ROOTS OF THE ONE-SIDED N-SHIFT

J. R. BLUM[1]
UNIVERSITY OF NEW MEXICO
H. D. BRUNK[2] and D. L. HANSON[2]
UNIVERSITY OF MISSOURI

1. Introduction and summary

In his booklet on ergodic theory [1] Halmos raises the question of the existence of p-th roots of measure-preserving transformations, and more specifically the question of the existence of p-th roots of the N-shifts (see problem 4 on page 97). On page 56 of the same book he indicates that if $N = k^2$, then the N-shift has a square root. Clearly, essentially the same argument shows that if $N = k^p$, then the N-shift has a p-th root.

The main purpose of this paper is to show that the one-sided N-shift has a p-th root if and only if $N = k^p$ for some positive integer k. The problem of the existence of roots seems to be more difficult for the bilateral N-shift than for the one-sided N-shift. At least our methods involve the many-to-one nature of the one-sided N-shift and its roots, and cannot be used on the bilateral shifts.

2. Notation

The following symbols will be used:

N is a positive integer;

$\Omega = \{\omega = (\omega_1, \omega_2, \cdots) | \omega_i \in \{0, 1, \cdots, N-1\} \text{ for all } i\}$;

Σ is the smallest σ-field containing all sets of the form $\{\omega | \omega_i = k\}$;

P is a probability measure on (Ω, Σ) defined so that the sequence $\{\omega_k\}$ of coordinate projection random variables is an independent sequence, and so that $P\{\omega | \omega_i = k\} = 1/N$ for $k = 0, 1, \cdots, N-1$ and all i;

T is the one-sided N-shift defined by $T(\omega_1, \omega_2, \cdots) = (\omega_2, \omega_3, \cdots)$;

Σ^0 is the subcollection of 2^Ω consisting of all subsets of sets (in Σ) of measure zero;

$\Sigma^* = \{E_1 + E_2 | E_1 \in \Sigma \text{ and } E_2 \in \Sigma^0\}$. This is a σ-field;

P^* is the completion of P to Σ^*;

$\omega + j/N = (\omega_1', \omega_2, \cdots)$ where $\omega = (\omega_1, \omega_2, \cdots)$, $0 \leq \omega_1' \leq N-1$, and $\omega_1' = \omega_1 + j \pmod{N}$.

[1] Research supported by NSF Grant GP-1816.
[2] Research supported by the Air Force Office of Scientific Research, Office of Aerospace Research, U. S. Air Force, Grant Nr AF-AFOSR-746-65.

3. Results

For our first two lemmas we state some relatively well-known facts about T.

LEMMA 1. *The one-sided N-shift T satisfies the following relations:*

(i) $A \in \Sigma(\Sigma^*) \Rightarrow TA \in \Sigma(\Sigma^*)$ *and* $T^{-1}A \in \Sigma(\Sigma^*)$;

(ii) T *is onto;*

(iii) T *is measure preserving (that is,* $A \in \Sigma^*$ *implies* $P^*(A) = P^*(T^{-1}A)$*);*

(iv) $P^*(A) = 0$ *implies* $P^*(TA) = 0$ *and* $P^*(A) = 1$ *implies* $P^*(TA) = 1$;

(v) T *is ergodic (that is,* $A \in \Sigma^*$ *and* $A = T^{-1}A$ *implies* $P^*(A) = 0$ *or* $P^*(A) = 1$).

LEMMA 2. *If* $A \in \Sigma^*$, $E \in \Sigma^*$, $P^*(E) = 1$, *and* $E \cap T^{-1}A \subset A$, *then* $P^*(A) = 0$ *or* $P^*(A) = 1$.

PROOF. Set $A_\infty = \bigcup_{n=0}^{\infty} \bigcap_{k=n}^{\infty} T^{-k}A$. One shows that $P^*(T^{-k}A \,\Delta\, A) = 0$ for all k, from which it follows that $P^*(A_\infty \,\Delta\, A) = 0$ or $P^*(A) = P^*(A_\infty)$. Note that A_∞ is invariant (namely, $T^{-1}A_\infty = A_\infty$) so that $P^*(A_\infty) = 0$ or $P^*(A_\infty) = 1$.

Suppose U and V are point transformations from Ω into Ω which are Σ-measurable (that is, $U^{-1}\Sigma \subset \Sigma$ and $V^{-1}\Sigma \subset \Sigma$), or Σ^*-measurable ($U^{-1}\Sigma^* \subset \Sigma^*$ and $V^{-1}\Sigma^* \subset \Sigma^*$), and which are nonsingular (namely, $A \in \Sigma^*$ and $P^*(A) = 0$ implies $P^*(U^{-1}A) = 0$ and $P^*(V^{-1}A) = 0$).

