Math-Net.Ru

Общероссийский математический портал

J. Hančl, A. Jaššová, P. Lertchoosakul, R. Nair, Polynomial Actions in Positive Characteristic, *Совр. пробл. матем.*, 2012, выпуск 16, 45–51

DOI: <https://doi.org/10.4213/spm33>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением <http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 3.80.253.173

26 апреля 2023 г., 10:05:05

Polynomial Actions in Positive Characteristic

J. Hančl^a, A. Jaššová^b, P. Lertchoosakul^b, R. Nair^b

^a *University of Ostrava, Czech Republic*

^b *University of Liverpool, UK*

In honour of Professor A. A. Karatsuba's 75th birthday

1. Introduction

Let q be a power of a prime p and $\mathbb{F}_q$ be the finite field with q elements. Denote by $\mathbb{F}_q[X]$ and $\mathbb{F}_q(X)$ the ring of polynomials with coefficients in $\mathbb{F}_q$ and the quotient field of $\mathbb{F}_q[X]$ respectively. For each $P/Q \in \mathbb{F}_q(X)$ define $|P/Q| = q^{\deg(P) - \deg(Q)}$ where for an element $g \in \mathbb{F}_p[X]$ we have denoted its degree by $\deg(g)$. Note that with respect to the valuation function $|\cdot|$ the integral domain $\mathbb{F}_q[X]$ is a Euclidean domain and so also a principal ideal domain and a unique factorization domain. In particular Bezout's identity is satisfied. Let $\mathbb{F}_q((X^{-1}))$ denote the field of formal Laurent series

$$\mathbb{F}_q((X^{-1})) = \{a_n X^n + \cdots + a_0 + a_{-1} X^{-1} + \cdots : n \in \mathbb{Z}, a_i \in \mathbb{F}_q\},$$

and let

$$\mathbb{L} = \{a_{-1} X^{-1} + a_{-2} X^{-2} + \cdots : a_i \in \mathbb{F}_q\}.$$

Also $d_q(x, y) = |x - y|$ for $x, y \in \mathbb{F}_q(X)$ defines a metric on $\mathbb{F}_q(X)$ and $\mathbb{F}_q((X^{-1}))$ is its completion with respect to this metric. The metric extends to $\mathbb{F}_q((X^{-1}))$ by completion and by implication to its subset $\mathbb{L}$. Note that this metric is non-archemedian since $|x + y| \leq \max(|x|, |y|)$. As $\mathbb{F}_q[X]$ is a unique factorisation domain, each of its elements has a canonical factorisation into a unique product of irreducible elements – in effect the fundamental theorem of arithmetic for the ring $\mathbb{F}_q[X]$. Because of this we can speak of two elements P, Q of $\mathbb{F}_q[X]$ as being coprime in a well defined sense. We write this briefly as $(P, Q) = 1$.

For $x \in \mathbb{F}_q((X^{-1}))$ let $[x]$ denote the unique $P \in \mathbb{F}_q[X]$ such that $x - [x] \in \mathbb{L}$ and let $\{x\} = x - [x]$. We readily check that for $x \in \mathbb{L}$ and $P, Q \in \mathbb{F}_q[X]$ we have $\{P\{Qx\}\} = \{PQx\}$. This means $\mathbb{F}_p[X]$ defines a commutative action on $\mathbb{L}$. As $x \rightarrow \{Qx\}$ is a continuous endomorphism of the additive group $\mathbb{L}$, it preserves Haar measure μ on the compact abelian group $\mathbb{L}$, characterised by the identity

$$\mu(\{a_{-1} X^{-1} + a_{-2} X^{-2} + \cdots \in \mathbb{L} : a_{-1} = x_1, \dots, a_{-n} = x_n\}) = \frac{1}{q^n}$$

for any $x_1, \dots, x_n \in \mathbb{F}_q$. See [1] for details of this. Chapter 1 of [2] also gives more general background.

