ISRAEL JOURNAL OF MATHEMATICS, Vol. 53, No. 1, 1986

CONSTRAINTS ON THE DEGREE OF A SOFIC HOMOMORPHISM AND THE INDUCED MULTIPLICATION OF MEASURES ON UNSTABLE SETS

BY

MIKE BOYLE

Mathematical Sciences Department,

IBM T. J. Watson Research Center, Yorktown Heights, New York, USA

ABSTRACT

Let f be an endomorphism of an irreducible sofic system S, where S has entropy $\log \lambda$. The *degree* of f is the number d such that f is d to 1 almost everywhere. Then d divides a power of the greatest common divisor of the nonleading coefficients of the minimal polynomial of λ. Also, f multiplies the natural measure on unstable sets of generic points by a positive unit of the ring generated by $1/\lambda$ and the algebraic integers of $Q[\lambda]$. Related results hold for bounded to one homomorphisms of sofic systems.

§0. Introduction

Suppose S is an irreducible sofic shift (in particular, S may be of finite type), and f is a factor map from S onto a subshift T of equal entropy. It is well known that there is a number d such that f is d to 1 almost everywhere (every bilaterally transitive point of T has exactly d preimages under f); endorsing the terminology of [16], we call this number the *degree* of f. An old theorem of L. R. Welch (14.9 of [12]) shows that if f is an endomorphism of the full shift on n symbols, then the degree of f divides a power of n. Generalizing, we find that for any irreducible sofic shift, the entropy of the shift provides severe and computable constraints on the possible degrees of endomorphisms; other factor maps also have constrained degrees.

Let S be irreducible sofic with entropy $\log \lambda$. Let $U(\lambda)$ be the set of positive integers which divide some power of the greatest common divisor of the nonleading coefficients of the minimal polynomial of λ. Then, given another sofic shift T of equal entropy, there is a finite set E of positive integers such that the

Received November 1, 1984 and in revised form June 3, 1985

degree d of any factor map from S onto T factors as $d = eu$, where $e \in E$ and $u \in U(\lambda)$. In particular, if f is an endomorphism, then $d \in U(\lambda)$. In the category of finite type (or even almost of finite type) subshifts, the set E may be chosen for S independent of T.

The proofs of these results involve two steps. Certain closed open sets are shown by way of magic words to have preimages under f which split into d pieces of equal measure (with respect to the measure of maximal entropy). This splitting then forces $1/d$ to lie in a $\mathbf{Z}[1/\lambda]$-module naturally associated with the ranges of the maximal measures on closed open sets, and thereby provides algebraic constraints.

Similar arguments show an endomorphism f of S multiplies a natural σ-finite measure on the unstable set of a typical point by a constant $R(f)$ depending only on f. This refines a result of Cuntz and Krieger. Similarly one obtains $L(f)$ via stable sets. The maps $f \mapsto L(f)$ and $f \mapsto T(f)$ are homomorphisms from the endomorphism semigroup of S into the positive units of the ring generated by $1/\lambda$ and the algebraic integers of $Q[\lambda]$. The algebraic constaint on the range follows from showing $L(f)R(f)\deg(f) = 1$.

Welch's proof involved certain integers which counted maximal numbers of right/left compatible extensions for a block code defining an endomorphism f of a full shift (see section 14 of [12]). These integers depended not only on f but also on the particular block code used to define f. Milnor [16] pointed out that the numbers could be normalized to depend only on f, and in proving a result from [4] related the normalized numbers to the multiplication of induced measures on stable/unstable sets by an automorphism of the shift. This connection of Welch's numbers to measures suggested to me the basic idea of this paper, using extremal arguments with a measure to constrain degrees.

I especially thank Wolfgang Krieger and Brian Marcus for helpful discussions.

§1. Background, notation and Markov magic words

I will assume a little familiarity with subshifts of finite type and symbolic dynamics. Basic definitions and facts adequate for this paper are listed in [3], section 1. For a thorough introduction, consult [1], section 3; [9], chapters 7, 17 and 25; [6]; [13]; and [18]. A *sofic* shift is a subshift which is a factor of a subshift of finite type. Sofic references are included in the bibliography.

I will use the same symbol for the domain of a subshift and the shift map on that domain. For a sofic shift T, several conditions ar equivalent ([7] and [11]): some point has a dense forward orbit; the periodic points are dense and T has a dense orbit: there exists a unique measure of maximal entropy which is nonzero on nonempty open sets; for any T-words U and W, there is some word V such that UVW is a T-word; T is a factor of an irreducible subshift of finite type; T is a factor of an irreducible subshift of finite type by a one-block bounded-to-one map which is one to one almost everywhere. Such shifts I will call *irreducible sofic* shifts.

If UVW is an allowed word for a subshift S, where U, V and W have lengths u, v and w, let

$$UV^iW = \{x \in S : x_{-u+i} \cdots x_{v+w-1+i} = UVW\}, \text{ e.g. } V^0 = \{x \in S : x_0 \cdots x_{v-1} = V\}.$$

We will be concerned only with subshifts S with a unique measure of maximal entropy, denoted μ_S. If S is a subshift of finite type on symbols $\{1, \ldots, n\}$ defined by an irreducible zero-one matrix A, let λ be the spectral radius of A. The entropy $h(S)$ of S is $\log \lambda$. The number λ is a simple root of the characteristic polynomial, in particular λ is an algebraic integer. Choose positive left and right eigenvectors l and r for λ, and let η be their inner product. Then μ_S is defined by requiring

$$\mu_S(W^0) = (\lambda^{-k} l(i) r(j))/\eta \tag{1.1}$$

for any S-word W of length $k+1$ with initial symbol i and terminal symbol j. Notice that by multiplying l and r by a suitable number, we may require the entires of l and r (and therefore η) to lie in $\mathbf{Z}[\lambda]$.

