J. Math. Soc. Japan
Vol. 22, No. 4, 1970

Spectrum of a substitution minimal set

By Teturo KAMAE

(Received Jan. 19, 1970)

§ 1. Summary

K. Jacobs ([1]) reported as an example of Toeplitz type sequences that

```
0 0 0 0 0 0 0 0 0 0 0 0 0 0 ···
 1   1   1   1   1   1     ···
   0       0       0       ···
       1               1   ···
               0           ···
= 0100010101000100010001010 ···
```

is strictly ergodic and has a rational pure point spectrum. This sequence has the following properties:

(i) It is a shift of the sequence 001000101010001··· which is invariant under the substitution $0 \to 0010$, $1 \to 1010$ of length 4.

(ii) The $(2i+1)$-th symbol of it is 0 for $i=0, 1, 2, \cdots$.

In this paper, we prove that if some general conditions like (i) (ii) above are satisfied for a sequence over some finite alphabet, then it is strictly ergodic and has a rational pure point spectrum. That is, our main results are the followings:

I. If M is a minimal set associated with a substitution of some constant length, then M is strictly ergodic.

II. Let M be a strictly ergodic set associated with a substitution of length p^k, where p is a prime number and k is any positive integer. Assume that for some (or, equivalently, any) $\alpha \in M$, there exist integers $h \geqq 0$ and $r \geqq 1$, such that (ip^h+r)-th symbol of α is the same for $i=0, 1, 2, \cdots$. Then, M has a rational pure point spectrum $\{\omega ; \omega^{p^i}=1 \text{ for some } i=0, 1, 2, \cdots\}$.

§ 2. Notations and definitions

Let C be any finite set of symbols which contains at least two elements. Let $N=\{0, 1, 2, \cdots\}$ be the set of non-negative integers. Let T be the shift transformation on the power space C^N. That is, T is defined as follows:

$$(T\alpha)(n)=\alpha(n+1),$$

where $\alpha\in C^N$ and $n\in N$. For $p\in N$, let $N_p=\{0, 1, \cdots, p-1\}$. Let $C^*=\bigcup_{p\in N} C^{N_p}$ be the disjoint sum, where $C^{N_0}=\{\Lambda\}$ and Λ is the empty sequence. C^N or C^* may be considered as the set of infinite or finite sequences over C, respectively. We identify C^{N_1} with C. $L(\xi)$ denotes the length of $\xi\in C^*$. That is, $L(\xi)$ equals k, such that $\xi\in C^{N_k}$. For $\alpha\in C^N$, define $L(\alpha)=\infty$. For $\xi\in C^*$ and $\alpha\in C^*\cup C^N$, the *juxtaposition* of ξ and α in this order is denoted by $\xi*\alpha$, that is,

$$(\xi*\alpha)(n)=\begin{cases}\xi(n) & \cdots \text{ if } 0\leqq n\leqq L(\xi)-1\\ \alpha(n-L(\xi)) & \cdots \text{ if } L(\xi)\leqq n\leqq L(\xi)+L(\alpha)-1.\end{cases}$$

For $\xi\in C^*$ and $\alpha\in C^*\cup C^N$, ξ is called a *prefix* or a *section* of α, if there exists η, such that $\alpha=\xi*\eta$, or if there exist η and ζ, such that $\alpha=\eta*\xi*\zeta$, respectively. For $\xi\in C^*$ and $\eta\in C^*$, ξ is called a *suffix* of η, if there exists ζ, such that $\eta=\zeta*\xi$. For $\xi\in C^*$, $\Gamma_\xi=\{\alpha\in C^N;\ \xi \text{ is a prefix of } \alpha\}$ denotes the cylinder set. C^N is a topological space with the family of cylinder sets as its open base. For $\alpha\in C^N$, denote

$$\text{range}(\alpha)=\{\alpha(n)\in C;\ n\in N\}$$

$$\text{Orb}(\alpha)=\{T^n\alpha;\ n\in N\}$$

$$\overline{\text{Orb}}(\alpha)=\text{closure of Orb}(\alpha).$$

For the notions such as a *minimal set*, a *strictly ergodic* (*i. e.* minimal and *uniquely ergodic*, at the same time) *set* or an *almost periodic sequence* and their properties about shift dynamical system (C^N, T), refer [**2**] and [**5**]. Let $S\subset C^N$ be a strictly ergodic set. There uniquely exists a probability measure μ on S (with respect to the Borel field on S), such that T is a measure preserving transformation on S for μ. Consider the Hilbert space $L_2(S, \mu)$ over complex numbers. Let U be the isometrical linear operator on $L_2(S, \mu)$, such that $(Uf)(\alpha)=f(T\alpha)$, where $f\in L_2(S, \mu)$ and $\alpha\in S$. U is uniquely determined by the strictly ergodic set S. U is called to *have a pure point spectrum*, if there exists a base $\{f_i\}$ of $L_2(S, \mu)$ each term of which is a proper function of U ([**6**]). By a proper value or a proper function of S or α, such that $\overline{\text{Orb}}(\alpha)=S$, we mean those of U defined above. Also, by the statement that S or α, such that $\overline{\text{Orb}}(\alpha)=S$, has a pure point spectrum, we mean that U has a pure point spectrum.