LEMMA 3. *If U and V are Σ-measurable, then they are also Σ*-measurable.*

PROOF. If $E \in \Sigma^*$, then we can assume that $E = E_1 + E_2$ with $E_1 \in \Sigma$ and $E_2 \subset E^0$ where $E^0 \in \Sigma$, $P(E^0) = 0$. Now $E_2 \subset E^0 - E_1$ and $P(E^0 - E_1) = 0$. It follows that $U^{-1}(E) = U^{-1}(E_1) + U^{-1}(E_2)$ with $U^{-1}(E_1) \in \Sigma$, $U^{-1}(E^0 - E_1) \in \Sigma$, $P[U^{-1}(E^0 - E_1)] = 0$, and $U^{-1}(E_2) \subset U^{-1}(E^0 - E_1)$. Thus $U^{-1}E \in \Sigma^*$ and similarly, $V^{-1}E \in \Sigma^*$.

Now let $D_0 = \{\omega | UV(\omega) = VU(\omega) = T(\omega)\}$ and note that D_0 is in Σ^*. Define

$$D = D_0 \cap U^{-1}D_0 \cap V^{-1}D_0. \tag{1}$$

We assume that $P^*(D_0) = 1$. It follows from the nonsingularity of U and V that $P^*(D) = 1$ also.

LEMMA 4. *If* $\omega \in D$, *then* $TU(\omega) = UT(\omega)$ *and* $TV(\omega) = VT(\omega)$.

LEMMA 5. *If* $P^*(E) = 1$, *then* $UE \in \Sigma^*$, $VE \in \Sigma^*$, *and* $P^*(UE) = P^*(VE) = 1$.

PROOF. First $UE \supset UV(D \cap V^{-1}E) = T(D \cap V^{-1}E)$. However,

$$P^*[T(D \cap V^{-1}E)] = P^*(D \cap V^{-1}E) = 1, \tag{2}$$

so UE has inner P^* measure 1. Thus $UE \in \Sigma^*$ and $P^*(UE) = 1$. The remaining conclusions follow by interchanging U and V in the above argument.

LEMMA 6. *The transformations U and V are measure preserving.*

PROOF. We will show that U is measure preserving. The proof that V is measure preserving is identical and omitted.

For $A \in \Sigma^*$ define $\mu(A) = P^*(U^{-1}A)$. We see that μ is a probability measure which is absolutely continuous with respect to P^*, since U is nonsingular. Note that lemma 4 implies $D \cap U^{-1}T^{-1}A = D \cap T^{-1}U^{-1}A$. Thus

$$(3)\qquad \mu(A) = P^*(U^{-1}A) = P^*(T^{-1}U^{-1}A) = P^*(D \cap T^{-1}U^{-1}A) = P^*(D \cap U^{-1}T^{-1}A) = P^*(U^{-1}T^{-1}A) = \mu(T^{-1}A)$$

so that T is measure preserving with respect to μ.

The remainder of the proof is similar to that of theorem 1 and corollary 1 of [2].

Let A be a maximal positive set for the signed measure $P^* - \mu$ as guaranteed by the Hahn decomposition theorem. The set

$$(4)\qquad A_\infty = \bigcup_{n=0}^{\infty} \bigcap_{k=n}^{\infty} T^{-k}A$$

can be shown to be a maximal positive set for $P^* - \mu$. But A_∞ is invariant, hence $P^*(A_\infty) = 0$ or 1. But since μ is absolutely continuous with respect to P^*, we have $P^*(A_\infty) = 0$ implies $\mu(A_\infty) = 0$, and $P^*(A_\infty) = 1$ implies $P^*(A_\infty^c) = 0$ implies $\mu(A_\infty^c) = 0$ implies $\mu(A_\infty) = 1$. In either case $(P^* - \mu)A_\infty = 0$. Similarly $P^* - \mu$ can be shown to be zero on a maximal negative set so $P^* \equiv \mu$. Thus $P^*(U^{-1}A) = P^*(A)$ for $A \in \Sigma^*$.

Lemma 7. *If $E \in \Sigma^*$, then $P^*(T^{-1}E) = P^*(U^{-1}V^{-1}E) = P^*(V^{-1}U^{-1}E)$.*

Proof. The lemma follows from the observations that $D \cap U^{-1}V^{-1}E = D \cap V^{-1}U^{-1}E = D \cap T^{-1}E$ and that $P^*(D) = 1$.