Any factor map which maps an irreducible sofic shift S onto an irreducible sofic shift T of equal entropy takes μ_S to μ_T. For such a map there exists an integer N such that no point in T has more than N preimages in S. To compute μ_T for an irreducible sofic shift T, let f be a 1-block factor map from a 1-step subshift of finite type of equal entropy onto T. Now for each T-word W, $\mu_T(W^0) = \mu_S f^{-1}(W^0)$ will be a sum of boundedly many terms of the form (1.1).

The covering map f above may be chosen so that in addition every bilaterally transitive point in T has a unique preimage in S (f is 1–1 a.e.). Then it is well known (e.g., see the proof of 3.33 in [1]) that there exists a T-word W (a *magic word* for f) such that for some integer I, if x and y are points in $f^{-1}(W^0)$ then $x_I = y_I$. One can check that such a word W satisfies the following definition.

(1.2) Definition. Let W be an allowed word in an irreducible sofic shift T of entropy $\log \lambda$. Then W is a *Markov word* for T if the following hold:

(1) if AW and WB are T-words, then AWB is a T-word;

(2) for any T-words AWC and BWC, the conditional probabilities $\mu_T[W^0C \mid AW^0]$ and $\mu_T[W^0C \mid BW^0]$ are equal;

(3) if $AWUWB$ is a T-word and WU has length k, then $\mu_T(A^0WUWB) = \lambda^{-k}\mu_T(A^0WB)$.

Note that any word containing a Markov word is a Markov word.

Above, the shift T is *almost of finite type* (AFT) if by passing to a higher block presentation of T we may also require that the map f be left and right resolving (see [15] and [5]). In this case,

(1.3) the fraction of words of length k with a unique preimage word under f goes to 1 exponentially as k goes to infinity.

The rest of this section is devoted to the main technical tool for the sequel, "Markov magic words." This is a refinement of standard arguments for bounded-to-one maps from irreducible subshifts of finite type to the case where the domain is sofic. The underlying ideas go back at least to [12] (sections 10 and 11), via [1] (section 3) and [8] (section 3).

Let f be some fixed factor map from an irreducible sofic shift S onto a subshift T of equal entropy. The *coding length* of f is the minimal positive integer k such that for some integer i, $(fx)_0$ is a function only of $x_i \cdots x_{i+k-1}$. Consider the set $\mathcal{W}$ of T-words W for which the following hold:

(i) W is a Markov word for T,

(ii) there exist integers j and k, such that $k - j + 1 \geqq$ coding length of f, and for each x in $f^{-1}(W^0)$, $x_j \cdots x_k$ is Markov for S.

To see that $\mathcal{W}$ is nonempty, pick a point y bilaterally transitive for T, with preimages $x^1, \dots, x^m$. Each of these preimages is bilaterally transitive for S (see the proof of 6.9 in [6]). Pick a Markov word U for S and a Markov word V for T. Now pick a positive integer N greater than the coding length of f such that U occurs in each of the m words $(x^i)_{-N} \cdots (x^i)_N$ and V occurs in $y_{-N} \cdots y_N$. Finally a routine compactness argument shows that for some positive L, if

$$(fz)_{-(N+L)} \cdots (fz)_{(N+L)} = y_{-(N+L)} \cdots y_{(N+L)}$$

then

$$z_{-N} \cdots z_N = (x^i)_{-N} \cdots (x^i)_N \qquad \text{for some } i.$$

Thus the word $y_{-(N+L)} \cdots y_{(N+L)}$ is in $\mathcal{W}$.

Choose a word W for which the number of possible words $x_j \cdots x_k$ in (ii) above is minimal. Call such a word a *Markov magic word* for f. Let $(W^0)_1, \dots, (W^0)_d$ denote the partition of $f^{-1}(W^0)$ by the words in coordinates j through k given by (ii). Now suppose WVW is a T-word, and let L be the length of VW. Given i, the minimality of d guarantees that for some j,

$$(W^0)_i \cap f^{-1}(W^0VW) \cap S^{-L}(W^0)_j \neq \varnothing.$$

Similarly, for some j

$$S^{-L}(W^0)_i \cap f^{-1}(W^0VW) \cap (W^0)_j \neq \varnothing.$$

In particular, the set

$$\{x_j \cdots x_{k+L} : x \in f^{-1}(W^0VW)\}$$

contains at least d words. Moreover, for x in $(W^0)_i \cap f^{-1}(W^0VW)$ (or in $S^{-L}(W^0)_i \cap f^{-1}(W^0VW)$) only one word may occur as $x_j \cdots x_{k+L}$. Otherwise, at least $d+1$ words could occur as $x_j \cdots x_{k+L}$ in $f^{-1}(W^0VW)$; the Markov condition on the words $x_j \cdots x_k$ would let us find at least $d+n$ words which could occur as $x_j \cdots x_{k+nL}$ for x in $f^{-1}(W^0(VW)^n)$; then f would take infinitely many points of S into the periodic orbit $(VW)^\infty$, a contradiction.

These arguments have several easy and useful consequences, summarized in the proposition below. If AWB is a T-word, then $(AW^0B)_i$ is used to represent the set $f^{-1}(AW^0B) \cap (W^0)_i$. A point x is *left transitive* if $\{T^nx : n < 0\}$ is dense. A point x is *bilaterally transitive* if it is left and right transitive.

(1.4) PROPOSITION. *Let f be a factor map from an irreducible sofic shift S onto an irreducible sofic shift T. Let W be a Markov magic word for f; such words exist. Let the d sets $(W^0)_1, \ldots, (W^0)_d$ give the induced partition of $f^{-1}(W^0)$.*

Then the following hold.