By a *substitution of length* $p\geqq 2$, we mean a function defined on C which takes values on C^{N_p}. By a *homogeneous substitution*, we mean a substitution of length p for some $p\geqq 2$. Let θ be any homogeneous substitution. We extend θ to a function $C^*\cup C^N\to C^*\cup C^N$ which we also denote by θ, as follows:

$$\theta(\alpha)=\theta(\alpha(0))^*\theta(\alpha(1))^*\theta(\alpha(2))^*\cdots,$$

which belongs to C^* or C^N as $\alpha\in C^*$ or C^N, respectively. Let θ be any homogeneous substitution. A minimal set $S\subset C^N$ is called to be *associated with* θ, if $\theta(S)\subset S$. A minimal set is called a *homogeneous substitution minimal set,* if there exists a homogeneous substitution with which it is associated. For the general properties of a substitution minimal set on a space of two-sided sequences, refer [**3**].

For integers $p\geqq 2$ and $n\geqq 0$, let

$$n=\sum_{i=0}^{k-1}a_i p^{k-i-1}$$

$$(a_0\neq 0 \text{ if } n\neq 0,\ 0\leqq a_i\leqq p-1;\ i=0,1,\cdots,k-1)$$

be the p-adic development of n. Define $p(n)\in N_p^*$ by $p(n)(i)=a_i$ $(i=0,1,\cdots,k-1)$. Let $p\geqq 2$ be any integer. By a *finite-state machine* over N_p, we mean a quadruple $M=(K,\delta,q_0,\tau)$, where K is any nonempty finite set, δ is a function $K\times N_p\to K$, q_0 is any element of K, and τ is a function $K\to C$. δ is called the *next state function* of M. We extend δ to a function $K\times N_p^*\to K$ which we also denote by δ, so as to satisfy $\delta(q,\xi^*\eta)=\delta(\delta(q,\xi),\eta)$ for any $q\in K$ and $\xi,\eta\in N_p^*$. Define $\lambda_M^{(p)}\in C^N$ by $\lambda_M^{(p)}(n)=\tau(\delta(q_0,p(n)))$, where $n\in N$. For any integer $p\geqq 2$, F_p denotes the set of $\alpha\in C^N$, such that $\alpha=\lambda_M^{(p)}$ for some finite-state machine M over N_p. And, $\tilde{F}_p$ denotes the set of $\alpha\in C^N$, such that $\alpha=\lambda_M^{(p)}$ for some finite-state machine $M=(K,\delta,q_0,\tau)$ over N_p, such that τ is a one-to-one mapping. Denote

$$F=\bigcup_{p\geqq 2}F_p.$$

An element of F is called a *finite-rank sequence* over C. $\alpha\in C^N$ is called an *ultimately periodic sequence,* if there exists a non-negative integer n, such that $T^n\alpha$ is a periodic sequence. It is known ([**4**]) that for multiplicatively independent integers $p, p'\geqq 2$, $F_p\cap F_{p'}$ equals the set of all ultimately periodic sequences.

Let $M=(K,\delta,q_0,\tau)$ be a finite-state machine over N_p $(p\geqq 2)$. We define the following notions:

DEFINITION 1. Let $q,q'\in K$. Denote $q\sim q'$ (M), if for any $\xi\in N_p^*$, $\tau(\delta(q,\xi))=\tau(\delta(q',\xi))$ holds. The negation of $q\sim q'$ (M) is denoted by $q\nsim q'$ (M).

DEFINITION 2. The next state function δ is called *strongly connected,* if for any $q,q'\in K$, there exists $\xi\in N_p^*$, such that $\delta(q,\xi)=q'$.

DEFINITION 3. $\xi\in N_p^*$ is called a *reset sequence* (of M), if for any $q,q'\in K$, $\delta(q,\xi)\sim\delta(q',\xi)$ (M) holds. A reset sequence ξ is called a *minimal reset sequence,* if any suffix $(\neq\xi)$ of ξ is not a reset sequence.

DEFINITION 4. Let $X_0, X_1, X_2, \cdots$ be a sequence of independent and identically distributed random variables each of which takes values on N_p with equal probability $1/p$. For any non-negative integer n and $q, q' \in K$, let

$$P_{qq'}^{(n)} = \text{Prob}\,\{\delta(q, X_0 * X_1 * \cdots * X_{n-1}) = q'\}\,.$$

Then, the system of transition probabilities $\{P_{qq'}^{(n)};\, q, q' \in K, n \in N\}$ defines on K a stationary Markov chain, which we call the *Markov chain associated with* δ.