Let (Y, β, m) denote a probability space, with a set Y , a σ -algebra of its subsets β and a probability measure m . A partition of (Y, β, m) is a finite or countable collection of elements $\alpha = (A_i)_{i \in I}$ of β such that A_i, A_j are pairwise disjoint for all distinct pairs $i \neq j$ and $\bigcup_{i \in I} A_i = Y$. We say a map $T: Y \rightarrow Y$ is measure preserving if $T^{-1}A := \{x \in Y : Tx \in A\}$ is in β if A is and $m(T^{-1}A) = m(A)$. We say that it is ergodic if $m(T^{-1}A) = m(A)$ for $A \in \beta$ means that $m(A)$ is either 0 or 1. For a two generator commutative semigroup of measure preserving transformations $\{T^m S^n : (m, n) \in \mathbb{Z}_+^2\}$, we say it is ergodic if for each pair of elements $A, B \in \beta$ with $m(A) > 0$

This work was supported by the European Regional Development Fund in the IT4Innovations Centre of Excellence project (CZ.1.05/1.1.00/02.0070) and by the grants no. P201/12/2351 and ME09017.

and $m(B) > 0$ there exists $(m, n) \in \mathbb{Z}_+^2$ such that $m(T^m S^n A \cap B) > 0$. Here we have used $\mathbb{Z}_+$ to denote the non-negative integers. Note, for a measure preserving transformation T , that $T^{-1}\alpha = (T^{-1}A_i)_{i \in I}$ is a partition of X if $\alpha = (A_i)_{i \in I}$ is a partition of X . Given two partitions $\alpha_1 = (A_i^1)_{i \in I}$ and $\alpha_2 = (A_j^2)_{j \in J}$ we use $\alpha_1 \vee \alpha_2$ to denote the partition $(A_i^1 \cap A_j^2)_{(i,j) \in I \times J}$. For a finite partition $\alpha = \{A_1, \dots, A_n\}$, we define its entropy to be $H(\alpha) = -\sum_{i=1}^n m(A_i) \log m(A_i)$. For a measure preserving transformation (Y, β, m, T) we define its entropy with respect to $\alpha = \{A_1, \dots, A_n\}$ to be the limit

$$h(T, \alpha) = \lim_{n \rightarrow \infty} \frac{1}{n} H\left(\bigvee_{j=0}^{n-1} T^{-j}\alpha\right),$$

which is always known to exist [3], being the limit of a decreasing sequence bounded below. We define $h(T) = \sup_{\alpha} h(T, \alpha)$, where the supremum is taken over all finite partitions α from β . We call $h(T)$ the entropy of the “dynamical system” (Y, β, m, T) . A systematic account of this fundamental invariant can be found in Chapter 4 of [3] or [4]. For convenience for a partition α we occasionally write α_m^n to denote $T^{-m}\alpha \vee \dots \vee T^{-n}\alpha$ for $n > m \geq 0$.

Our theorem is the extension of a result in [5] to positive characteristic. The method of proof is adapted from that given by Parry [6] however. We have tried to keep the exposition as self contained as possible to meet the needs of readers not familiar with ergodic theory. There are however limits to the extent to which this is possible and some prior acquaintance with the theory of entropy of dynamical systems would be helpful. All that is needed however is available from standard references which we cite.

THEOREM. *Suppose P and Q are coprime non-zero elements of $\mathbb{F}_q[X]$, and let T_P and T_Q denote the continuous endomorphisms of $\mathbb{L}$ defined by $x \rightarrow \{Px\}$ and $x \rightarrow \{Qx\}$ respectively. Suppose T_P and T_Q both preserve the non-atomic measure m and that $\{T_Q^m T_P^n : (m, n) \in \mathbb{Z}_+^2\}$ is ergodic. Let $h(T_P)$ and $h(T_Q)$ denote the entropies of T_P and T_Q respectively with respect to m . Then either $h(T_P) = h(T_Q) = 0$ or m is Haar measure on $\mathbb{L}$.*

The context of this result is the following. In [7] Furstenberg asked whether the only non-atomic measure that is preserved for coprime natural numbers a, b by both the maps $x \rightarrow ax \pmod{1}$ and $x \rightarrow bx \pmod{1}$ is Lebesgue measure. In particular he was interested in the case $a = 2$ and $b = 3$. This problem remains open. Lyons [5] obtained a first partial result under the extra assumptions that m satisfies a measure theoretic condition called exactness with respect to one of the maps $x \rightarrow ax \pmod{1}$, $x \rightarrow bx \pmod{1}$ assuming a and b are relatively-prime. Rudolph [5] used symbolic dynamics to give a new proof without the exactness assumption assuming that a and b are coprime, the ergodicity of the joint action and that one of the maps $x \rightarrow ax \pmod{1}$, $x \rightarrow bx \pmod{1}$, has positive entropy. Two years later Johnson [8] was able to prove Rudolph’s theorem assuming only that a and b are multiplicatively independent i.e. that there are no positive integers u, v such that $a^u = b^v$, instead of requiring coprimality. A different approach was taken by Host in [9] and [10]. Assuming only that m is a -invariant, ergodic and with positive entropy, Host noticed that the desired result would follow for an integer b from the stronger statement that for m -almost every x , the sequence $(b^n x)_{n \geq 1}$ is uniformly distributed modulo 1. In other words, the requirement is that m -almost every x is normal in base q . In effect Host’s work links the problem to that of normality to multiple bases for which there is a large literature. By Weyl’s criterion, for $h \in \mathbb{Z} \setminus \{0\}$ this is equivalent to