(1) *If y is a point in T in which W occurs infinitely often to the left and to the right of the zero coordinate, then y has exactly d preimages in S.*

(2) *Every bilaterally transitive point of T has d preimages.*

(3) *If WVW is a T-word and VW has length L, then for each i in $\{1, \ldots, d\}$ there exist unique j and k with $(W^0VW)_i \cap S^{-L}(W^0)_j \neq \varnothing$ and $(W^0VW)_k \cap S^{-L}(W^0)_i \neq \varnothing$.*

(4) *If VWX is a T-word, then $(VW^0X)_i \neq \varnothing$, $1 \leqq i \leqq d$.*

(5) *Any T-word containing W is a Markov magic word for f.*

(6) *If $VWXWY$ is a T-word, where WX has length L and*

$$(W^0XW)_i \cap S^{-L}(W^0)_i \neq \varnothing,$$

then

$$\frac{\mu_S(VW^0XWY)_i}{\mu_T(VW^0XWY)} = \frac{\mu_S(VW^0Y)_i}{\mu_T(VW^0Y)}, \qquad 1 \leqq i \leqq d. \qquad \blacksquare$$

PROOF. The arguments should be clear, except perhaps for (6), which we now make explicit. By (1.2.3)

$$\mu_T(VW^0XWY) = \lambda^{-L}\mu_T(VW^0Y),$$

so it is enough to show

$$\mu_s(VW^0XWY)_i = \lambda^{-L}\mu_S(VW^0Y)_i.$$

Let $j \cdots k$ be those S-coordinates chosen so that for any x in $f^{-1}(W^0)$, the word $x_j \cdots x_k$ is Markov and the number of such words is minimal. Let $\bar{W}$ be the S-word such that for any x in $(W^0)_i$,

$$x_j \cdots x_k = \bar{W}.$$

Let $\bar{X}$ be the S-word such that for any x in $(W^0XW)_i$,

$$x_j \cdots x_{k+L} = \bar{W}\bar{X}\bar{W}.$$

Then for any S-words $\bar{A}$ and $\bar{B}$, because $\bar{W}$ is Markov,

$$(\bar{A}\bar{W}^i\bar{X}\bar{W}\bar{B}) \cap (VW^0XWY)_i \neq \varnothing$$

if and only if

$$(\bar{A}\bar{W}^i\bar{B}) \cap (VW^0Y) \neq \varnothing.$$

So, if $\{\bar{A}\bar{W}^i\bar{B}\}$ is a collection of disjoint sets with union $(VW^0Y)_i$, then $\{\bar{A}\bar{W}^i\bar{X}\bar{W}\bar{B}\}$ is a collection of disjoint sets with union (VW^0XWY). Therefore it is enough to show

$$\mu_s(\bar{A}\bar{W}^i\bar{X}\bar{W}\bar{B}) = \lambda^{-L}\mu_s(\bar{A}\bar{W}^i\bar{B}).$$

Because $\bar{X}\bar{W}$ has length L, this follows from (1.2.3). ∎

In the sequel, the particular words and coordinates defining the $(W^0)_i$ from a given W are tacitly fixed with W and generally suppressed from the notation.

(1.5) Remark. If S in (1.4) is a subshift of finite type, then the arguments adapt to show that *every* point in T has at least d preimages. This may fail when S is sofic.

For example, let T be the two-shift on symbols 0 and 1. Define f from T to T by $f(x)_i = x_i + x_{i+1}$ (mod 2). Define g from T to a sofic S by collapsing only the two fixed points of T. Now define h from S to T by $f = hg$. Then h has degree two, but one of the fixed points of T has a unique preimage under h. ∎

§2. Constraints on the degrees of factor maps from an irreducible sofic shift

The following lemma is the heart of the paper. It tells us that if a map has degree d, then the inverse image of a typical clopen set is the disjoint union of d clopen sets of equal measure.

(2.1) SPLITTING LEMMA. *Suppose S and T are irreducible sofic shifts of equal entropy, f factors S onto T, and W is a Markov magic word for f.*

Then for any T-word VWX,

$$\mu_S(VW^0X)_i = \frac{1}{d}\,\mu_T(VW^0X), \qquad 1 \leqq i \leqq d.$$

PROOF. For $1 \leqq i \leqq d$, define the ratio sets

$$\mathcal{R}_i = \left\{\frac{\mu_S(VW^0X)_i}{\mu_T(VW^0X)} : VWX \text{ is a } T\text{-word}\right\}.$$

In $\mathcal{R}_i$, we allow V and X to be empty, e.g. $VWX = W$ is a T-word. Each $\mathcal{R}_i$ is finite, so $M_i = \max \mathcal{R}_i$ is defined.

We observe a crucial extension property: if VWX and AWB are T-words, then for any given i, j we may find words U, Y such that $UVWXY$ is a T-word and

$$\frac{\mu_S(UVW^0XY)_j}{\mu_T(UVW^0XY)} = \frac{\mu_S(AW^0B)_i}{\mu_T(AW^0B)}.$$

To show this, choose S-words $\bar{A}\bar{W}_i\bar{B}$ and $\bar{V}\bar{W}_j\bar{X}$ such that $f(\bar{A}\bar{W}_i^0\bar{B}) \subset AW^0B$ and $f(\bar{V}\bar{W}_j^0\bar{X}) \subset VW^0X$. For clarity, require that each (barred) S-word have at least the length of the corresponding (unbarred) T-word.

Now by irreducibility find S-words $\bar{C}$ and $\bar{D}$ such that $(\bar{A}\bar{W}_i\bar{B})\bar{C}(\bar{V}\bar{W}_j\bar{X})\bar{D}(\bar{A}\bar{W}_i\bar{B})$ is an S-word. Let C and D be the T-words such that

$$f(\bar{A}\bar{W}_i^0\bar{C}\bar{V}\bar{W}_j\bar{X}\bar{D}\bar{W}_i\bar{B}) \subset AW^0CVWXDWB.$$

Let $U = AWC$, $Y = DWB$. Then

$$\begin{aligned}\frac{\mu_S(UVW^0XY)_j}{\mu_T(UVW^0XY)} &= \frac{\mu_S(AWCVW^0XDWB)_j}{\mu_T(AWCVW^0XDWB)} \\ &= \frac{\mu_S(AW^0CVWXDWB)_i}{\mu_T(AW^0CVWXDWB)} && \text{by (1.4.3)} \\ &= \frac{\mu_S(AW^0B)_i}{\mu_T(AW^0B)} && \text{by (1.4.6).}\end{aligned}$$

In particular, the extension property shows M_i is independent of i, say $M_i = M$.