§ 3. Strictly ergodicity

LEMMA 1. *$T\alpha \in F_p$ if and only if $\alpha \in F_p$, where $p \geqq 2$ is any integer.*

PROOF. Assume that $\alpha \in F_p$ and $\alpha = \lambda_M^{(p)}$, where $M = (K, \delta, q_0, \tau)$ is a finite-state machine over N_p. Let $K' = K \times K$. Define a function $\delta' : K' \times N_p \to K'$, as follows:

$$\delta'((q, q'), n) = \begin{cases} (\delta(q', n+1), \delta(q', n)) & \cdots \text{ if } 0 \leqq n \leqq p-2 \\ (\delta(q, 0), \delta(q', p-1)) & \cdots \text{ if } n = p-1\,. \end{cases}$$

Let $q_0' = (q_1, q_0)$, where $q_1 = \delta(q_0, 1)$. Let $\tau' : K' \to C$ be a function, such that $\tau'((q, q')) = \tau(q)$. Let $M' = (K', \delta', q_0', \tau')$. Then, it is easily verified that $T\alpha = \lambda_{M'}^{(p)}$. Conversely, let $T\alpha \in F_p$ and $T\alpha = \lambda_M^{(p)}$, where $M = (K, \delta, q_0, \tau)$ is a finite-state machine over N_p. Let $K' = N_3 \times K \times K$. Define a function $\delta' : K' \times N_p \to K'$, as follows:

$$\delta'((i, q, q'), n) = \begin{cases} (1, q, q') & \cdots \text{ if } i = 0 \text{ and } n = 0 \\ (2, \delta(q, p-1), \delta(q', 0)) & \cdots \text{ if } i \neq 0 \text{ and } n = 0 \\ (2, \delta(q', n-1), \delta(q', n)) & \cdots \text{ otherwise}\,. \end{cases}$$

Let $q_0' = (0, q_0, q_0)$. Let $\tau' : K' \to C$ be a function, such that

$$\tau'((i, q, q')) = \begin{cases} \alpha(0) & \cdots \text{ if } i = 1 \\ \tau(q) & \cdots \text{ otherwise}\,. \end{cases}$$

Let $M' = (K', \delta', q_0', \tau')$. Then, we have $\alpha = \lambda_{M'}^{(p)}$.

LEMMA 2. *Let $p \geqq 2$ be any integer. We have $F_{p^k} = F_p$ for $k = 1, 2, 3, \cdots$.*

PROOF. Being clear.

LEMMA 3. *Let $p \geqq 2$ be any integer. Let $M = (K, \delta, q_0, \tau)$ be any finite-state machine over N_p, such that δ is strongly connected and $\delta(q_0, 0) = q_0$. Then, $\lambda_M^{(p)}$ is an almost periodic sequence.*

PROOF. Let Card $K = r+1$. Since δ is strongly connected and $\delta(q_0, 0) = q_0$, for any $q \in K$, there exists $\xi \in N_p^*$ of length r, such that $\delta(q, \xi) = q_0$. Let $0 \leqq j \leqq k$ be any integers. Let $L(p(k)) = s$. For any integer $h \geqq 0$, there exists an integer $n \geqq 1$, such that

$$h \leqq np^{r+s} < (n+1)p^{r+s}-1 \leqq h+2p^{r+s}-1 .$$

Furthermore, there exists $\xi \in N_p^*$ of length r, such that $\delta(q_0, p(n)*\xi)=q_0$. Let $p(m)=p(n)*\xi$. Then, we have

$$h \leqq mp^s+j \leqq mp^s+k \leqq h+2p^{r+s}-1$$

and $\delta(q_0, p(mp^s+i))=\delta(q_0, p(i))$ for $i=j, j+1, \cdots, k$. Therefore, $\lambda_M^{(p)}(mp^s+i)=\lambda_M^{(p)}(i)$ for $i=j, j+1, \cdots, k$. Since h was arbitrary, this means that the section

$$\lambda_M^{(p)}(j)*\lambda_M^{(p)}(j+1)*\cdots*\lambda_M^{(p)}(k)$$

of $\lambda_M^{(p)}$ appears in any section of $\lambda_M^{(p)}$ of length $2p^{r+s}$. This completes the proof.

LEMMA 4. *Let $p \geqq 2$ be any integer. Let $M=(K, \delta, q_0, \tau)$ be a finite-state machine over N_p, such that δ is strongly connected and $\delta(q_0, 0)=q_0$. Then, for any $c \in C$,*

$$\frac{\text{Card}\{i;\ \lambda_M^{(p)}(i)=c,\ k \leqq i \leqq k+n-1\}}{n}$$

converges uniformly for $k \geqq 0$ as $n \to \infty$.

