ is said to be (k,m) homogeneous iff the following condition holds

$$(3) \qquad \bigwedge_{T \in E} \bigwedge_{U \in E} \bigwedge_{i < l(T)-k} \bigwedge_{j \geq 0} \left[i+jm+k \leq l(U) \wedge T|_{i,i+k-1} = U|_{i+jm,i+jm+k-1} \Rightarrow T|_{i+k} = U|_{i+jm+k} \right].$$

3. Basic theorems

A few properties of (k,m)-definable sets will be given.

T h e o r e m 1. A nonempty set $E \subseteq M^*$ is a (k,m)-definable set iff the following conditions are satisfied

$$(4) \qquad \bigwedge_{T \in E} (l(T) > k);$$

(5) $$\bigvee_{T\in E}\ \bigvee_{i\geqslant 0}\left[l(T|_{im+1}) > k \Rightarrow T|_{im+1} \in E\right];$$

(6) E is (k,m)-homogeneous.

C o r o l l a r y 1. A nonempty set $E \subseteq M^{\infty}$ is a (k,m)-definable set iff the condition (6) and the following one are satisfied

(7) $$\bigvee_{i\geqslant 0}\ (E|_{im+1} \subseteq E).$$

Let $R_{k,m} = \langle M, \varphi_1, \ldots, \varphi_m\rangle$ be an arbitrary (k,m)-register and $E = GR_{k,m}$.

T h e o r e m 2. $E \subseteq M^{0}$ iff the following condition holds

(8) $$\bigvee_{i\geqslant 1}\ (E|_{1,k} = E|_{i,i+k-1}).$$

Proofs of Theorems 1 and 2 for the (k,m)-registers with total transition functions have been given in [1] and [2], respectively. The extension for the case where $R_{k,m}$ consists of partial transition functions is immediate.

T h e o r e m 3. $E \subseteq M^{\infty}$ iff the following condition holds

(9) $$\bigvee_{i\leqslant m}\ (E|_{i,i+k-1} \subseteq D_{\varphi_i}).$$

The proof is obvious.

4. Equivalence of (k,m)-registers

In this and next section only the (k,m)-registers $R_{k,m}$ with partial transition functions such that $GR_{k,m} \subseteq M^{\infty}$ will be considered.

A necessary and sufficient condition for two (k,m)-registers to be equivalent will be given.

D e f i n i t i o n 5. Two registers $R_{k,m}$ and $S_{k,p}$ are said to be equivalent (denoted by $R_{k,m} \sim S_{k,m}$) iff $GR_{k,m} = GS_{k,m}$.

C o r o l l a r y 2. The relation $\sim$ is an equivalence relation in the set of all (k,m)-registers (k is a fixed number and m - an arbitrary one).

Let $R_{k,m} = \langle M, \varphi_1, \ldots, \varphi_m \rangle$, $S_{k,m} = \langle M, \psi_1, \ldots, \psi_m \rangle$ be two (k,m)-registers and $E = GR_{k,m}$, $F = GS_{k,m}$.

T h e o r e m 4. $R_{k,m} \sim S_{k,m}$ iff the following conditions are satisfied[1)]

$$D_{\varphi_1} = D_{\psi_1} \tag{10}$$

$$\bigwedge_{i \leq m} \bigwedge_{U \in E|_{i,i+k-1}} \left[U \in D_{\psi_i} \Leftrightarrow \varphi_i(U) = \psi_i(U) \right]. \tag{11}$$

Necessity. The proof is by way of contradiction. If (10) is not satisfied then we have immediately $E \neq F$.

Suppose now that the following condition holds

$$\bigvee_{i \leq m} \bigvee_{U \in E|_{i,i+k-1}} \left[U \notin D_{\psi_i} \vee \varphi_i(U) \neq \psi_i(U) \right]. \tag{12}$$

Then there are two sequences $T \in E$, $U \in F$ such that $T|_{1,i+k-1} \neq U|_{1,i+k-1}$ $(i \leq m)$ and $T \neq U$. Therefore we have $E \neq F$.

The proof of sufficiency is obvious.

C o r o l l a r y 3. Suppose that (k,m)-registers $R_{k,m}$ and $S_{k,m}$ are of the class $D^{k,m}$ (i.e. $E \subseteq M^0$ and

---

1) If we omit the assumption that $E \subseteq M^\infty$ then the condition (11) should be replaced by the following one

$$\bigwedge_{i \leq m} \bigwedge_{U \in E|_{i,i+k-1}} \left[(U \in D_{\varphi_i} \cup D_{\psi_i}) \vee (U \in D_{\varphi_i} \cap D_{\psi_i} \Rightarrow \varphi_i(U) = \psi_i(U)) \right]$$

$F \subseteq M^0$). Then $R_{k,m} \sim S_{k,m}$ iff the condition (10) and the following one are satisfied

$$(13) \qquad \bigvee_{i \leq m} \bigvee_{U \in D_{\varphi_i}} (\varphi_i(U) = \psi_i(U)).$$

E x a m p l e 1. Let us define a (3,3)-register $R_{3,3} = \langle M, \varphi_1, \varphi_2, \varphi_3 \rangle$ as follows $D_{\varphi_i} = M^3$, $\varphi_i(U) = 1$ for all $U \in M^3$ and $1 \leq i \leq 3$.