Theorem 1. *If U and V are measurable (Σ or Σ^*) point transformations from Ω into Ω which are nonsingular, and such that $P^*\{\omega | UV(\omega) = VU(\omega) = T(\omega)\} = 1$, then there exist positive integers n and m such that*

(i) $mn = N$,

(ii) $P^*\left\{\omega \,\middle|\, \begin{array}{l}\text{exactly } m \text{ out of the collection}\\ U(\omega),\ U(\omega + 1/n),\ \cdots,\ U(\omega + (N-1)/N) \text{ equal } U(\omega)\end{array}\right\} = 1,$

(iii) $P^*\left\{\omega \,\middle|\, \begin{array}{l}\text{exactly } n \text{ out of the collection}\\ V(\omega),\ V(\omega + 1/N),\ \cdots,\ V(\omega + (N-1)/N) \text{ equal } V(\omega)\end{array}\right\} = 1.$

Proof. Let

$$(5)\qquad A_k = \left\{\omega \,\middle|\, \begin{array}{l}\text{exactly } k \text{ members of the collection}\\ U(\omega),\ U\left(\omega + \frac{1}{N}\right),\ \cdots,\ U\left(\omega + \frac{N-1}{N}\right) \text{ are equal to } U(\omega)\end{array}\right\},$$

$$(6)\qquad B_k = \left\{\omega \,\middle|\, \begin{array}{l}\text{exactly } k \text{ members of the collection}\\ V(\omega),\ V\left(\omega + \frac{1}{N}\right),\ \cdots,\ V\left(\omega + \frac{N-1}{N}\right) \text{ are equal to } V(\omega)\end{array}\right\}.$$

Note that $\sum_{k=1}^{n} A_k = \sum_{k=1}^{n} B_k = \Omega$ and that the A_k's and B_k's are measurable sets. Let m be the smallest integer such that $P^*(A_m) > 0$, and let n be the largest integer such that $P^*(B_n) > 0$.

Let

$$(7)\qquad G_1 = \left\{ \omega \,\middle|\, \begin{array}{l} \omega, \omega + \frac{1}{N}, \cdots, \omega + \frac{N-1}{N} \in D \cap [A_m \cup A_{m+1} \cup \cdots \cup A_n] \\ U(\omega) \in B_n \\ U(\omega), U(\omega) + \frac{1}{N}, \cdots, U(\omega) + \frac{N-1}{N} \in UD \end{array} \right\},$$

and note that $G_1 \subset U^{-1}B_n$ and $P^*[U^{-1}B_n - G_1] = 0$ so that $P^*(G_1) > 0$ and $G_1 \neq \phi$. Suppose $\omega \in G_1$. Exactly n members of the set

$$(8)\qquad \left\{ U(\omega), U(\omega) + \frac{1}{N}, \cdots, U(\omega) + \frac{N-1}{N} \right\}$$

are such that $V[U(\omega) + (\alpha/N)] = V[U(\omega)]$. Suppose these are $u_1, \cdots, u_n$. Now $U^{-1}(u_i) \cap D \neq \phi$ for each u_i, say $x_i \in U^{-1}(u_i) \cap D$. Since

$$(9)\qquad T^{-1}[T(\omega)] = \{y | T(y) = T(\omega)\} = \left\{ \omega, \omega + \frac{1}{N}, \cdots, \omega + \frac{N-1}{N} \right\},$$

we see that $x_i \in A_m \cup \cdots \cup A_n$ so that there are at least m points in the set $\{\omega, \omega + (1/N), \cdots, \omega + (N - 1/N)\}$ which have the same image under U as x_i does, namely u_i.

Thus $T\omega$ has n preimages under V (namely $u_1, \cdots, u_n$) such that each one of these has at least m preimages under U which are in D. We see that $T\omega$ has at least nm preimages under $VU = T$ which are in D, hence $nm \leq N$.