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=0}^{N-1} e^{2\pi i h b^n x} = 0,$$

m -almost everywhere, which implies

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=0}^{N-1} T_{b^n} m = \lambda,$$

in the weak* topology. Here λ denotes Lebesgue measure on $\mathbb{T}$. Johnson and Rudolph [11] noticed that this implies

$$\lim_{\substack{n \rightarrow \infty \\ n \in D}} T_{b^n} m = \lambda,$$

on a set D of density 1. Here the measure Tm is defined by $Tm(A) = m(T(A))$ by $A \in \beta$. This condition also implies $m = \lambda$. Thus, in a sense, Furstenberg's conjecture is the weakest among several possible statements. The least restrictive hypotheses under which a version of Rudolph's theorem can be proved appears in [12] where an approach based on 'subexponential cells' and p -adic collision numbers appears. See also [13] for an effective version of the problem. We hope to return to a more detailed analysis of this problem in positive characteristic elsewhere.

2. Proof of Theorem

We begin with some generalities. Suppose (Y, β, m) is a Lebesgue probability space. See p. 55 of [3] for the definition of Lebesgue probability spaces, which are the only probability spaces considered in this paper. Suppose S is a countable to one measure-preserving transformation of (Y, β, m) and that there exists $Z \in \beta$ with $m(Z) = 1$. Suppose that $SZ = Z$ and that S maps measurable sets to measurable sets and null sets to null sets. This enables one to define unambiguously the Radon-Nikodym derivative $S'(x) = \frac{dmS}{dm}(x)$. If T is a second such transformation commuting with S then $(ST)'(x) = S'(T(x))T'(x) = T'(S(x))S'(x)$. We write $f(x) = \log S'(x)$ and $g(x) = \log T'(x)$ and we have

$$f(Tx) - f(x) = g(Sx) - g(x). \quad (*)$$

We say a denumerable partition $\gamma = \{G_i\}_i$ of $\mathbb{L}$ is generating if the σ -algebra generated by $\bigvee_{i=1}^{\infty} T^{-i}\gamma$ is β modulo 0 i.e. the two σ -algebras coincide up to sets of zero. The importance of generating partitions γ is that $h(T) = H(\gamma)$ which greatly simplifies the computation of $h(T)$. See p. 96 of [3]. To $P \in \mathbb{F}[X]$ with $\deg(P) > 1$ we can associate a base P expansion of every $x \in \mathbb{L}$, analogous of the decimal expansion of every point in $[0, 1)$. The digits of the expansion are taken from the finite set $F_P = \{r \in \mathbb{F}_q[X] : \deg(r) < \deg(P)\}$. As with the decimal expansion, off a countable set, the expansion is unique. If for $x \in \mathbb{L}$ the sequence of digits of x is $(x_n)_{n \geq 1}$, with $x_n \in F_P$ for each natural number n . Then one checks readily that if $H_r = \{x \in \mathbb{L} : x_1 = r\}$ for $r \in F_P$ then the collection of sets $\{H_r\}_{r \in F_P}$ is a generating partition for the map $T_P x = \{Px\}$ on $\mathbb{L}$. For partitions γ and η , let

$$I(\gamma|\eta)(x) = - \sum_i \chi_{G_i}(x) (\log m(G_i|\eta))$$

where $m(A|\eta)$ denotes the conditional measure of the set A given the σ -algebra generated by the partition η . Note that for x in $\mathbb{L}$ if the elements of the the partitions γ and η to which x belongs are G and E , then $I(\gamma|\eta)(x) = m(G \cap E)/m(E)$. Evidently I is a non-negative function. In [14] it is shown that $f(x) = \lim_{n \rightarrow \infty} I(\gamma|\bigvee_{i=1}^n T^{-i}\gamma)(x)$. In particular $f(x) \geq 0$ and similarly $g(x) \geq 0$. We define pointwise, the Perron-Frobenius operators by

