2. R. M. Smullyan, *Theory of formal systems*, Annals of Mathematics Studies No. 47, Princeton Univ. Press, Princeton, N. J., 1961.

3. S. C. Kleene, *Introduction to metamathematics*, Van Nostrand, New York, 1952.

4. J. C. E. Dekker, *A theorem of hypersimple sets*, Proc. Amer. Math. Soc. 5 (1954), 791–796.

YESHIVA UNIVERSITY

ENTROPY FOR NONINVERTIBLE TRANSFORMATIONS

JOHN D. FERGUSON[1]

1. **Introduction.** In 1959, Sinai (see [1]) gave an improved version of the definition of entropy for a measure-preserving transformation on a probability space. Included in the same paper was a theorem which made possible the computation of the entropy of certain invertible measure-preserving transformations. In this paper we prove a theorem, similar to that of Sinai, for measure-preserving transformations which are not necessarily invertible.

2. **Preliminaries.** Let $(X, \mathbf{S}, \mu)$ be a probability space, and T a measure-preserving transformation on X. If $\mathbf{A}$ and $\mathbf{C}$ are subfields of $\mathbf{S}$ with $\mathbf{A}$ finite, then the "entropy" and "conditional entropy" of $\mathbf{A}$, denoted $\overline{H}(\mathbf{A})$ and $\overline{H}(\mathbf{A}/\mathbf{C})$, respectively, are defined in Halmos [2]. Using these concepts, the entropy of T is defined as follows. Let $\mathbf{A}$ be a finite subfield of $\mathbf{S}$, then $\bigvee_{j=0}^{m} T^{-j}\mathbf{A}$ is a finite subfield of $\mathbf{S}$, and it follows from a theorem in information theory that

$$h(T, \mathbf{A}) = \lim_{m \to \infty} (1/(m+1))\overline{H}\left(\bigvee_{j=0}^{m} T^{-j}\mathbf{A}\right)$$

exists. Then the entropy of T is $h^*(T)$, where

$$h^*(T) = \sup\{h(T, \mathbf{A}) \mid \mathbf{A} \text{ a finite subfield of } \mathbf{S}\}.$$

Sinai's essential idea was to avoid taking the supremum by exhibiting a finite subfield $\mathbf{A}$ of $\mathbf{S}$ for which $h(T, \mathbf{A})$ gave the supremum, but his proof depended on the invertibility of T. The theorem proved below replaces the supremum over all finite subfields $\mathbf{A}$ by a supre-

Received by the editors February 2, 1963 and, in revised form, August 1, 1963.

[1] Some of the contents of this paper were included in the author's doctoral dissertation, under the direction of Professor G. A. Hedlund, at Yale University, where the author held a National Science Foundation Graduate Fellowship.

mum over a countable collection of subfields, and allows noninvertible T. We require the following results, which may be found in Halmos [2].

Let $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$, $\boldsymbol{D}$ be subfields of $\boldsymbol{S}$ with $\boldsymbol{A}$ and $\boldsymbol{B}$ finite, then

(1) $\overline{H}(\boldsymbol{A}) = -\sum_A \mu(A) \log \mu(A)$, where the summation is over all the atoms A of $\boldsymbol{A}$.

(2) $\overline{H}(\boldsymbol{A} \vee \boldsymbol{B}) = \overline{H}(\boldsymbol{B}) + \overline{H}(\boldsymbol{A}/\boldsymbol{B})$.

(3) If $\boldsymbol{A} \subseteq \boldsymbol{B}$, then $\overline{H}(\boldsymbol{A}) \leqq \overline{H}(\boldsymbol{B})$.

(4) If $\boldsymbol{A} \subseteq \boldsymbol{C}$, then $\overline{H}(\boldsymbol{A}/\boldsymbol{C}) = 0$.

(5) $\overline{H}(T^{-1}\boldsymbol{A}/T^{-1}\boldsymbol{C}) = \overline{H}(\boldsymbol{A}/\boldsymbol{C})$.

