AN UNCOUNTABLE FAMILY OF GROUP AUTOMORPHISMS, AND A TYPICAL MEMBER

Thomas Ward

November 1996

To appear, Bulletin London Math. Society

Abstract. We describe an uncountable family of compact group automorphisms with entropy $\log 2$. Each member of the family has a distinct dynamical zeta function, and the members are parametrised by a probability space. A positive proportion of the members have positive upper growth rate of periodic points, and almost all of them have an irrational dynamical zeta function.

If infinitely many Mersenne numbers have a bounded number of prime divisors, then a typical member of the family has upper growth rate of periodic points equal to $\log 2$, and lower growth rate equal to zero.

1. Introduction

If $\alpha : X \to X$ is an automorphism of a compact abelian group, then α is ergodic if and only if α is measurably isomorphic to a Bernoulli shift by [.lind structure skew.]. It follows that the equivalence relation of measurable isomorphism on the set of compact group automorphisms with prescribed entropy is trivial. In this note we show that the equivalence relation of topological conjugacy on the set of compact group automorphisms with entropy $\log 2$ has uncountably many equivalence classes, and that uncountably many of these classes are distinguished by the dynamical zeta function. The examples constructed are parametrized by elements of $\Omega = \{0,1\}^{\mathbb{N}}$ ($\mathbb{N} = \{1,2,\dots\}$), which is naturally thought of as the probability space for a repeated fair coin–toss. Some properties of a typical example are shown.

Let $P = \{p_0 = 2, p_1 = 3, \dots\}$ denote the primes, and let S be any subset of P containing 2. The sets S are in one–to–one correspondence with elements of Ω: let $\omega_S(k) = 1$ if $p_k \in S$ and 0 otherwise, and send S to the point $\omega_S \in \Omega$. If Ω is given the product $(\frac{1}{2}, \frac{1}{2})$–measure μ, then $\{S \mid \{2\} \subset S \subset P\}$ inherits the structure of a probability space. For a rational r, let $\operatorname{ord}_p(r)$ denote the signed multiplicity with

1991 *Mathematics Subject Classification.* 22D40, 58F20.

The author gratefully acknowledges support from NSF grant DMS-94-01093 at the Ohio State University

which the prime p divides r, and set $|r|_p = p^{-\mathrm{ord}_p(r)}$. Each set S defines a ring of S–integers,

$$R_S = \{x \in \mathbb{Q} \mid |x|_p \le 1 \text{ for all } p \notin S\}.$$

Define a map $\alpha_S : X_S \to X_S$ as follows: the compact abelian group X_S is the dual (character) group of the additive group R_S; the automorphism α_S is the dual of the automorphism $r \mapsto 2r$ of R_S. Dynamical systems of this form have been extensively studied (see [.chothi everest ward periodic.] and [.chothi thesis.]). In order to make this note self–contained, simple versions of two results from [.chothi everest ward periodic.] are included.

The number of periodic points of α_S is given by

$$\mathrm{Fix}_n(\alpha_S) = |2^n - 1| \times \prod_{p \in S} |2^n - 1|_p \le |2^n - 1| \tag{1}$$

(this follows from a more general result in [.chothi everest ward periodic.], Section 6 and [.chothi thesis.]; a direct proof is given below in the Appendix). The dynamical zeta function associated with α_S, defined by

$$\zeta_{\alpha_S}(z) = \exp \sum_{n=1}^{\infty} \frac{z^n}{n} \mathrm{Fix}_n(\alpha_S),$$

is therefore convergent in $\{z \in \mathbb{C} \mid |z| < \frac{1}{2}\}$. The upper and lower growth rates of periodic points are

$$p^+(\alpha_S) = \limsup_{n\to\infty} \frac{1}{n} \log \mathrm{Fix}_n(\alpha_S); \quad p^-(\alpha_S) = \liminf_{n\to\infty} \frac{1}{n} \log \mathrm{Fix}_n(\alpha_S).$$

The entropy of α_S is $\log 2$ for any S (see [.lind ward p-adic.]).