Let

$$(10)\qquad G_2 = \left\{ \omega \,\middle|\, \begin{array}{l} V(\omega), V\left(\omega + \frac{1}{N}\right), \cdots, V\left(\omega + \frac{N-1}{N}\right) \in D \\ \omega, \omega + \frac{1}{N}, \cdots, \omega + \frac{N-1}{N} \in D \cap \{B_1 \cup \cdots \cup B_n\} \\ V(\omega) \in A_m \\ V(\omega), V(\omega) + \frac{1}{N}, \cdots, V(\omega) + \frac{N-1}{N} \in D \cap VD \end{array} \right\}.$$

Note that $G_2 \subset V^{-1}A_m$ and $P^*[V^{-1}A_m - G_2] = 0$ so that $P^*(G_2) > 0$ and $G_2 \neq \phi$. Suppose $\omega \in G_2$. Exactly m members of the set

$$(11)\qquad \left\{ V(\omega), V(\omega) + \frac{1}{N}, \cdots, V(\omega) + \frac{N-1}{N} \right\}$$

are such that $U[V(\omega) + k/N] = U[V(\omega)]$. Suppose these are $v_1, \cdots, v_m$. Now $V^{-1}(v_k) \cap D \neq \phi$, say $y_k \in V^{-1}(v_k) \cap D$. We have

$$(12)\qquad T^{-1}(T\omega) = \left\{ \omega, \omega + \frac{1}{N}, \cdots, \omega + \frac{N-1}{N} \right\},$$

and since $y_k \in D \cap V^{-1}V(\omega)$, we see that $y_k \in T^{-1}(T\omega)$. However,

$$\omega, \omega + \frac{1}{N}, \cdots, \omega + \frac{N-1}{N} \in B_1 \cup \cdots \cup B_n, \tag{13}$$

so $y_k \in B_1 \cup \cdots \cup B_n$.

Thus there are no more than n preimages of each v_k which are in

$$\left\{\omega, \omega + \frac{1}{N}, \cdots, \omega + \frac{N-1}{N}\right\}. \tag{14}$$

It follows that $T\omega$ has m preimages under U (namely $v_1, \cdots, v_m$) such that each of these has at most n preimages under V which are in D, so that we have at most nm of these preimages. These are all preimages under T, and if they are all such preimages, then $N \leq nm$. We are done if $V(\omega + k/N) \in \{v_1, \cdots, v_m\}$ for each k. If this is not the case, then either

$$V\left(\omega + \frac{k}{N}\right) \in \left\{V(\omega), V(\omega) + \frac{1}{N}, \cdots, V(\omega) + \frac{N-1}{N}\right\} - \{v_1, \cdots, v_m\} \tag{15}$$

(which contradicts $T(\omega + k/N) = T(\omega)$), or else

$$V\left(\omega + \frac{k}{N}\right) \notin \left\{V(\omega), V(\omega) + \frac{1}{N}, \cdots, V(\omega) + \frac{N-1}{N}\right\}. \tag{16}$$

But since $V(\omega)$ and $V(\omega + k/N) \in D$, we have

$$\begin{aligned} T(V(\omega)) = VU(V(\omega)) = V[T(\omega)] &= V\left[T\left(\omega + \frac{k}{N}\right)\right] \\ &= V\left[UV\left(\omega + \frac{k}{N}\right)\right] = T\left[V\left(\omega + \frac{k}{N}\right)\right]. \end{aligned} \tag{17}$$

Thus both $V(\omega)$ and $V(\omega + k/N)$ are in D, and preimages of $T(V(\omega))$ under T, hence $V(\omega + k/N) = V(\omega) + j/N$ for some j. We have already seen that these circumstances imply $V(\omega + k/N) \in \{v_1, \cdots, v_m\}$.

Now that we have shown that $mn = N$, let us look again at the points in G_1. We saw that if $\omega \in G_1$, then $T\omega$ has n preimages under V, and that each of these had at least m-preimages under U which are in D. Since $mn = N$ and $T\omega$ has the N preimages $\omega, \omega + 1/N, \cdots, \omega + (N-1)/N$ (in D) under $UV = T$, it follows that each preimage under V of $T\omega$ has *exactly* m preimages (in D) under U. In particular, $U(\omega)$ is a preimage under V of $T\omega$, and therefore has exactly m preimages (in D and thus in $\omega, \omega + 1/N, \cdots, \omega + (N-1)/N$) under U, hence $\omega \in A_m$. Thus $G_1 \subset A_m$.

Similarly, looking at G_2 we argue that if $\omega \in G_2$, then $V(\omega)$ has exactly n preimages (in $\omega, \omega + 1/N, \cdots, \omega + (N-1)/N$) under V, and hence $\omega \in B_n$. Thus $G_2 \subset B_n$.