Now suppose VWX is a T-word such that

$$(*) \qquad \frac{\mu_S(VW^0X)_i}{\mu_T(VW^0X)} = M,$$

and consider the symbols α such that $VWX\alpha$ is a T-word. Then

$$M\mu_T(VW^0X) = \mu_S(VW^0X)_i = \sum_\alpha \mu_S(VW^0X\alpha)_i$$
$$\leqq \sum_\alpha M\mu_T(VW^0X\alpha) = M\mu_T(VW^0X).$$

Therefore $\mu_S(VW^0X\alpha)_i = M\mu_T(VW^0X\alpha)$ for each α. Inducting this argument on both sides of VWX gives a stability property: if $UVWXY$ is a T-word and (*) holds for VWX, then

$$\frac{\mu_S(UVW^0XY)_i}{\mu_T(UVW^0XY)} = M.$$

Using the stability and extension properties, we easily find a T-word VWX such that $\mu_S(VW^0X)_i = M\mu_T(VW^0X)$, $1 \leqq i \leqq d$. Since $\mu_T(VW^0X) = \mu_S f^{-1}(VW^0X) = \Sigma\mu_S(VW^0X)_i$, this forces $M = 1/d$. Thus $\mathcal{R}_i = \{1/d\}$ for each i, otherwise for some T-word UWY we would find

$$\mu_T(UW^0Y) = \sum_i \mu_S(UW^0Y)_i$$
$$< \sum_i \left(\frac{1}{d}\right) \mu_T(UW^0Y) = \mu_T(UW^0Y),$$

a contradiction. ■

(2.2) THEOREM. *Let S and T be irreducible sofic shifts of entropy* $\log\lambda$. *Then there exists a finite set E of positive integers such that for any factor map of S onto T, we have* $\deg f = eu$, *where $e \in E$ and u is a positive integer which is a unit in the ring* $\mathbf{Z}[1/\lambda]$.

PROOF. Suppose f factors S onto T and $\deg f = d$. Let W be a Markov magic word for T, with $\mu_T(W^0) = \alpha\lambda^{-n}$, $\alpha \in Q(\lambda)$. Choose β in $\mathbf{Z}[\lambda]$ such that for any closed open set C of S, $\beta\mu_S C \in \mathbf{Z}[1/\lambda]$. By the splitting lemma,

$$\beta\left(\frac{\alpha\lambda^{-n}}{d}\right) \in \mathbf{Z}[1/\lambda], \qquad \text{or} \qquad \frac{\beta\alpha}{d} \in \mathbf{Z}[1/\lambda].$$

Pick a rational integer m such that

$$\left(\frac{m}{\beta\alpha}\right) \in \mathbf{Z}[\lambda] \subset \mathbf{Z}[1/\lambda],$$

so that

$$\left(\frac{m}{\beta\alpha}\right)\left(\frac{\beta\alpha}{d}\right) = \frac{m}{d} \in \mathbf{Z}[1/\lambda].$$

Let E be the set of positive integers dividing m. Write $d = eu$, where $e = \gcd(m, d) \in E$. Let $l = m/e$. Then

$$\frac{l}{u} = \frac{le}{ue} = \frac{m}{d} \in \mathbf{Z}[1/\lambda],$$

with l and u relatively prime. If p is a prime dividing u, then

$$\left(\frac{l}{p}\right) = \left(\frac{u}{p}\right)\left(\frac{l}{u}\right) \in \mathbf{Z}[1/\lambda],$$

and therefore $1/p \in \mathbf{Z}[1/\lambda]$. It follows by multiplying that $1/u \in \mathbf{Z}[1/\lambda]$. ■

The rational integral units of $\mathbf{Z}[1/\lambda]$ are readily computed from the following proposition.

(2.3) Proposition. *Let λ be an algebraic integer with minimal polynomial $r(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, and suppose $d \in \mathbf{Z}$. Then the following conditions are equivalent.*

(1) *d is a unit in $\mathbf{Z}[1/\lambda]$.*

(2) *If p is a rational prime dividing d, then p divides a_i, $0 \leqq i \leqq n-1$.*

(3) *d divides some power of the greatest common divisor of $\{a_i : 0 \leqq i \leqq n-1\}$.*

Proof. (2) $\Leftrightarrow$ (3): This is clear.

(2) $\Rightarrow$ (1): Here $1/p = -\lambda^{-n} \sum_{i=0}^{n-1} (a_i/p)\lambda^i \in \mathbf{Z}[1/\lambda]$, for each prime divisor of d. Therefore $1/d \in \mathbf{Z}[1/\lambda]$.

(1) $\Rightarrow$ (2): Suppose p is a prime divisor of d. Then $1/p = (d/p)(1/d) \in \mathbf{Z}[1/\lambda]$, so for some integers b_i and some positive m, $1/p = \sum_{i=0}^{m} b_i\lambda^{-i}$. Let

$$q(x) = x^m - \sum_{i=0}^{m} pb_i x^{m-i} \in \mathbf{Z}[x].$$

Since $q(\lambda) = 0$, the polynomial $r(x)$ divides $q(x)$ in $\mathbf{Z}[x]$, say $q = rs$.

Now (2) follows from the argument of the Gauss Lemma. Choose the integers i and j minimal for the following property: the term in r of degree i and the term in s of degree j have coefficients nonzero mod p. Then the term in q of degree $(i+j)$ has coefficient nonzero mod p. Thus $i + j = m$, and only the leading coefficients of r and s can be nonzero mod p. ■

(2.4) Corollary. *Let S and T be irreducible sofic shifts of entropy* $\log \lambda$. *Let $U(\lambda)$ be the set of positive integers which divide some power of the greatest common divisor of the nonleading coefficients of the minimal polynomial of λ.*

Then there is a finite set E of integers such that for any factor map f of S onto T, *we have* $\deg f = eu$, *where* $e \in E$ *and* $u \in U(\lambda)$. *If* f *is an endomorphism, then* $\deg f \in U(\lambda)$.