(6) $\overline{H}(\boldsymbol{A} \vee \boldsymbol{B}/\boldsymbol{C}) \leqq \overline{H}(\boldsymbol{A}/\boldsymbol{C}) + \overline{H}(\boldsymbol{B}/\boldsymbol{C})$.

(7) If $\boldsymbol{C} \subseteq \boldsymbol{D}$, then $\overline{H}(\boldsymbol{A}/\boldsymbol{D}) \leqq \overline{H}(\boldsymbol{A}/\boldsymbol{C})$.

(8) If $\boldsymbol{C}_1 \subseteq \boldsymbol{C}_2 \subseteq \cdots$ are subfields of $\boldsymbol{S}$ then

$$\lim_{n \to \infty} \overline{H}(\boldsymbol{A}/\boldsymbol{C}_n) = \overline{H}\left(\boldsymbol{A} \Big/ \bigvee_{n=1}^{\infty} \boldsymbol{C}_n\right).$$

3. Computing entropy.

THEOREM. *Let T be a measure-preserving transformation on X. Suppose there exists a sequence $\{\boldsymbol{A}_n\}$, $n = 1, 2, \cdots$, of finite subfields of $\boldsymbol{S}$, such that, if $\boldsymbol{B}_n$ denotes $\bigvee_{j=0}^{\infty} T^{-j}\boldsymbol{A}_n$, then*

(a) $\boldsymbol{B}_1 \subseteq \boldsymbol{B}_2 \subseteq \cdots$, *and*

(b) $\boldsymbol{S} = \bigvee_{n=1}^{\infty} \boldsymbol{B}_n$.

Then $h^*(T) = \limsup h(T, \boldsymbol{A}_n)$.

PROOF. Let $\boldsymbol{B}$ be a finite subfield of $\boldsymbol{S}$. Then, for $m, k \geqq 0$, and $n \geqq 1$, it follows that

$$\overline{H}\left(\bigvee_{i=0}^{k} T^{-i}\boldsymbol{B}\right) \leqq \overline{H}\left(\bigvee_{i=0}^{k} T^{-i}\boldsymbol{B} \vee \bigvee_{j=0}^{m+k} T^{-j}\boldsymbol{A}\right)$$

$$= \overline{H}\left(\bigvee_{j=0}^{m+k} T^{-j}\boldsymbol{A}_n\right) + \overline{H}\left(\bigvee_{i=0}^{k} T^{-i}\boldsymbol{B} \Big/ \bigvee_{j=0}^{m+k} T^{-j}\boldsymbol{A}_n\right),$$

by (3) and (2). Now the second term in the sum above is dominated by

$$\sum_{i=0}^{k} \overline{H}\left(T^{-i}\boldsymbol{B} \Big/ \bigvee_{j=0}^{m+k} T^{-j}\boldsymbol{A}_n\right),$$

according to (6), and this is less than or equal to

$$\sum_{i=0}^{k} \overline{H}\left(T^{-i}\boldsymbol{B} \Big/ \bigvee_{j=i}^{m+i} T^{-j}\boldsymbol{A}_n\right),$$

according to (7). Now for any pair of subfields $\boldsymbol{A}$ and $\boldsymbol{B}$ of $\boldsymbol{S}$, $T^{-1}(\boldsymbol{A}\vee\boldsymbol{B}) = T^{-1}\boldsymbol{A}\vee T^{-1}\boldsymbol{B}$, therefore

$$\bigvee_{j=i}^{m+i} T^{-j}\boldsymbol{A}_n = T^{-i}\left(\bigvee_{j=0}^{m} T^{-j}\boldsymbol{A}_n\right).$$