An arbitrary (3,3)-register $S_{3,3} = \langle M, \psi_1, \psi_2, \psi_3 \rangle$ defined as follows $\varphi_1 = \psi_1$; $G = \{001, 011, 101, 111\} \subseteq D_{\psi_2}$ and $\psi_2(U) = 1$ for all $U \in G$; $H = \{011, 111\} \subseteq D_{\psi_3}$ and $\psi_3(U) = 1$ for all $U \in H$ is equivalent to $R_{3,3}$. Its generable sequence have the form: 00(1), 00(1), 010(1), 0(1), 100(1), 10(1), 110(1), (1), where $b_1,\ldots,b_n(b_{n+1})$ denotes a cyclic sequence $T = t_1,t_2,\ldots$ such that $t_i = b_i$ for all i, $1 \leq i \leq n$ and $t_j = b_{n+1}$ for all $j > n$.

5. Reducibility problem for (k,m)-registers

The problem when for a (k,m)-register $R_{k,m}$ there exists an equivalent (k,p)-register $S_{k,p}$ with $p \leq m$ will be considered. A necessary and sufficient condition for a (k,m)-register $R_{k,m}$ to be reducible will be given.

Let $R_{k,m} = \langle M, \varphi_1,\ldots,\varphi_m \rangle$ be a (k,m)-register and $E = GR_{k,m}$.

D e f i n i t i o n 6. $R_{k,m}$ is said to be p-reducible for $1 \leq i \leq m$ iff there is a (k,p)-register $S_{k,p}$ equivalent to $R_{k,m}$.

If $p \neq m$ then $R_{k,m}$ is said to be reducible.

C o r o l l a r y 4. $R_{k,m}$ is reducible iff there is a (k,p)-register $S_{k,p} = \langle M, \psi_1,\ldots,\psi_p \rangle$ such that $\varphi_i = \psi_i$ for $1 \leq i \leq p$ and $R_{k,m} \sim S_{k,p}$.

T h e o r e m 5. A (k,m)-register $R_{k,m}$ is p-reducible ($p \leq m$) iff the following condition is satisfied

$$(14) \qquad \bigvee_{i \geq 0} (E|_{im+p+1} \subseteq E).$$

P r o o f . Necessity. As E is (k,m)-definable set then it follows from Corollary 1 that

$$(15) \qquad \bigvee_{i \geq 0} (E|_{im+1} \subseteq E).$$

Since $R_{k,m}$ is p - reducible then the following inclusion holds

$$(16) \qquad \bigvee_{j \geq 0} (E|_{jp+1} \subseteq E).$$

Putting in (16) $j = 1$ and taking into considerations (15) we obtain (14).

Proof of sufficiency immediately follows from (14), (15) and Corollary 1.

C o r o l l a r y 5. For every p - reducible (k,m)-register $R_{k,m} \in D^{k,m}$ there is a unique (k,p)-register $S_{k,p}$ such that $R_{k,m} \sim S_{k,p}$.

T h e o r e m 6. Let $R_{k,m}$ be a p-reducible (k,m)-register of class $D^{k,m}$. If p is the least number of all numbers q for which $R_{k,m}$ is q-reducible, then m is divisible by p.

P r o o f . Necessity. Suppose that E is p-reducible for $p \leq m$ and m is not divisible by p. Let q be such a number that $pq < m$ and $p(q+1) > m$. It is easy to see that E is pq - reducible. As $E \subseteq M^0$ then it follows from Theorems 2 and 5 that $E = E|_{pq+1}$. Since E is (k,m)-definable set then we have $E = E|_{m+1}$. Hence we obtain

$$(17) \qquad E = E|_{m-pq+1}.$$

Using (17) and Theorem 5 we obtain that E is $(m - pq)$-reducible, where $m - pq < p$. Therefore p is not the least number such that E is p - reducible and Theorem 6 has been proved.

R e m a r k 2. If in Theorem 6 we omit the assumption that $R_{k,m} \in D^{k,m}$, then the obtained statement is false.

E x a m p l e 2. Let us define a (3,3)-register $R_{3,3} = \langle M, \varphi_1, \varphi_2, \varphi_3 \rangle$ as follows $\varphi_1(U) = 1$ for all $U \in M^3$, $\varphi_2(001) = 0$ and $\varphi_2(V) = 1$ for all $V \in M^3 - \{001\}$, $\varphi_3(W) = 1$ for all $W \in M^3$. The definable set by $R_{3,3}$ has the form $\{00010(1), 010(1), 10010(1), 110(1), 00(1), 0(1), 10(1), (1)\}$. Consider now a (3,2)-register $S_{3,2} = \langle M, \varphi_1, \varphi_2 \rangle$. It is easy to verify that $R_{3,3} \sim S_{3,2}$. Therefore $R_{3,3}$ is 2 - reducible, but it is not 1 - reducible.

REFERENCES

[1] S.W. G o l o m b : Shift - register sequences, San Francisco 1967.

[2] Z. G r o d z k i : The controlled shift - registers, Elektronische Informationsverarbeitung und Kybernetik 11 (1975) 143 - 150.

[3] Z. G r o d z k i , J. Ż u r a w i e c k i : The (k,m)-computation sets, Reports on Mathematical Logic 6(1976), 79-86.

INSTITUTE OF MATHEMATICS, HIGHER ENGINEERING SCHOOL, LUBLIN
Received June 26, 1976.