PROOF. The existence of E is immediate from (2.2) and (2.3). If f is an endomorphism with $\deg f = eu$, then f^k is an endomorphism with $\deg(f^k) = e^k u^k$. This forces some power of e, and therefore e itself, to lie in $U(\lambda)$. ■

In some cases the splitting lemma holds for all clopen sets.

(2.5) THEOREM. *Suppose* S *and* T *are irreducible sofic shifts of equal entropy,* T *is almost finite type* (AFT) *and* f *has degree* d.

Then for any closed open set C *in* T, $f^{-1}C$ *is the disjoint union of* d *clopen sets of equal* μ_S *measure.*

PROOF. It is enough to consider for C a given set of the form W^0, where W is a T-word. Given n, consider the partition of W^0 into sets VW^0X, where V and X are words of length n, and let B_n be the union of those VW^0X for which VWX is not a Markov magic word for f. Then $\mu_T(B_n)$ goes to zero exponentially as n goes to infinity. By (1.3), for large n we may find a clopen set D contained in W^0 which is the disjoint union of d sets of equal μ_T measure, one of which is B_n. Then $f^{-1}D$ splits as required. By (2.1), $f^{-1}(W^0 \sim D)$ splits. So, $f^{-1}(W^0)$ splits. ■

(2.6) COROLLARY. *Let* S *be an irreducible sofic shift of entropy* $\log \lambda$. *Suppose* $\eta \in Q(\lambda)$ *and for every closed open set* C *in* S, $\mu_S C \in (1/\eta)\mathbf{Z}[1/\lambda]$. (*For example, if* S *is finite type with* μ_S *defined from* (1.1) *with* l *and* r *over* $\mathbf{Z}[1/\lambda]$, *then* $\eta = lr$ *will do.*)

Then for any factor map f *of degree* d *from* S *onto an* AFT *shift of equal entorpy,* $\eta/d \in \mathbf{Z}[1/\lambda]$. *The set of such* d *is finite modulo multiplication by positive integers which are units in* $\mathbf{Z}[1/\lambda]$.

PROOF. By (2.5), $1/d \in (1/\eta)\mathbf{Z}[1/\lambda]$. The last claim follows the argument in (2.2). ■

(2.7) REMARK. In particular, in the category of shifts of finite type, the set E of (2.4) may be chosen independent of T.

(2.8) EXAMPLES. If in (2.6) S is the two-shift, we may set $\eta = 1$; thus d must be a power of 2. (This may also be deduced from theorem 4.3 of [15] and theorem 14.9 of [12].) If in (2.6) S is the golden mean shift, defined by the matrix $\left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right)$, we may set $\eta = \lambda^2 + 1$, with minimal polynomial $x^2 - 5x + 5$. Here $\mathbf{Z}[1/\lambda] = \mathbf{Z}[\lambda]$, and d must be 1. ■

I do not know if the AFT condition in (2.5), (2.6) or (2.7) may be dropped. The remaining examples of this section address sharpness questions raised by (2.3).

(2.9) Example. There is a noninvertible endomorphism of a mixing subshift of finite type S, where S has entropy $\log\lambda$ and λ is an algebraic unit.

Proof. Let S be the set of all bisequences on symbols $\{0,1,2\}$ in which 2 is always preceded by 0. Then S is given by the matrix

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

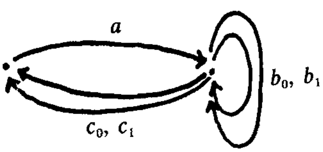
with characteristic polynomial $x(x^2-2x-1)$. Define the endomorphism f by

$$\begin{aligned}(fx)_i &= x_i + x_{i+1} \quad (\text{mod } 2) \text{ if } \{x_i, x_{i+1}\} \subset \{0,1\},\\ &= x_i \qquad\qquad \text{otherwise.}\end{aligned}$$

Clearly f is well defined. Since $f(x)_i\,(fx)_{i+1}$ and x_{i+1} determine x_i, f is bounded-to-one. A point x has two preimages if and only if there is an integer n such that $x_i \neq 2$ when $i \geqq n$. ■

(2.10) Example. A mixing subshift of finite type S may admit a degree two endomorphism, even though the entropy of S is $\log\lambda$ where $\lambda/2$ is not an algebraic integer.

Proof. Define S from the matrix $\left(\begin{smallmatrix} 0 & 1 \\ 2 & 2 \end{smallmatrix}\right)$, so λ has minimal polynomial x^2-2x-2 and $\lambda/2$ has minimal polynomial $x^2-x-\frac{1}{2}$. The state symbols of S are the edges of the graph



where the given symbols name the edges. An edge e may precede an edge f in S iff the terminal vertex of e is the initial vertex of f. Define the endomorphism f by

$$\begin{aligned}(fx)_i &= a \qquad \text{if } x_i = a\\ (fx)_i &= d_{j+k} \quad \text{if } x_ix_{i+1}x_{i+2} = d_jae_k \text{ or } x_ix_{i+1} = d_je_k,\end{aligned}$$

where $\{d,e\} \subset \{b,c\}$ and $j+k$ is interpreted mod 2. ■

The trick above works as well for a defining matrix $\binom{0\ 1}{8\ 2}$ with (reducible) characteristic polynomial $x^2-2x-8=(x-4)(x+2)$. The trick also works for other prime degrees p, but always it forces the characteristic polynomial of the defining matrix to be a monomial mod p. Must this always hold? Does the zeta function of an irreducible subshift of finite type (sofic shift?) constrain the degrees of endomorphisms?

§3. Endomorphisms multiply the natural measure on unstable sets

Much of this section is implicit in the literature (but deserves an explicit exposition). More detailed acknowledgements, especially to work of Cuntz and Krieger, are deferred to (3.7) below.