PROOF. Let $\{P_{qq'}^{(n)};\ q, q' \in K, n \in N\}$ be the system of transition probabilities of the Markov chain associated with δ. Since this Markov chain is non-cyclic and ergodic, for any $c \in C$, there exists a real number $0 \leqq \omega \leqq 1$, such that

$$\lim_{n\to\infty} \sum_{q' \in \tau^{-1}(c)} P_{qq'}^{(n)}=\omega$$

for any $q \in K$. For sufficiently small $\varepsilon>0$, let d be an integer, such that $n \geqq d$ means

$$\sup_{q \in K} \left| \sum_{q' \in \tau^{-1}(c)} P_{qq'}^{(n)}-\omega \right| \leqq \frac{\varepsilon}{2} .$$

Let $n \geqq \frac{4}{\varepsilon}p^d$ be any integer. Let $m=\left[\frac{n}{p^d}\right]-1$. Let k be any non-negative integer. Then, there exists an integer $h \geqq 1$, such that

$$k \leqq hp^d < (h+m)p^d-1 \leqq k+n-1 .$$

Let $j \geqq 1$ be any integer. Let $\delta(q_0, p(j))=q$. Then, we have

$$\frac{\text{Card}\{i;\ \lambda_M^{(p)}(i)=c,\ jp^d \leqq i \leqq (j+1)p^d-1\}}{p^d}=\sum_{q' \in \tau^{-1}(c)} P_{qq'}^{(d)} .$$

Therefore, it is easily verified that

$$\left| \frac{\text{Card}\{i;\ \lambda_M^{(p)}(i)=c,\ k \leqq i \leqq k+n-1\}}{n}-\omega \right| \leqq \varepsilon .$$

This completes the proof.

LEMMA 5. *Let* $p \geqq 2$ *be any integer. Let* $\alpha \in F_p$ *be any almost periodic sequence. Then, there exist a positive integer* k *and a finite-state machine* $M' = (K', \delta', q_0', \tau')$ *over* N_{pk}, *such that*

(i) δ' *is strongly connected and* $\delta'(q_0', 0) = q_0'$,

(ii) $\lambda_{M'}^{(p^k)} \in \overline{\mathrm{Orb}}(\alpha)$.

Moreover, if $\alpha \in \tilde{F}_p$, *then*

(iii) τ' *is one-to-one*,

in addition to (i) (ii).

PROOF. Let $\alpha = \lambda_M^{(p)}$, where $M = (K, \delta, q_0, \tau)$ is a finite-state machine over N_p (τ is one-to-one, if $\alpha \in \tilde{F}_p$). Let $E \subset K$ be any ergodic component of the Markov chain associated with δ, such that $\delta(q_0, p(n)) \in E$ for some positive integer n. It is easily seen that there exist $q_0' \in E$ and a positive integer k, such that

$$\delta(q_0', \underbrace{0*0*\cdots*0}_{k}) = q_0' .$$

Define

$$\eta^{(i)} = \underbrace{0*0*\cdots*0}_{k-L(p(i))}*p(i)$$

for $i = 0, 1, \cdots, p^k - 1$. Define a function $\delta'' : E \times N_{pk} \to E$, as $\delta''(q, i) = \delta(q, \eta^{(i)})$, where $q \in E$ and $i \in N_{pk}$. The extension of δ'' to a function $E \times N_{pk}^* \to E$ is also denoted by δ''. Let

$$K' = \{q \in E ;\ \delta''(q_0', \xi) = q \text{ for some } \xi \in N_{pk}^*\} .$$

The restriction of δ'' to $K' \times N_{pk}^*$ is denoted by δ'. Then, δ' is a function $K' \times N_{pk}^* \to K'$ which is strongly connected and satisfies $\delta'(q_0', 0) = q_0'$. Let τ' be the restriction of τ to K'. Let $M' = (K', \delta', q_0', \tau')$. Then, M' satisfies (i) (and (iii), if $\alpha \in \tilde{F}_p$). Let m be a positive integer, such that $\delta(q_0, p(m)) = q_0'$. For any positive integer j, let $h = mp^{kj}$. Then, it is easily seen that

$$\lambda_{M'}^{(p^k)}(i) = \lambda_M^{(p)}(h+i)$$

for $i = 0, 1, \cdots, p^{kj} - 1$. Thus, we have the condition (ii).

Let $\alpha \in C^N$. For a positive integer k, let D be the k products of C. Define $\varphi_k(\alpha) \in D^N$, as follows:

$$\varphi_k(\alpha)(n) = (\alpha(n),\ \alpha(n+1), \cdots, \alpha(n+k-1)) \in D ,$$

where $n \in N$.