Denote by λ_n the normalised Haar measure on the (finite) subgroup of points with period n; $\{\lambda_n\}$ is the set of periodic point measures. The periodic points are said to be uniformly distributed with respect to Haar measure along the sequence (n_j) if λ_{n_j} converges weak* to Haar measure λ on X_S.

Theorem. *The uncountable family $\{\alpha_S\}$ of compact group automorphisms has the following properties.*

(a) *If $S \ne T$ then $\zeta_{\alpha_S} \ne \zeta_{\alpha_T}$.*
(b) *The function ζ_{α_S} is almost surely irrational.*
(c) *Each α_S is isomorphic to a Bernoulli shift.*
(d) *With probability greater than zero, $p^+(\alpha_S) > 0$ and Haar measure is in the closure of the periodic point measures.*

Corollary. *There exist examples with S infinite and with $p^+(\alpha_S) > 0$. There exist examples with irrational dynamical zeta function.*

Such examples are of interest because the local behaviour of α_S is hyperbolic in two directions (corresponding to the valuations $|\cdot|$ and $|\cdot|_2$) and isometric in all the directions corresponding to elements of S. It follows that an example with S infinite is far from expansive; on the other hand having a positive upper growth rate of periodic points is typically associated with expansive or hyperbolic behaviour. Also, it is not straightforward to exhibit such examples: in [.chothi everest ward periodic.] and [.chothi thesis.] Heath–Brown's work on the Artin conjecture is used to show there is an infinite S for which the map dual to multiplication by 2 or 3 or 5 must have $p^+ > 0$, and the Hadamard Quotient Theorem is used to give explicit examples of irrational zeta functions. The situation is analogous to the difference between showing there must be some transcendental numbers and the difficulty involved in exhibiting one.

Conditional Theorem. *Conditional on the indicated conjectures, the family* $\{\alpha_S\}$ *has the following properties.*

- (e) *If infinitely many Mersenne numbers are prime powers, then almost surely* $p^+(\alpha_S) = \log 2$, $p^-(\alpha_S) = 0$ *and the closure of the periodic point measures contains Haar measure and the point mass at the identity.*
- (f) *If infinitely many Mersenne numbers have a bounded number of prime divisors, then almost surely* $p^+(\alpha_S) = \log 2$, $p^-(\alpha_S) = 0$ *and the closure of the periodic point measures contains Haar measure.*

Proofs

(a) It is enough to show that the set S can be reconstructed from the function ζ_{α_S}. For an odd prime p, let $n = n(p)$ be the smallest natural number for which p divides $2^n - 1$. Then by equation (1),

$$\mathrm{ord}_p\left(\mathrm{Fix}_n(\alpha_S)\right) = \begin{cases} 0 & \text{if } p \in S; \\ \mathrm{ord}_p(2^n - 1) > 0 & \text{if } p \notin S. \end{cases}$$

It follows that the coefficients of ζ_{α_S} determine the elements of S.

(b) By Theorem 2(a) of [.bowen lanford restrictions.], there are only countably many rational dynamical zeta functions, so by (a) almost all of them must be irrational.

(c) It is clear that each α_S is ergodic (see Section 5 of [.chothi everest ward periodic.]), so this follows from [.lind structure.]. For these simple dynamical systems one may however see this directly. Let η denote the partition of the additive circle $\mathbb{T} = [0,1)/0 \sim 1$ into the two sets $[0, \frac{1}{2})$,$[\frac{1}{2}, 1)$. Dual to the inclusion $\mathbb{Z} \hookrightarrow R_S$ is a surjective homomorphism $\pi : X_S \to \mathbb{T}$. Let $S = \{q_1, q_2, \dots\}$ (if S has $\ell < \infty$ elements define q_k to be 1 for all $k > \ell$), and define for each $r \in \mathbb{N}$ a partition ξ_r of X_S by $\xi_r = f_r \pi^{-1}(\eta)$, where f_r is the map dual to multiplication by $q_1^r \dots q_r^r$ on R_S. Now $\pi^{-1}(\eta)$ is a Bernoulli factor of α_S, so for each r so is ξ_r. On the other hand, as a set X_S is given by $\mathbb{T} \times \prod_{p \in S} \mathbb{Z}_p$ (see [.chothi everest ward periodic.], Section 3 for the details). Under this correspondence the product of the partitions into intervals of length 2^{-m} on $\mathbb{T}$ and into discs determined by the first r p-adic digits of the first r factors in $\prod_{p\in S}\mathbb{Z}_p$ is measurable with respect to the σ–algebra generated by $\bigvee_{|k|\le m}\alpha_S^k\xi_r$. It follows that the σ–algebra generated by ξ_r under α_S increases as $r\to\infty$ to the whole Borel σ–algebra. Since each factor is Bernoulli, the monotone theorem (Theorem 2 in [.ornstein bernoulli infinite.]) shows that α_S is isomorphic to a Bernoulli shift.