$$L_{-f}w(x) = \sum_{Sy=x} e^{-f(y)} w(y)$$

and

$$L_{-g}w(x) = \sum_{Ty=x} e^{-g(y)} w(y).$$

In view of the identity (*), we have $L_{-f}L_{-g} = L_{-g}L_{-f}$. These operators map non-negative functions to non-negative functions such that $L_{-f}1 = 1$ and $L_{-g}1 = 1$. Suppose f denotes

the characteristic function of an element of β . Then T being measure preserving can be written $\int_Y f \circ T(x) dm = \int_Y f(x) dm$. Taking linear combinations the same identity holds for simple functions f and by approximation all functions in $L^1(X)$. In particular, T defines a unitary map of $L^2(X)$. Moreover on $L^1(X)$ we have (writing $(Sw)(x) = w(Sx)$, $(Tw)(x) = w(Tx)$) that $SL_{-f} = \mathbb{E}(\cdot | S^{-1}\beta)$ and $TL_{-g} = \mathbb{E}(\cdot | T^{-1}\beta)$. See p. 20 of [15] for the definition and basic properties of the conditional expectation operator $\mathbb{E}(\cdot | \beta)$. Also for a σ -algebra β we use $T^{-1}\beta$ to denote the σ -algebra $\{T^{-1}A : A \in \beta\}$. We also have that $L_{-f}Sw = w$ and $L_{-g}Tw = w$ for any $w \in L^1(Y)$. Finally with respect to the inner product on $L^2(Y)$ it is easy to check that L_{-f} and L_{-g} are the duals of S and T respectively.

LEMMA 1. *Suppose, for almost all x that $T: S^{-1}x \rightarrow S^{-1}Tx$ is bijective. Then $fT = f$ and $gS = g$.*

Proof. Note that $L_{-f}(e^g) = e^g$. This is because

$$\sum_{Sy=x} e^{-f(y)+g(y)} = \sum_{Sy=x} e^{-f(Ty)+g(Sy)} = e^{g(x)} \sum_{Sy=x} e^{-f(Ty)} = e^{g(x)}.$$

Hence $\mathbb{E}(e^g | S^{-1}\beta) = e^{g(S)}$, from which we conclude that $e^{g(S)} = e^g$ and therefore $g \circ S = g$ and $f \circ T = f$ as required.

More detailed information about the properties of the Perron–Frobenius operators may be found in [16].

We now choose $S = T_P$ and $T = T_Q$ on $\mathbb{L}$ and recall that we assume $(P, Q) = 1$. We suppose that S, T preserve a Borel probability measure m on $\mathbb{L}$ with respect to which the action of the semi-group $\{S^m T^n : m, n \in \mathbb{Z}^+\}$ is ergodic but that neither of S nor T are assumed to be ergodic. Note that because $(P, Q) = 1$ it is clear the hypotheses of Lemma 1 are satisfied and so that $f \circ T = f$ and that $g \circ S = g$. To each $x \in \mathbb{L}$ and each $n \in \mathbb{N} \cup \{0\}$ we associate a function $d(x, n)$ defined on the points r/P^n in $\mathbb{L}$ with r, P in $\mathbb{F}_q[X]$. Each element of $S^{-n}S^n(x)$ is of the form $x + r/P^n$. To each $y = r/P^n$ such that $S^n x = S^n y$ the function $d(x, n)$ assigns the value $e^{-f^n(y)}$ where $f^n(y) = \sum_{j=0}^{n-1} f(S^j y)$. One checks easily from the definition of f that $f^n(x) = \log \prod_{i=0}^{n-1} S'(S^i(x))$. From this and the fact that $L_{-f}1 = 1$ we get the elementary identity $e^{-f^{n-1}(y)} = \sum_{Sz=y} e^{-f^n(z)}$. From this it is clear that $d(x, n-1)$ can be expressed in terms of certain $d(\cdot, n)$. In particular if D_n is the smallest σ -algebra with respect to which all of the distributional functions $d(x, 1), \dots, d(x, n)$ are measurable, then $D_1 \subset D_2 \subset \dots \subset D_n$. Furthermore $f + f^{n-1} \circ S = f^n(x)$ so that $S^{-1}D_{n-1} \subset D_n$. Finally we note that $f^n \circ T = f^n$ so that $d(n, x)(r/P^n) = d(n, Tx)(Qr/P^n)$ if for $r \in \mathbb{F}_q[X]$ we have $|r/P^n| \leq 1$. Also $T^{-1}D_n = D_n$.