LEMMA 6. *If* $\alpha \in F$, *then* $\varphi_k(\alpha)$ *is a finite-rank sequence over* D.

PROOF. Let $\alpha \in F_p$ ($p \geqq 2$). Then, from Lemma 1, $T^i\alpha \in F_p$ for $i = 0, 1, 2, \cdots$. For $i = 0, 1, \cdots, k-1$, let $M^{(i)} = (K^{(i)}, \delta^{(i)}, q_0^{(i)}, \tau^{(i)})$ be a finite-state machine over

N_p, such that $\lambda_M^{(p)}(i) = T^i\alpha$. Let $K = K^{(0)} \times K^{(1)} \times \cdots \times K^{(k-1)}$. Define a function $\delta: K \times N_p \to K$ and $\tau: K \to D$, as follows:

$$\delta((q^{(0)}, q^{(1)}, \cdots, q^{(k-1)}), n) = (\delta^{(0)}(q^{(0)}, n), \delta^{(1)}(q^{(1)}, n), \cdots, \delta^{(k-1)}(q^{(k-1)}, n))$$

$$\tau(q^{(0)}, q^{(1)}, \cdots, q^{(k-1)}) = (\tau^{(0)}(q^{(0)}), \tau^{(1)}(q^{(1)}), \cdots, \tau^{(k-1)}(q^{(k-1)})),$$

where $(q^{(0)}, q^{(1)}, \cdots, q^{(k-1)}) \in K$ and $n \in N_p$. Let $q_0 = (q_0^{(0)}, q_0^{(1)}, \cdots, q_0^{(k-1)})$. Let $M = (K, \delta, q_0, \tau)$. Then, we have $\lambda_M^{(p)} = \varphi_k(\alpha)$.

THEOREM 1. *Let $S \subset C^N$ be any minimal set which intersects with F. Then, S is a strictly ergodic set.*

PROOF. It is sufficient to prove that for any $\xi \in C^*$ (ξ is not the empty sequence), there exists $\gamma \in S$, such that

$$\frac{\text{Card}\,\{i;\ h \leqq i \leqq h+n-1 \text{ and } \xi \text{ is a prefix of } T^i\gamma\}}{n}$$

converges uniformly for $h \geqq 0$ as $n \to \infty$. Let $L(\xi) = k$. Let $\alpha \in S \cap F$. Let D be the k products of C. Then, $\varphi_k(\alpha)$ is an almost periodic and finite-rank sequence over D. From Lemma 4 and Lemma 5, there exists $\beta \in \overline{\text{Orb}}\,(\varphi_k(\alpha)) \subset D^N$, such that

$$\frac{\text{Card}\,\{i;\ \beta(i) = (\xi(0), \xi(1), \cdots, \xi(k-1)),\ h \leqq i \leqq h+n-1\}}{n}$$

converges uniformly for $h \geqq 0$ as $n \to \infty$. Since $\overline{\text{Orb}}\,(\varphi_k(\alpha)) = \varphi_k(\overline{\text{Orb}}\,(\alpha)) = \varphi_k(S)$, there exists $\gamma \in S$, such that $\varphi_k(\gamma) = \beta$. It is easily seen that γ satisfies the required property.

COROLLARY 1. *Let $S \subset C^N$ be a homogeneous substitution minimal set. Then, S is a strictly ergodic set.*

To prove Corollary 1, it is sufficient to prove the following lemma.

LEMMA 7. *Let $S \subset C^N$ be a minimal set associated with a substitution θ of length $p \geqq 2$. Then, there exists a positive integer k, such that S intersects with $\tilde{F}_{p^k}$.*

PROOF. It is easily seen that there exist a positive integer k and $\alpha \in S$, such that $\theta^k(\alpha) = \alpha$. Let $K = \text{range}\,(\alpha)$. Define a function $\delta: K \times N_{p^k} \to K$, as follows:

$$\delta(q, n) = \text{the } (n+1)\text{-th symbol of } \theta^k(q) = \theta^k(q)(n),$$

where $q \in K$ and $n \in N_{p^k}$. Let q_0 be the initial symbol of α. Let $\tau: K \to K \subset C$ be the identity mapping. Let $M = (K, \delta, q_0, \tau)$. Then, we have $\alpha = \lambda_M^{(p^k)}$ and τ is one-to-one.

§ 4. Spectrum

Lemma 8. *Let* $M=(K, \delta, q_0, \tau)$ *be a finite-state machine over* N_p $(p \geqq 2)$, *such that* $\lambda_M^{(p)} \in C^N$ *is not an ultimately periodic sequence. Then, there exist* $q, q' \in K$ *and* $\xi \in N_p^*$, *such that*

(i) $\xi \neq \Lambda$, $q \nsim q'(M)$

(ii) $\delta(q, \xi)=q$, $\delta(q', \xi)=q'$.

