A SET GENERATED BY A MATRIX OVER A FINITE COMMUTATIVE RING

Taizo SADAHIRO[1] Ken KURIYAMA[2]

1 Department of Administration, Kumamoto Prefectural University

2 Department of Kansei Design Engineering, Faculty of Engineering, Yamaguchi University

A combinatorial problem was posed in relation to the theory of stochastic automata [1]. The problem is whether there exists a subset of $\{0,1,\dots r-1\}^m$ with a combinatorial property called (m,k)-property. When $r=2$, we have shown the existence of such a subset by giving an algorithm to construct it [2]. The method has been to use the number of dimensions of subspaces of $(\mathbf{Z}/2\mathbf{Z})^m$ and the binomial theorem. This paper shows an algorithm to construct such a subset as a submodule of $(\mathbf{Z}/r\mathbf{Z})^m$ for any integer $r \geq 2$.

Key Words *: finite ring,submodule of* $(\mathbf{Z}/r\mathbf{Z})^m$*,* (m,k)*-property.*

Throughout this paper by *k-consecutive* we mean possibly *cyclically* consecutive elements of length k: Let $k < m$ be positive integers and let $\mathbf{a} = (a_1, a_2, \dots, a_m)$ be a sequence of length m. The following m sequences

$$(a_1,\dots,a_k),(a_2,\dots,a_{k+1}),\dots,$$
$$(a_{m-k+1},\dots,a_m),(a_{m-k+2},\dots,a_m,a_1),\dots,$$
$$(a_m,a_1,\dots,a_{k-1})$$

are the k-consecutive subsequences of $\mathbf{a}$ *starting with position* $1,2,\dots,m$ respectively.

Definition 1. *A set* $L \subseteq \{0,1,\dots,r-1\}^m$ *has* (m,k)-property *if for any distinct* $a,b \in L$ *(considered as sequences of length m), the k-consecutive subsequences of a and b starting with position i are distinct for every* $i \in \{1,\dots,m\}$.

Clearly, such a set L has cardinality at most r^k. Suppose a k by m matrix over $\mathbf{Z}/r\mathbf{Z}$ satisfies the following condition:

(*) For every $i \in \{1,2,\dots,m\}$, k row vectors of k by k submatrix obtained by k-consecutive columns with starting point i are linearly independent over $\mathbf{Z}/r\mathbf{Z}$.

Then the submodule generated by its k row vectors is a rank-k free submodule of $(\mathbf{Z}/r\mathbf{Z})^m$with (m,k)-property.

Theorem 1. *Let r be a positive integer. There exists a subset of* $\{0,1,\dots,r-1\}^m$ *which has* (m,k)*-property and has* r^k *elements.*

Proof. We will show we can construct a k by m matrix with property (*) by induction on m. In the case $m=k$, k by k unit matrix satisfies the condition(*). Let M_m be a k by m matrix over $\mathbf{Z}/r\mathbf{Z}$ which satisfies the condition(*) and one more condition:

(+) The k by k matrix which consists of the first k columns of M_m is an upper triangular matrix and the k by k matrix of the last k columns is a lower lower triangular matrix.

Clearly the unit matrix satisfies this condition. Let $\mathbf{e}_i$ be the ith row vector of M_m and put

$$M_{m+1} = \begin{pmatrix} \mathbf{e}_1 - \mathbf{e}_2 & 0 \\ \mathbf{e}_2 - \mathbf{e}_3 & 0 \\ \vdots & \vdots \\ \mathbf{e}_{k-1} - \mathbf{e}_k & 0 \\ \mathbf{e}_k & 1 \end{pmatrix}.$$

Then M_{m+1} is a k by $m+1$ matrix which satisfies the condition (*) and (+). □

Example 1. $r = 2$ *and* $k = 3$

- $m = 3$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

- $m = 4$

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

- $m = 5$

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

References

[1] Taiho Kanaoka and Singo Tomita,: Homogeneous Decomposition of Stochastic Systems, *Theoretical Computer Science,* 40 pp245-255, 1985

[2] Taizo Sadahiro, Taiho Kanaoka, Shingo Tomita and Ken Kuriyama, An application of Galois Field to a combinatorial problem in stochastic system (in Japanese), *Journal of the faculty of liberal arts of Yamaguchi University,* 29 pp55-58, 1995

(Received May 15, 1998)

ある有限可換環上の行列が生成する集合について

貞広 泰造, 栗山 憲

確率オートマトンの問題の中で現れるある組み合わせ的な性質をもつ集合を有限環 $\mathbf{Z}/r\mathbf{Z}$ 上の加群として構成できることを示す。