We digress briefly to consider some arithmetical issues in $\mathbb{F}_q[X]$, which may be well known but a convenient reference to which is unknown to the authors. Given $c \in \mathbb{F}_q[X]$ with $|c| > 1$ let $\mathbb{F}_q[X]/c\mathbb{F}_q[X]$ denote the collection of cosets $r + c\mathbb{F}_q[X]$ with $|r| < |c|$. Because the analogue of Bezout's theorem holds in $\mathbb{F}_q[X]$ if $(s, t) = 1$ then there exist $x, y \in \mathbb{F}_q[X]/c\mathbb{F}_q[X]$ such that $sx + ty = 1$. In particular if $(u, c) = 1$ then there is a unique and well defined solution to the equation $ux \equiv 1 \pmod{c}$ in $\mathbb{F}_q[X]/c\mathbb{F}_q[X]$. Here of course $\equiv$ denotes belonging to the same coset in $\mathbb{F}_q[X]/c\mathbb{F}_q[X]$. We will use $G_{q,c}$ to denote the set of reduced “residue classes” in $\mathbb{F}_q[X]/c\mathbb{F}_q[X]$. Using right cancellation on the multiplicative group $G_{q,c}$, given $d \in G_{q,s}$ we have $\prod_{x \in G_{q,c}} (dx) \equiv \prod_{x \in G_{q,c}} x \pmod{c}$. If we let $\phi_q(c)$ the cardinality of the finite group $G_{q,c}$. We have an analogue of the Fermat–Euler theorem $d^{\phi_q(c)} \equiv 1 \pmod{c}$.

We now return to our primary concern. As $Q^{\phi_q(P^n)} \equiv 1 \pmod{P^n}$ we have

$$d(n, x) \left(\frac{r}{P^n} \right) = d(n, T^{\phi_q(P^n)} x) \left(\frac{r}{P^n} \right)$$

and $T^{-\phi_q(P^n)}B = B$ for all $B \in D_n$. Let $B(c, \rho)$ denote the open ball center c and radius ρ in $\mathbb{L}$ and consider $\gamma = \{B(r, 1/|PQ|)\}_{\{r \in \mathbb{F}[X]: |r| \leq PQ\}}$ – a partition of $\mathbb{L}$. The metric on $\mathbb{L}$ is defined in the introduction. We can find $(r_n)_{n \geq 1}, (s_n)_{n \geq 1} \subset \mathbb{N}$, such that each element of $\bigvee_{i=0}^{r_n} S^{-i}\gamma$ is contained in an absolutely bounded number of elements of $\bigvee_{i=0}^{s_n} T^{-i}\gamma$ and vice versa. We can for instance choose $r_n = n \deg(P)$ and $s_n = n \deg(Q)$. This means that for any sub- σ -algebra η

$$\left| H\left(\bigvee_{i=0}^{r_n} S^{-i}\gamma \mid \bigvee_{i=0}^{s_n} T^{-i}\gamma \vee \eta\right) - H\left(\bigvee_{i=0}^{s_n} T^{-i}\gamma \mid \bigvee_{i=0}^{r_n} S^{-i}\gamma \vee \eta\right) \right|$$

is bounded and therefore

$$\lim_{n \rightarrow \infty} \left(\frac{1}{s_n} H\left(\bigvee_{i=0}^{s_n} T^{-i}\gamma \mid \eta\right) - \left(\frac{\deg(P)}{\deg(Q)}\right) \frac{1}{r_n} H\left(\bigvee_{i=0}^{r_n} S^{-i}\gamma \mid \eta\right) \right) = 0.$$

When $T^{-1}\eta = \eta$ the individual limits exist, which we denote by $h(T|\eta)$ and $h(S|\eta)$, respectively, so we get

LEMMA 2. *We have $h(T|\alpha) = \deg(P)\deg(Q)h(S|\alpha)$.*

We also have from the following lemma.