Proof. Assume that there do not exist $q, q' \in K$ and $\xi \in N_p^*$ satisfying the above (i) (ii). Let $\mathrm{Card}\, K=r$. Let $\eta \in N_p^*$ be any sequence of length r^2. Assume that $\delta(q_1, \eta) \nsim \delta(q_2, \eta)$ (M) for some $q_1, q_2 \in K$. There exists $\xi \neq \Lambda$, such that $\eta=\eta' * \xi * \eta''$ for some $\eta', \eta'' \in N_p^*$, and

$$\delta(q_1, \eta')=\delta(q_1, \eta' * \xi) \tag{1}$$

$$\delta(q_2, \eta')=\delta(q_2, \eta' * \xi) . \tag{2}$$

Let $q=\delta(q_1, \eta')$ and $q'=\delta(q_2, \eta')$. Then, q, q' and ξ satisfy (i) (ii) above, contradicting our assumption. Thus, $\delta(q_1, \eta) \sim \delta(q_2, \eta)$ (M) for any $q_1, q_2 \in K$, and η is a reset sequence. Since any $\eta \in N_p^*$, such that $L(\eta)=r^2$, is a reset sequence, $\lambda_M^{(p)}$ must be an ultimately periodic sequence.

Lemma 9. *Let* $M=(K, \delta, q_0, \tau)$ *be a finite-state machine over* N_p $(p \geqq 2)$, *such that* $\lambda_M^{(p)}$ *is not an ultimately periodic sequence. Assume that* M *has at least one reset sequence. Then, for any* n, *there exists a minimal reset sequence* ξ, *such that* $L(\xi) \geqq n$.

Proof. Let $\eta \in N_p^*$ be a reset sequence. From Lemma 8, there exists $\zeta \in N_p^*$, such that $L(\zeta) \geqq n$, which is not a reset sequence. Since $\eta * \zeta$ is a reset sequence and ζ is not, there exists a minimal reset sequence ξ which has ζ as its suffix. This completes the proof.

Lemma 10. *Let* $M=(K, \delta, q_0, \tau)$ *be a finite-state machine over* N_p $(p \geqq 2)$, *such that* τ *is one-to-one,* δ *is strongly connected, and* $\delta(q_0, 0)=q_0$. *Let* $\mathrm{Card}\, K=k$. *Assume that*

$$\lambda_M^{(p)}(ip^h+r)=\lambda_M^{(p)}(r)$$

for $i=0, 1, \cdots, 2p^{2k}-1$, *where* h *and* r *are non-negative integers. Let*

$$\xi=\begin{cases} \underbrace{0*0*\cdots*0}_{h-L(p(r))}*p(r) \cdots \textit{if } h \geqq L(p(r)) \\ \textit{suffix of } p(r) \textit{ of length } h \cdots \textit{if } h<L(p(r)) . \end{cases}$$

Then, ξ *is a reset sequence, and*

$$\lambda_M^{(p)}(ip^h+r)=\lambda_M^{(p)}(r)$$

holds for any integer $i \geqq -\left[\frac{r}{p^h}\right]$.

PROOF. Let $b=\left[\frac{r}{p^h}\right]$. There exists an integer $n\geqq 1$, such that

$$b\leqq np^{2k}<np^{2k}+p^{2k}-1\leqq b+2p^{2k}-1\,.$$

Since δ is strongly connected and $\delta(q_0, 0)=q_0$, for any $q, q'\in K$, there exists $\eta\in N_p^*$, such that $L(\eta)=2k$ and $\delta(q, \eta)=q'$. Let $q=\delta(q_0, p(n))$ and q' be any state. Let η be as above. Let $p(m)=p(n)*\eta$. Since $0\leqq m-b\leqq 2p^{2k}-1$, we have

$$\begin{aligned}\tau(\delta(q', \xi))&=\tau(\delta(q_0, p(n)*\eta*\xi))\\&=\tau(\delta(q_0, p((m-b)p^h+r)))\\&=\lambda_M^{(p)}((m-b)p^h+r)\\&=\lambda_M^{(p)}(r)\,.\end{aligned}$$

Since q' is an arbitrary state and τ is one-to-one, this means that ξ is a reset sequence.

THEOREM 2. *Let $S\subset C^N$ be a minimal set associated with a substitution of length p^k, where p is a prime number and k is any positive integer. Assume that for some (or, equivalently, any) $\alpha\in S$, there exist non-negative integers h and r, such that $\alpha(ip^h+r)=\alpha(r)$ for $i=0, 1, 2, \cdots$. Then, S has a pure point spectrum. Moreover, if S is an infinite set, then the point spectrum of S is $\rho(p)=\{\omega\,;\,\omega^{p^i}=1$ for some $i\in N\}$.*

PROOF. When S is a finite set, our theorem is clear. Assume that S is an infinite set. From Lemma 5 and Lemma 7, there exists a finite-state machine $M=(K, \delta, q_0, \tau)$ over N_{p^k} (k is a positive integer which may differ from k in the statement of Theorem 2), such that

(i) δ is strongly connected and $\delta(q_0, 0)=q_0$

(ii) $\lambda_M^{(p^k)}\in S$

(iii) τ is one-to-one.