Thus,

$$\begin{aligned}\overline{H}\left(\bigvee_{i=0}^{k} T^{-i}\boldsymbol{B} \Big/ \bigvee_{j=0}^{m+k} T^{-j}\boldsymbol{A}_n\right) &\leqq \sum_{i=0}^{k} \overline{H}\left(T^{-i}\boldsymbol{B} \Big/ T^{-i}\bigvee_{j=0}^{m} T^{-j}\boldsymbol{A}_n\right)\\ &= \sum_{i=0}^{k} \overline{H}\left(\boldsymbol{B} \Big/ \bigvee_{j=0}^{m} T^{-j}\boldsymbol{A}_n\right)\\ &= (k+1)\overline{H}\left(\boldsymbol{B} \Big/ \bigvee_{j=0}^{m} T^{-j}\boldsymbol{A}_n\right),\end{aligned}$$

by (5). Hence

$$\begin{aligned}\frac{1}{k+1}\,\overline{H}\left(\bigvee_{i=0}^{k} T^{-i}\boldsymbol{B}\right) \leqq \frac{m+k}{1+k}\cdot\frac{1}{m+k}\cdot\overline{H}\left(\bigvee_{j=0}^{m+k} T^{-j}\boldsymbol{A}_n\right)\\ + \overline{H}\left(\boldsymbol{B} \Big/ \bigvee_{j=0}^{m} T^{-j}\boldsymbol{A}_n\right).\end{aligned}$$

Hence, letting $k\to\infty$,

$$h(T, \boldsymbol{B}) \leqq h(T, \boldsymbol{A}_n) + \overline{H}\left(\boldsymbol{B} \Big/ \bigvee_{j=0}^{m} T^{-j}\boldsymbol{A}_n\right),$$

and, letting $m\to\infty$,

$$h(T, \boldsymbol{B}) \leqq h(T, \boldsymbol{A}_n) + \overline{H}(\boldsymbol{B}/\boldsymbol{B}_n), \text{ by (8).}$$

Finally, letting $n\to\infty$,

$$\begin{aligned}h(T, \boldsymbol{B}) &\leqq \limsup h(T, \boldsymbol{A}_n) + \overline{H}\left(\boldsymbol{B} \Big/ \bigvee_{k=1}^{\infty} \boldsymbol{B}_k\right)\\ &= \limsup h(T, \boldsymbol{A}_n), \text{ by (8) and (4).}\end{aligned}$$

It now follows that $h^*(T) = \sup h(T, \boldsymbol{A}_n) = \limsup h(T, \boldsymbol{A}_n)$. This completes the proof of the theorem.

4. An example. Let S denote the set of all infinite sequences of zeros and ones, with uniform product measure (see [3, p. 5]), and let n be an integer greater than one. If $f(x_1, x_2, \cdots, x_n)$ is a polynomial over GF2, then f induces a mapping, f_∞, of S into S, defined as follows: if $y = \{y_m\}$, $m = 0, \pm 1, \pm 2, \cdots$, then $f_\infty(y) = z$ where $z = \{z_m\}$, and

$z_m = f(y_m, y_{m+1}, \cdots, y_{m+n-1})$, $m = 0, \pm 1, \pm 2, \cdots$. Concerning f_∞, the following statements are valid:

(a) f_∞ is a measurable transformation of S into S.

(b) f_∞ is measure-preserving iff f_∞ is onto.

(c) If $f(x_1, x_2, \cdots, x_n) = x_1 + g(x_2, \cdots, x_{n-1}) + x_n$, where g is a polynomial over GF2, then:

(i) f_∞ is precisely 2^{n-1} to 1, and onto;

(ii) f_∞ is ergodic and strongly mixing;

(iii) the entropy of f_∞ is $(n-1)$ log 2.

The proof of (c) (iii) may be accomplished by using the theorem proved above (see [4]); however, since f_∞ is not invertible, Sinai's theorem cannot be used.

References

1. Y. Sinai, *On the concept of entropy for a dynamical system*, Dokl. Akad. Nauk SSSR 124 (1959), 768–771.

2. P. R. Halmos, *Entropy in ergodic theory*, Lecture Notes, University of Chicago, Chicago, Illinois, 1959.

3. ———, *Lectures on ergodic theory*, Chelsea, New York, 1956.

4. J. D. Ferguson, *Some properties of mappings on sequence spaces*, Dissertation, Yale University, New Haven, Connecticut, 1962.

Institute for Defense Analyses