Suppose S is a subshift. Given $x \in S$, $n \in \mathbf{Z}$, let $x_{(-\infty,n]}=\{y \in S : y_i = x_i,\ i \leqq n\}$. Let $W^u(x)=\bigcup_{n\in\mathbf{Z}} x_{(-\infty,n]}$, the *unstable set* of x. Make $W^u(x)$ a σ-compact space by taking as a basis for the topology the collection $\{y_{(-\infty,n]} : y \in W^u(x), n \in \mathbf{Z}\}$.

Let A be a $k\times k$ irreducible zero-one matrix with spectral radius λ and positive left and right eigenvectors l and r for λ. Suppose S is the irreducible subshift of finite type on symbols $\{1,\dots,k\}$ defined by A. Then on each $W^u(x)$ there is a σ-finite Borel measure μ^x determined by

$$\mu^x y_{(-\infty,n]}=\lambda^{-n}r(y_n); \qquad y\in W^u(x), \qquad n\in\mathbf{Z}. \tag{3.1}$$

Notice the family of measures $\{\mu^x\}$ will vary in (3.1) by a universal scalar multiple as the choice of the eigenvector r varies.

(3.2) PROPOSITION. *Let S be an irreducible subshift of finite type with entropy $\log\lambda$. Then there exists a collection $\{\mu^x\}$ of Borel measures on the unstable sets $W^u(x)$ of S satisfying the following properties for every x, y in S and n in $\mathbf{Z}$:*

(1) *$\mu^x x_{(-\infty,n]}$ is finite and nonzero;*

(2) *$\mu^x x_{(-\infty,n]}=\lambda^{-1}\mu^{Sx}(Sx)_{(-\infty,n-1]}$;*

(3) *there exists a positive integer N such that if $x_0\cdots x_N=y_0\cdots y_N$ then $\mu^x x_{(-\infty,N]}=\mu^y y_{(-\infty,N]}$.*

If $\{\nu^x\}$ is another such collection satisfying these properties, then there is a scalar M such that $M\nu^x=\mu^x$, for all x in S.

REMARK. The properties (1) and (2) determine μ^x up to a scalar on any given $W^u(x)$. The Markov property (3) relates the various μ^x.

PROOF. Any irreducible subshift of finite type is topologically conjugate to one defined by an irreducible zero-one matrix. Then the collection of measures given by (3.1) transports to S and satisfies the required properties.

Suppose $\{\mu^x\}$ and $\{\nu^x\}$ are two such collections on S, with N as in (3) for both. By (2), the sets of ratios

$$\left\{\frac{\mu^x x_{(-\infty,n]}}{\nu^x x_{(-\infty,n]}} : x \in S,\ n \in \mathbf{Z}\right\} \quad \text{and} \quad \left\{\frac{\mu^x x_{(-\infty,0]}}{\nu^x x_{(-\infty,0]}} : x \in S\right\}$$

are equal. By (1) and (3), there is a positive finite maximum M to this set. Let $z_{(-\infty,0]}$ be a set on which this maximum is achieved.

A simple extremal argument (of the sort used in the stability step of (2.1)) shows that if $x_{(-\infty,0]} = z_{(-\infty,0]}$ and $n \geqq 0$, then $\mu^x x_{(-\infty,n]} = M\nu^x x_{(-\infty,n]}$. By irreducibility, for any word W of length N, we may find x in S and $m > 0$ such that $x_{(-\infty,0]} = z_{(-\infty,0]}$ and $x_m \cdots x_{m+N-1} = W$, so $\mu^x x_{(-\infty,m+N-1]} = M\nu^x x_{(-\infty,m+N-1]}$. Now (2) and (3) show that $\mu^x = M\nu^x$, for all x in S. ■

(3.3) Remark. In (3.2), for a given x the measure of maximal entropy μ_S determines (induces) μ^x up to a scalar multiple by way of conditional measures. For each n, there is a scalar γ_n such that if $y \in x_{(-\infty,n]}$, $m \in \mathbf{Z}$, then

$$\mu^x y_{(-\infty,m]} = \gamma_n \lim_{k\to-\infty} \mu_S\left[y_{[k,m]} \,\middle|\, x_{[k,n]}\right].$$

The scalars γ_n are determined by the nesting of the sets $x_{(-\infty,n]}$ once $\mu^x x_{(-\infty,0]}$ is set.

Also, it is easy to show that it is now necessary to assume a priori that the scalar λ in (2) is given by the entropy. ■

(3.4) Proposition. *Let S be an irreducible sofic shift with entropy* $\log\lambda$. *Let $\mathcal{S}$ be a set of left transitive points of S. Then there exists a collection $\{\mu^x\}$ of measures on $\{W^u(x) : x \in \mathcal{S}\}$ satisfying the following properties for every x, y in $\mathcal{S}$ and n in* $\mathbf{Z}$:

(1) $\mu^x x_{(-\infty,n]}$ *is finite and nonzero*;

(2) $\mu^x x_{(-\infty,n]} = \lambda^{-1}\mu^{Sx}(Sx)_{(-\infty,n-1]}$;

(3) *for each x there exists $N > 0$ such that if $x_{-N}\cdots x_0 = y_{-N}\cdots y_0$, then* $\mu^x x_{(-\infty,0]} = \mu^y y_{(-\infty,0]}$;

(4) *the set $\{\mu^x x_{(-\infty,0]} : x \in \mathcal{S}\}$ is finite.*

If $\{\nu^x\}$ is another such collection, then there is a positive number M such that $M\nu^x = \mu^x$, for all $x \in \mathcal{S}$.

Proof. Consider any 1-block, 1–1. a.e. map f from a 1-step irreducible SFT $\hat{S}$ onto S. Let $\{\mu^{\hat{x}}\}$ be a collection for $\hat{S}$ as in (3.2). Then for each x in $\mathcal{S}$, there exists $\hat{x}$ in $\hat{S}$ such that $f^{-1}W^u(x) = W^u(\hat{x})$.