Let $\alpha=\lambda_M^{(p^k)}$ and $\alpha(ip^h+r)=\alpha(r)$ for $i=0, 1, 2, \cdots$. From Lemma 10, M has a reset sequence. Moreover, since S is an infinite set, α is not an ultimately periodic sequence. Therefore, from Lemma 9, for any non-negative integer n, there exists a minimal reset sequence ξ, such that $L(\xi)\geqq n+1$. Define $s\in N$, as follows:

$$\xi=0*0*\cdots*0*p^k(s)\,,$$

where if ξ consists only of 0's, then define $s=0$. We have $\alpha(ip^{kL(\xi)}+s)=\alpha(s)$ for any integer $i\geqq -\left[\frac{s}{p^{kL(\xi)}}\right]$. For any integer i, $\bar{i}$ denotes the residue class modulo $p^{kL(\xi)}$ which contains i. Let

$$E=\{\bar{m}\,;\ \alpha(ip^{kL(\xi)}+m)=\alpha(s)\ \text{for any integer}\ i,\ \text{such that}\ ip^{kL(\xi)}+m\geqq 0\}\,.$$

Since $\bar{s}\in E$, E is not empty. For any integer j, let $E+j=\{\overline{m+j}\,;\ \bar{m}\in E\}$. We prove that if $E+j=E$, then j must be a multiple of p^{kn}. Let $E+j=E$ and j' be the greatest common divisor of j and $p^{kL(\xi)}$. Then, j' must be either a multiple of p^{kn} or a divisor of p^{kn}. Assume the latter, then we have $E+ip^{kn}=E$ for any integer i. Therefore, $\alpha(ip^{kn}+s)=\alpha(s)$ for any integer $i\geqq-\left[\frac{s}{p^{kn}}\right]$. This means that the suffix of ξ of length $n(<L(\xi))$ is a reset sequence, contradicting the assumption that ξ is a minimal reset sequence. Thus, if $E+i=E+j$, then we have $i\equiv j\ (\mathrm{mod}\,p^{kn})$. From Lemma 10, there exists an integer L_n, such that for any non-negative integer i and $\bar{j}\notin E$, there exists an integer j', satisfying

(i) $j'\in\bar{j}$

(ii) $i\leqq j'\leqq i+L_n-1$

(iii) $\alpha(j')\neq\alpha(s)$.

Let $\eta\in C^*$ be any section of α of length L_n. Let

$$E_\eta=\{\bar{m}\,;\ \eta(ip^{kL(\xi)}+m)=\alpha(s)\ \text{for any integer}\ i,\ \text{such that}\ 0\leqq ip^{kL(\xi)}+m\leqq L_n-1\}\,.$$

Then, from the above discussion, there exists an integer j, such that $E=E_\eta+j$. Moreover, this j is uniquely determined up to modulo p^{kn}. Define $G_n(\eta)$, such that $0\leqq G_n(\eta)\leqq p^{kn}-1$ and $E=E_\eta+G_n(\eta)$. For $\beta\in\overline{\mathrm{Orb}}\,(\alpha)=S$, define $g_n(\beta)$, such that $g_n(\beta)=G_n(\eta)$, where η is the prefix of β of length L_n. Then, it is clear that $g_n(T\beta)\equiv g_n(\beta)+1\ (\mathrm{mod}\,p^{kn})$ for any $\beta\in S$. Let ω_n be any primitive p^{kn}-th root of 1. Let f_n be a complex valued function defined on S, such that

$$f_n(\beta)=\omega_n{}^{g_n(\beta)}\,.$$

Then, it is clear that $f_n\in L_2(S,\mu)$, where μ is the T-invariant probability measure on S, and that f_n is a proper function corresponding to a proper value ω_n of the strictly ergodic set S. Since n was any non-negative integer and the point spectrum of S is a multiplicative subgroup, this means that the point spectrum of S includes $\rho(p)$.