This direct argument for the Bernoullicity of automorphisms of one–dimensional solenoids comes from Wilson [.wilson endomorphisms solenoid.]. Notice that if $S=\{2\}$ the corresponding α_S is the natural invertible extension of the circle doubling map, and is finitarily isomorphic to the Bernoulli $(\frac{1}{2},\frac{1}{2})$–shift.

(d) First notice that the set $\{\omega_S \mid p^+(\alpha_S)=0\}$ is measurable. Write $F_n(S)=\frac{1}{n}\log \mathrm{Fix}_n(\alpha_S)$; from the formula (1) this is a continuous (locally constant) function of S: a set T is close to S if the same members of the first M primes are in S and T for some large M, and continuity follows since for fixed n the quantity 2^n-1 can only be divisible by finitely many primes. Then the set in question is

$$\{\omega_S \mid p^+(\alpha_S)=0\}=\bigcap_{N\in\mathbb{N}}\bigcap_{k\in\mathbb{N}}\bigcup_{n>k}\{\omega_S \mid F_n(S)<\tfrac{1}{N}\}.$$

Assume that $p^+(\alpha_S)=0$ for almost every S. Then we have, for those S

$$\lim_{n\to\infty}\frac{1}{n}\log \mathrm{Fix}_n(\alpha_S)=0, \tag{2}$$

so by (1)

$$\lim_{n\to\infty}\frac{1}{n}\log\prod_{p\in S}|2^n-1|_p=-\log 2. \tag{3}$$

Now by the Artin–Whaples formula, if S^c comprises all odd primes not in S together with 2, then

$$\prod_{p\in S^c}|2^n-1|_p\times\prod_{p\in S}|2^n-1|_p=\frac{|2^n-1|_2}{|2^n-1|}=\frac{1}{|2^n-1|}.$$

Equation (3) therefore implies that

$$\lim_{n\to\infty}\frac{1}{n}\log\prod_{p\in S^c}|2^n-1|_p=0,$$

so that $p^+(\alpha_{S^c})=p^-(\alpha_{S^c})=\log 2$ almost surely (since the map $\omega_S\mapsto\omega_{S^c}$ is an invertible μ–preserving transformation of Ω). It follows that p^+ cannot be zero on a set of full measure.

Notice that this argument also shows that if $p^+(\alpha_S)=0$ on a set of positive measure, then there is (another) set of positive measure with $p^+(\alpha_S)=p^-(\alpha_S)$, lending support to the natural conjecture that $p^+(\alpha_S)>0$ almost surely.

We claim that $p^+(\alpha_S) > 0$ implies that Haar measure lies in the weak*–closure of $\{\lambda_n\}$. To see this, let (n_j) be a sequence for which

$$\mathrm{Fix}_{n_j}(\alpha_S) = |R_S/(2^{n_j}-1)R_S| \to \infty \quad \text{as} \quad j \to \infty,$$

and assume that λ_{n_j} does not converge to λ. Then $\widehat{\lambda_{n_j}}$ does not converge pointwise to $\widehat{\lambda}$, and since $\widehat{\lambda}(r) = 0$ for all $r \in R_S \backslash \{0\}$, this requires that there is an element $r \in R_S \backslash \{0\}$ with $\widehat{\lambda_{n_j}}(r) \neq 0$ for infinitely many values of j. This requires that

$$r \in (2^{n_j} - 1)\, R_S$$

for infinitely many j. It follows that

$$|R_S/(2^{n_j}-1)R_S| \leq |R_S/r \cdot R_S| < \infty$$

for infinitely many j, which contradicts the choice of sequence (n_j). (This proof follows that of [.chothi everest ward periodic.], Section 8).