Define $\mu^x = \mu^{\hat{x}} \circ f^{-1}$. Now (1), (2) and (4) are immediate, and (3) follows for a given x in $\mathcal{S}$ by choosing N so that $x_{[-N,0]}$ is a magic word for f. The uniqueness argument mimics (3.2). ∎

Analogous measures, $\{\nu^x\}$ say, may be defined on the stable sets

$$W^s(x) = \bigcup_n x_{[n,\infty)}.$$

In place of (3.1), we set

$$\nu^x x_{[n,\infty)} = \lambda^n l(x_n), \tag{3.5}$$

where l is a positive left eigenvector for λ. In the sofic case, we consider right-transitive points.

(3.6) THEOREM. *Suppose S and T are irreducible sofic shifts of equal entropy and f factors S onto T. Choose families $\{\mu_S^x\}$ and $\{\mu_T^x\}$ for left transitive x as in (3.4). Given $f(x) = y$, with y (and thus x) left transitive, $z \in W^u(y)$ and $n \in \mathbf{Z}$, define the ratio*

$$R(x, y, z, n) = \frac{\mu_S^x(f^{-1}(z_{(-\infty,n]}) \cap W^u(x))}{\mu_T^y(z_{(-\infty,n]})}.$$

Then $R(x, y, z, n)$ is the same number R for any x, y, z, n; so, $f_*\mu^x = R\mu^y$ for all such x and y. If $S = T$, require $\{\mu_S^x\} = \{\mu_T^x\}$; then R is a number $R(f)$ which depends only on f, and is invariant under recodings.

PROOF. The set of such $R(x, y, z, n)$ is finite, say with maximum M. Choose $\bar{x}$ and $\bar{y}$ so that $R(\bar{x}, \bar{y}, \bar{y}, 0) = M$. Pick N so that $\bar{y}_{[-N,0]} = W$ a Markov magic word for f, and I so that $\bar{x} \in S^N(W^0)_I$. Then $R(x, y, y, n) = R(\bar{x}, \bar{y}, \bar{y}, 0) = M$ whenever $y_{[n-N+1,n]} = W$ and $x \in S^{-n}(W^0)_I$; this holds for infinitely many negative numbers n for x and y left transitive. But if $R(x, y, y, n) = M$, then the simple extremal argument of (2.1) shows $R(x, y, z, m) = M$ whenever $z_{(-\infty,m]} \subset y_{(-\infty,n]}$. If $\{\mu_S^x\} = \{\mu_T^x\}$, then in the ratios the arbitrary scaling factors cancel, and the invariance follows from (3.4). ∎

(3.7) ACKNOWLEDGEMENTS. The measures μ^x and their essential uniqueness on an unstable set are well known for subshifts of finite type. Proposition (3.2) can be developed from the hyperbolic differential viewpoint along the lines of [2]. A direct demonstration of (3.2) may be recovered from the proof of (3.3) in [8]. This proof of Cuntz and Krieger also proves a slightly weaker version of (3.6): there is a number $\tilde{R}$ such that $\tilde{R}\mu_T^y = \Sigma_{fx=y} f_*\mu_S^x$, for each left transitive y. (So, for endomorphisms, $\tilde{R}(f) = (\deg f)R(f)$.) Their proof also invokes magic words, and uses an ergodic argument in place of an extremal argument.

(3.8) Definition. Let $L(f)$ be the number obtained by proving the analogue of (3.6) on stable sets. Alternatively, $L(f)$ is $R(f)$ computed with respect to S^{-1}.

(3.9) Lemma. *Suppose T is an irreducible sofic shift, and f is an endomorphism of T of degree d. Then $dL(f)R(f)=1$.*

Proof. Let ϕ be a 1–1 a.e., 1-block factor map of a 1-step irreducible subshift of finite type S onto T (if T is finite type, then $\phi=\mathrm{id}$). Let l and r be positive left and right eigenvectors of an irreducible zero-one matrix defining S, with $lr=1$; so, if $U=u_0\cdots u_n$ is an S-word, then $\mu_S U^0=\lambda^{-n}l(u_0)r(u_n)$. Define $\{\mu_S^x\}$ and $\{\nu_S^x\}$ for S as in (3.1) and (3.5). Then define the corresponding measures for bilaterally transitive y in T by

$$\mu_T^y=\phi_*\mu_S^x,\quad \nu_T^y=\phi_*\nu_S^x;\qquad x=\phi^{-1}(y).$$

Let W be a magic word for ϕ which is a Markov magic word for f, with integers $j\leqq k$ such that there are d possible words $V_1,\dots,V_d$ which may occur as $x_j\cdots x_k$ for x in $f^{-1}(W^0)$, and each of these words is a magic word for ϕ. Choose V_i, defining $(W^0)_i$. Now for some integer I and some symbol α, $x\in\phi^{-1}(W^0)_i$ implies $x_I=\alpha$. Similarly choose J and β so that $x\in\phi^{-1}(W^0)$ implies $x_J=\beta$. Now choose n and collections of S-words $\mathcal{A}$, $\mathcal{B}$, $\bar{\mathcal{A}}$ and $\bar{\mathcal{B}}$ such that

$$\phi^{-1}(W^0)_i=\{x\in S: x_{-n}\cdots x_{I-1}\in\mathcal{A},\ x_I=\alpha,\ x_{I+1}\cdots x_n\in\mathcal{B}\}$$

and

$$\phi^{-1}(W^0)=\{x\in S: x_{-n}\cdots x_{J-1}\in\bar{\mathcal{A}},\ x_J=\beta,\ x_{J+1}\cdots x_n\in\bar{\mathcal{B}}\}.$$

Then

$$\left(\frac{\mu_T(W^0)_i}{\mu_T(W^0)}\right)=\frac{\left(\sum\limits_{\substack{a_1\cdots a_n\\ \in\mathcal{A}}} l(a_1)\right)\left(\sum\limits_{\substack{b_1\cdots b_n\\ \in\mathcal{B}}} r(b_n)\right)\lambda^{-2n}}{\left(\sum\limits_{\substack{a_1\cdots a_n\\ \in\bar{\mathcal{A}}}} l(a_1)\right)\left(\sum\limits_{\substack{b_1\cdots b_n\\ \in\bar{\mathcal{B}}}} r(b_n)\right)\lambda^{-2n}}=L(f)R(f).$$

Now

$$dL(f)R(f)=\sum_i\left(\frac{\mu_T(W^0)_i}{\mu_T(W^0)}\right)=1. \qquad\blacksquare$$

The result above gives an alternate proof of (2.1), actually closer to the proof of Welch's result in [12]. But the basic idea of (2.1) seems more clear without $R(f)$ and $L(f)$.