To complete the proof, we prove that $\{f_i^j\,;\ i,j\in N\}$ generates the Hilbert space $L_2(S,\mu)$. It is easily seen that $\{f_i^j\,;\ i,j\in N\}$ is multiplicatively closed. Let

$$\Delta_{n,m}=\{\beta\in S\,;\ g_n(\beta)=m\}\,,$$

where $n\in N$ and $0\leqq m\leqq p^{kn}-1$. Then, the characteristic function of $\Delta_{n,m}$

belongs to the linear subspace spanned by $\{f_i^j ; i, j \in N\}$, since it equals

$$\frac{1}{p^{kn}} \sum_{i=0}^{p^{kn}-1} \frac{f_n^i}{\omega_n^{mi}} .$$

Let

$$\Delta = \{\Delta_{n,m} ;\ n \in N,\ 0 \leqq m \leqq p^{kn}-1\} .$$

To complete the proof, it is sufficient to prove that for any cylinder set Γ_η that intersects with S, there exists $B \subset S$ belonging to the σ-field generated by Δ, such that $B \subset \Gamma_\eta$ and $\mu(\Gamma_\eta - B) = 0$. To prove this, it is sufficient to prove that for almost every (μ) $\beta \in \Gamma_\eta$, there exists $V \in \Delta$, such that $\beta \in V \subset \Gamma_\eta$, since Δ is a countable family. Let

$$I_n = \{i \in N;\ 0 \leqq i \leqq p^{kn} - L(\eta),\ p^k(i+j) \text{ is a reset sequence of } M \text{ for any } j \in N, \text{ such that } 0 \leqq j \leqq L(\eta)-1\}$$

$$c_n = \frac{\text{Card } I_n}{p^{kn}} .$$

Since M has a reset sequence and any sequence which has a reset sequence as its section is itself a reset sequence, the above c_n tends to 1 as $n \to \infty$. Let

$$R_n = \{\alpha(i) * \alpha(i+1) * \cdots * \alpha(i+L_n-1) ;\ i \equiv j \pmod{p^{kn}} \text{ for some } j \in I_n\}$$

$$R_n' = \{\alpha(i) * \alpha(i+1) * \cdots * \alpha(i+L_n-1) ;\ i \equiv j \pmod{p^{kn}} \text{ for some } j \in N, \text{ such that } 0 \leqq j \leqq p^{kn}-1 \text{ and } j \notin I_n\} .$$

Since R_n and R_n' are disjoint, we have

$$\mu(\bigcup_{\zeta \in R_n} \Gamma_\zeta) = c_n .$$

Let $g_n(\beta) \in I_n$ for some $n \in N$ and $\beta \in S$. For $j \in N$, such that $0 \leqq j \leqq L(\eta)-1$, we have $\beta(j) = \alpha(g_n(\beta)+j)$, since $\beta(j) = \alpha(ip^{kn} + g_n(\beta)+j)$ for some integer $i \geqq 0$ and $g_n(\beta)+j$ is a reset sequence of M. Let

$$W = \{\beta \in S;\ g_n(\beta) \in I_n \text{ for some } n \in N\} .$$

Since

$$\{\beta \in S;\ g_n(\beta) \in I_n\} = \bigcup_{\zeta \in R_n} \Gamma_\zeta \cap S ,$$

we have $\mu(W) = 1$. Let $\beta \in \Gamma_\eta \cap W$. Then, there exists $n \in N$, such that $g_n(\beta) \in I_n$. Let $g_n(\beta) = m$. For any $\gamma \in \Delta_{n,m}$, we have $\gamma(j) = \alpha(m+j) = \beta(j)$ for $j = 0, 1, \cdots, L(\eta)-1$. Since $\beta \in \Gamma_\eta$, we have $\gamma \in \Gamma_\eta$. Thus, $\Delta_{n,m} \subset \Gamma_\eta$. This completes the proof of Theorem 2.

COROLLARY 2. *Let $S \subset C^N$ be a minimal set associated with a substitution*

θ of length p^k, where p is a prime number and k is any positive integer. Assume that there exists an integer $0 \leqq i \leqq p^k-1$, such that $\theta(c)(i)$ is the same for any $c \in C$. Then, S has a rational pure point spectrum $\rho(p)$.

§ 5. Remark

Our results remain true in the case of two-sided sequences.

Osaka University

References

[1] K. Jacobs, Combinatorial construction in ergodic theory, Proc. international conference on functional analysis, Tokyo, 1969.
[2] F. Hahn and Y. Katznelson, On the entropy of uniquely ergodic transformations, Trans. Amer. Math. Soc., (2) **126** (1967), 335-360.
[3] W.H. Gottschalk, Substitution minimal sets, Trans. Amer. Math. Soc., **109** (1963), 467-491.
[4] A. Cobham, On the base-dependence of sets of numbers recognizable by finite automata, Math. Systems Theory, (2) 3 (1969), 186-192.
[5] S. Kakutani, Ergodic theory of shift transformations, Proc. 5-th Berkeley Symp., vol. 2, part 2 (1967), 405-413.
[6] P.R. Halmos, Lectures on ergodic theory, Publication Math. Soc. Japan, 1956.