LEMMA 3. *Let $D = \bigvee_{n=1}^{\infty} D_n$. Then $D \subset \bigcap_{n=0}^{\infty} S^{-n}\beta$.*

Proof. If $\eta = D = \bigvee_{n=1}^{\infty} D_n$ then $T^{-1}D = D$ and

$$h(T|D) = \lim_{n \rightarrow \infty} \frac{1}{s_n} H(\gamma \vee T^{-1}\gamma \vee \dots \vee T^{-s_n+1}\gamma | D),$$

which by the entropy cocycle property, for which see p. 7 of [4], is

$$\begin{aligned} &= \lim_{n \rightarrow \infty} \frac{1}{s_n} (H(T^{-1}\gamma \vee \dots \vee T^{-s_n+1}\gamma | D) + H(\gamma | T^{-1}\gamma \vee \dots \vee T^{-s_n+1}\gamma \vee D)) \\ &= \lim_{n \rightarrow \infty} \frac{1}{s_n} (H(\gamma \vee \dots \vee T^{-s_n+2}\gamma | D) + H(\gamma | \gamma_1^{s_n-1} \vee D)) \\ &\dots\dots\dots \\ &= \lim_{n \rightarrow \infty} \frac{1}{s_n} (H(\gamma) + H(\gamma | T^{-1}\gamma \vee D) + \dots + H(\gamma | \gamma_1^{s_n-1} \vee D)). \end{aligned}$$

By the martingale convergence theorem on p. 5 of [4] this is

$$= H\left(\gamma \mid \bigvee_{i=1}^{\infty} T^{-i}\gamma \vee D\right),$$

and as γ is a generator of β and $D \subseteq \beta$ this is

$$= H(\beta | T^{-1}\beta \vee D) = H(\beta | T^{-1}\beta) = h(T).$$

So by Lemma 2 $h(T) = h(T|D)$. Hence

$$H(D | S^{-1}\beta) = H(\beta \vee D | S^{-1}\beta) - H(\beta | D \vee S^{-1}\beta) \leq h(S) - h(S|D),$$

the inequality arising from

$$\begin{aligned} h(S|D) &= \lim_{n \rightarrow \infty} \frac{1}{n} H(\gamma \vee \dots \vee S^{-n}\gamma | D) \\ &= \lim_{n \rightarrow \infty} \frac{1}{n} \left(H\left(\gamma \mid \bigvee_{i=1}^n S^{-i}\gamma \vee D\right) + H\left(\bigvee_{i=1}^n S^{-i}\gamma \mid D\right) \right) \end{aligned}$$

and using the fact that $S^{-1}D \subset D$ we have

$$\begin{aligned} &\leq \lim_{n \rightarrow \infty} \frac{1}{n} \left(H\left(\gamma \mid \bigvee_{i=1}^n S^{-i}\gamma \vee D\right) + \cdots + H(\gamma \mid D) \right) \\ &= H\left(\gamma \mid \bigvee_{i=1}^n S^{-i}\gamma \vee D\right) = H(\beta \mid S^{-1}\beta \vee D). \end{aligned}$$

Thus we have $H(D \mid S^{-1}\beta) = 0$. This means that, as pointed out on p. 8 of [4], we have $D \subset S^{-1}\beta$. Repeated application gives $D \subset \bigcap_{n=0}^{\infty} S^{-n}\beta$ as required.

Thus for each pair of natural numbers n, N the set $d(x, n)$ is $S^N\beta$ measurable. We say x is symmetric if for each $n > 0$ there exist $y \neq x$, necessarily members of some subgroup G_x^n of $\{r/p^n : |r| \leq |P^n|\}$ such that $d(S^m(x), n) = d(S^m(y), n)$ for each $m \geq 0$. One checks readily that the set of symmetric points is invariant under both S and T . This means that the measure of the set of symmetric points is either null or of full measure. Arguing as in [5] we see that the set of symmetric points is null if and only if both S and T are invertible and of zero entropy. This means that all the groups G_x^n are trivial. Otherwise if almost all x are symmetric there is a non-trivial subgroup G of $\{r/P^n : |r| \leq |P^n|\}$ such that $E = \{x : G_x^1 = G\}$ has positive measure. Assuming the latter case we see that E is T invariant and thus for almost all x we have $T^n x \in E$ finitely often, i.e. $f^n(x) \rightarrow \infty$, since the joint action of S, T is ergodic. Now $|G_x^n| = e^{f^n(x)}$ so that the cardinality of G_x^n tends to infinity almost surely.