We have shown that

$$B_n \supset G_2 \overset{\text{a.e.}}{=} V^{-1}A_m \supset V^{-1}G_1 \overset{\text{a.e.}}{=} V^{-1}U^{-1}B_n \tag{18}$$

and

$$A_m \supset G_1 \overset{\text{a.e.}}{=} U^{-1}B_n \supset U^{-1}G_2 \overset{\text{a.e.}}{=} U^{-1}V^{-1}A_m. \tag{19}$$

An application of lemma 7 shows that $B_n \overset{\text{a.e.}}{=} T^{-1}B_n$ and $A_m \overset{\text{a.e.}}{=} T^{-1}A_m$. An application of lemma 2 shows that $P^*(A_m) = P^*(B_n) = 1$ and completes the proof of the theorem.

THEOREM 2. *The one-sided N-shift has a nonsingular and measurable p-th root S (in the sense that* $P^*\{\omega|T(\omega) = S^p(\omega)\} = 1$*) if and only if* $N = k^p$ *for some positive integer k.*

PROOF. Suppose $N = k^p$ and let $X = \{1, \cdots, k\}$. The following is hinted at on page 56 of [1]. Define

$$\Omega_X = \{x = ({}_1x, \cdots, {}_px)|{}_ix \in X \quad \text{for} \quad i = 1, \cdots, p\}. \tag{20}$$

Let ψ be any one of the $N!$ distinct mappings of $\{0, \cdots, N-1\}$ onto Ω_X. Define $x_\alpha = ({}_1x_\alpha, \cdots, {}_px_\alpha)$ for $\alpha \in \{0, \cdots, N-1\}$ by $x_\alpha = \psi(\alpha)$. Now suppose $\omega = (\omega_1, \omega_2, \cdots) \in \Omega$ and that $x_{\omega_i} = ({}_1x_{\omega_i}, {}_2x_{\omega_i}, \cdots, {}_px_{\omega_i})$.

Define

$$S\omega = [\psi^{-1}({}_2x_{\omega_1}, \cdots, {}_px_{\omega_1}, {}_1x_{\omega_2}), \psi^{-1}({}_2x_{\omega_2}, \cdots, {}_px_{\omega_2}, {}_1x_{\omega_3}), \cdots]. \tag{21}$$

In order to obtain $S\omega$, one encodes each digit ω_i of ω using ψ to find the corresponding p-tuple $x_{\omega_i} = \psi(\omega_i)$. Then one eliminates the first digit in the coded version of ω_1, namely, ${}_1x_{\omega_1}$, and one regroups into p-tuples. This amounts to a p-shift of the encoded version of ω. Finally one decodes each digit: S is Σ and Σ^* measurable, measure preserving, and is a p-th root of T everywhere (namely, $S^p\omega = T\omega$ for all ω).

Now suppose $P^*\{\omega|S^p(\omega) = T(\omega) = 1\}$ and that S is measurable and nonsingular. Let $U = S^{p-1}$ and $V = S$. From theorem 1 there exists some positive integer k such that

$$P^*\left\{\omega \left| \begin{matrix} \text{exactly } k \text{ out of the collection} \\ S(\omega), S\left(\omega + \frac{1}{N}\right), \cdots, S\left(\omega + \frac{N-1}{N}\right) \text{are equal to } S(\omega) \end{matrix} \right.\right\} = 1. \tag{22}$$

It is almost obvious that S^p is k^p-to-one almost everywhere. (A rigorous proof of this fact involves a little effort with sets of measure zero but will be omitted because the difficulties are of the type encountered in theorem 1.) Since T is N-to-one everywhere it follows that $N = k^p$.

4. Some remarks on generalizations

It is clear that the results given here are valid, not only for the one-sided N-shift, but for other ergodic transformations which are essentially N-to-1 as well. The essentials seem to be that there exists a transformation ψ such that on a set of measure one, $\omega, \psi(\omega), \cdots, \psi^{N-1}(\omega)$ are all different and $\omega = \psi^N(\omega)$; that ψ be measurable and nonsingular; and that $T(\omega) = T(\omega')$ if and only if $\omega' = \psi^k(\omega)$ for some k (provided we have restricted ω and ω' to some set of measure 1). We have used the fact that the one-sided N-shift is bimeasurable. It would be interesting to know whether it is necessary that T have this property.

It would also be interesting to know about roots of T in the case where ψ is of finite period for almost all ω but the period is a function of ω.

REFERENCES

[1] P. R. HALMOS, *Lectures on Ergodic Theory*, New York, Chelsea, 1956.

[2] J. R. BLUM and D. L. HANSON, "On invariant probability measures I," *Pacific J. Math.*, Vol. 10 (1960), pp. 1125–1129.