(3.10) THEOREM. *Let S be an irreducible sofic shift of entropy* $\log \lambda$. *Let* $\mathrm{End}(S)$ *denote the semigroup of endomorphisms of S. Let $\mathcal{O}_\lambda$ denote the ring of algebraic integers of $Q(\lambda)$, and $\mathcal{O}_\lambda[1/\lambda]$ the ring generated by $\mathcal{O}_\lambda$ and $1/\lambda$.*

Then the maps $R: f \mapsto R(f)$ and $L: f \mapsto L(f)$ give homomorphims of $\mathrm{End}(S)$ *into the positive units of $\mathcal{O}_\lambda[1/\lambda]$.*

PROOF. Clearly $R(fg) = R(f)R(g)$. Pick a family $\{\mu^x\}$ as in (3.4) for left transitive x, with $\mu^x x_{(-\infty,0]} \in \mathcal{O}_\lambda$ for all such x. Given f, fix k and $\tilde{f} = S^{-k}f$ such that for all x, $x_{(-\infty,0]}$ determines $(\tilde{f}x)_{(-\infty,0]}$. Then for all positive n, $x_{(-\infty,0]}$ determines $(\tilde{f}^n x)_{(-\infty,0]}$. Pick a left transitive point y and a preimage x; let $\mu^y y_{(-\infty,0]} = \alpha$. Computing $R(\tilde{f}^n)$ with respect to this pair, find $\alpha R(\tilde{f}^n) \in \mathcal{O}_\lambda$, $n > 0$. Therefore $\alpha[R(\tilde{f})]^n \in \mathcal{O}_\lambda$, $n > 0$, and so $R(\tilde{f}) \in \mathcal{O}_\lambda$. Since $R(\tilde{f}) = \lambda^k R(f)$, $R(f) \in \mathcal{O}_\lambda[1/\lambda]$.

Likewise, L is a homomorphism into $\mathcal{O}_\lambda[1/\lambda]$. By (3.9), $L(f)$ and $R(f)$ must always be units of this ring. ∎

(3.11) REMARKS. In particular, if in (3.10) λ is an algebraic unit, then $L(f)$ and $R(f)$ must be algebraic units. However, they need not lie in $\mathbf{Z}[1/\lambda]$. For example, let f be the golden mean shift, defined by the matrix $\left(\begin{smallmatrix}0 & 1\\ 1 & 1\end{smallmatrix}\right)$; let $S = f^3$. Let α be the golden mean, so

$$\lambda = \alpha^3 = \left(\frac{1+\sqrt{5}}{2}\right)^3 = 2 + \sqrt{5}.$$

Then

$$R(f) = \alpha^{-1} = \frac{1-\sqrt{5}}{2} \notin \mathbf{Z}[\sqrt{5}] = \mathbf{Z}[\lambda] = \mathbf{Z}[1/\lambda]. \quad ∎$$

Theorem (3.10) constrains the range of R and L. Are there other constraints?

REFERENCES

1. R. L. Adler and B. Marcus, *Topological entropy and equivalence of dynamical systems*, Mem. Amer. Math. Soc. **219** (1979).
2. R. Bowen and B. Marcus, *Unique ergodicity for horocycle foliations*, Israel J. Math. **26** (1977).
3. M. Boyle, *Lower entropy factors of sofic systems*, Ergodic Theory and Dynamical Systems **3** (1983).
4. M. Boyle and W. Krieger, *Periodic points and automorphisms of the shift*, preprint.
5. M. Boyle, B. Kitchens and B. Marcus, *A note on minimal covers for sofic systems*, to appear in Proc. Amer. Math. Soc.
6. E. Coven and M. Paul, *Endomorphisms of irreducible subshifts of finite type*, Math. Syst. Th. **8** (1974), 167–175.
7. E. Coven and M. Paul, *Sofic systems*, Israel J. Math. **20** (1975).
8. J. Cuntz and W. Krieger, *Topological Markov chains with dicyclic dimension groups*, Crelles J. **320** (1980), 44–51.

9. M. Denker, C. Grillenberger and K. Sigmund, *Ergodic Theory on Compact Spaces*, Lecture Notes in Maths. **527**, Springer-Verlag, Berlin, 1976.

10. D. Farmer, T. Toffoli and S. Wolfram, eds., *Cellular Automata*, Physica D, **10D** (1984), Nos. 1 and 2.

11. R. Fischer, *Sofic systems and graphs*, Monatsh. Math. **80** (1975), 179–186.

12. G. A. Hedlund, *Endomorphisms and automorphisms of the shift dynamical system*, Math. Syst. Th. **3** (1969), 320–375.

13. B. Kitchens, *Linear algebra and subshifts of finite type*, in *Contemporary Mathematics*, Vol. 26 (R. Beals et al., eds.), Amer. Math. Soc., Conference in Modern Analysis and Probability, 1984.

14. W. Krieger, *On sofic systems I*, Israel J. Math. **48** (1984).

15. B. Marcus, *Sofic systems and encoding data*, IEEE Trans. Inf. Theory (1985), 366–377.

16. J. Milnor, *Notes on surjective cellular automation-maps*, preliminary draft.

17. M. Nasu, *An invariant for bounded-to-one factor maps between transitive sofic subshifts*, Ergodic Theory and Dynamical Systems **5** (1985).

18. W. Parry and S. Tuncel, *Classification Problems in Ergodic Theory*, L. M. S. Lecture Notes **67**, Cambridge Univ. Press, 1982.

19. B. Weiss, *Subshifts of finite type and sofic systems*, Monatsh. Math. **77** (1973), 462–474.