Following [17, p. 326–330], for $\xi \in \mathbb{F}_q((X^{-1}))$ and $C \in \mathbb{F}_q[X]$ define $e_C(\xi)$ as follows. Let c_{-1} denote the coefficient of X^{-1} in the Laurent expansion of ξ . Let $\omega_1, \dots, \omega_k$ be a fixed basis for the expansion of $\mathbb{F}_q$ over $\mathbb{F}_p$. Then $c_{-1} = b_1\omega_1 + \cdots + b_k\omega_k$ with $b_j \in \mathbb{F}_p$ for $1 \leq j \leq k$. We define $e(\xi) = e^{2\pi i b_1/p}$ and set $e_C(\xi) = e(C\xi)$.

For each $C \in \mathbb{F}_q[X] \setminus \{0\}$ we have

$$\mathbb{E}(e_C(\xi) \mid S^{-n}\beta)(x) = \frac{\sum_{g \in G_x^n} e_C(x+g)}{|G_x^n|} = 0$$

when $f^n(x)$ is large enough, from which we conclude $\int_{\mathbb{L}} e_C(\xi) dm = 0$. Thus, when $h(S) > 0$ then m must be Haar measure. We have therefore proved our result.

Bibliography

- [1] B. Г. Спринджук, *Проблема Малера в метрической теории чисел*, Наука и техника, Минск, 1967; V. G. Sprindžuk, *Mahler's Problem in Metric Number Theory*, Transl. Math. Monogr., **25**, Amer. Math. Soc., Providence, RI, 1969.
- [2] M. H. Taibleson, *Fourier Analysis on Local Fields*, Mathematical Notes, **15**, Princeton Univ. Press, Princeton, NJ, 1975.
- [3] P. Walters, *An Introduction to Ergodic Theory*, Grad. Texts in Math., **79**, Springer-Verlag, Berlin, 1982.
- [4] W. Parry, *Entropy and Generators in Ergodic Theory*, W. A. Benjamin, New York, 1969.
- [5] D. J. Rudolph, “ $\times 2$ and $\times 3$ invariant measures and entropy”, *Ergodic Theory Dynam. Systems*, **10:2** (1990), 395–406.
- [6] W. Parry, “Squaring and cubing the circle – Rudolph’s theorem”, *Ergodic Theory of $\mathbf{Z}^d$ Actions*, London Math. Soc. Lecture Note Ser., **228**, Cambridge Univ. Press, Cambridge, 1996, 177–183.
- [7] H. Fürstenberg, “Disjointness in ergodic theory, minimal sets, and a problem in diophantine approximation”, *Math. Systems Theory*, **1:1** (1967), 1–49.
- [8] A. S. A. Johnson, “Measures on the circle invariant under multiplication by a nonlacunary subsemigroup of the integers”, *Israel J. Math.*, **77:1-2** (1992), 211–240.

- [9] B. Host, “Nombres normaux, entropie, translations”, *Israel J. Math.*, **91**:1-3 (1995), 419–428.
- [10] B. Host, “Some results of uniform distribution in the multidimensional torus”, *Ergodic Theory Dynam. Systems*, **20**:2 (2000), 439–452.
- [11] A. Johnson, D. J. Rudolph, “Convergence under $\times_q$ of $\times_p$ invariant measures on the circle”, *Adv. Math.*, **115**:1 (1995), 117–140.
- [12] E. Lindenstrauss, “ p -adic foliations and equidistribution”, *Israel J. Math.*, **122**:1 (2001), 29–42.
- [13] J. Bourgain, E. Lindenstrauss, P. Michel, A. Venkatesh, “Some effective results for $\times_a \times_b$ ”, *Ergodic Theory Dynam. Systems*, **29**:6 (2009), 1705–1722.
- [14] W. Parry, “On Rohlin’s formula for entropy”, *Acta Math. Acad. Sci. Hungar.*, **15**:1-2 (1964), 107–113.
- [15] W. Parry, *Topics in Ergodic Theory*, Cambridge Tracts in Math., **75**, Cambridge Univ. Press, Cambridge, 1981.
- [16] W. Parry, M. Pollicott, *Zeta Functions and the Periodic Orbit Structure of Hyperbolic Dynamics*, Astérisque, **187–188**, Soc. Math. France, Paris, 1990.
- [17] L. Kuipers, H. Niederreiter, *Uniform Distribution of Sequences*, Pure Appl. Math., John Wiley & Sons, New York, 1974.