(e) Let $q_1, q_2, \ldots$ be an increasing sequence with the property that $2^{q_j} - 1 = Q_j^{k(j)}$ is a prime power for all j. Then with probability one S contains infinitely many of the Q_j's. Along the corresponding sequence of q_j's the number of periodic points is one, so the corresponding periodic point measure is always the point mass at the identity and the lower growth rate is zero.

On the other hand, with probability one there is an infinite sequence of Q_j's not in S, and the growth rate along the corresponding sequence of q_j's is $\log 2$. As in (d) above, it follows that Haar measure is in the weak*–closure of the set of periodic point measures.

(f) Let $n_1, n_2, \ldots$ be a sequence with the property that $n_j \to \infty$ as $j \to \infty$ and there are exactly L primes dividing $2^{n_j} - 1$ for all j. Let $P(n_j) = \{p_1^{(j)}, \ldots, p_L^{(j)}\}$ be the set of primes dividing $2^{n_j} - 1$. Notice by Zsigmondy's theorem [.zsigmondy potenzreste.] that for each j there is a prime in $P(n_j) \backslash \bigcup_{\ell<j} P(n_\ell)$. Let

$$S_0 = \{p \mid p \in P(n_j) \text{ for infinitely many } j\}.$$

Then $|S_0| < L$ ($|S_0|$ cannot be equal to L since, for example, the greatest prime divisor of $2^n - 1$ is greater than or equal to $2n+1$ for $n \geq 12$ by [.schinzel primitive prime factors.]). Let $P'(n_j) = P(n_j) \backslash S_0$. Pick a subsequence $(n_{j(k)})$ as follows. Set $j(1) = 1$, and inductively choose $j(k+1)$ to have the property that

$$P'(n_{j(k+1)}) \cap \bigcup_{\ell \leq k} P'(n_{j(\ell)}) = \emptyset. \tag{4}$$

This is possible since the set S_0 has been removed. Notice that

$$L - |S_0| \leq |P'(n_{j(k)})| \leq L \tag{5}$$

for each k. Now consider sets

$$A_k = \{\omega_S \mid \omega_S(r) = 1 \text{ if } p_r \in P'(n_{j(k)})\},$$

where $p_1, p_2, \dots$ are the odd prime numbers. By (4), the sets $\{A_k\}$ are independent, and by (5)

$$2^{-L} \le \mu(A_k) \le 2^{-(L-|S_0|)}$$

for all k (recall that μ is the $(\frac{1}{2}, \frac{1}{2})$ measure on the space Ω). By the Borel–Cantelli lemma, it follows that

$$\mu\left(\bigcap_{n=1}^{\infty}\bigcup_{k=n}^{\infty} A_k\right) = 1,$$

so for every $S \in \Omega_t$ (Ω_t a set of full measure) we may pick a further subsequence $r_v = n_{j(k_v)}$ with the properties that $r_v \to \infty$ as $v \to \infty$, and $S \supset P'(r_v)$ for all v.

The same argument applied to the sets

$$B_k = \{\omega_S \mid \omega_S(r) = 0 \text{ if } p_r \in P'(n_{j(k)})\}$$

shows that for every $S \in \Omega_r$ (Ω_r a set of full measure) we may pick a sequence t_v with the properties that $t_v \to \infty$ as $v \to \infty$, and $p \notin S$ whenever $p \in P'(t_v)$ for all v.

Let S be a set in $\Omega_r \cap \Omega_t$, and write

$$I(n) = |2^n - 1|, \quad J(n) = \prod_{p \in S_0 \cap S} |2^n - 1|_p, \text{ and } K(n) = \prod_{p \in S \setminus S_0} |2^n - 1|_p.$$

Then

$$\mathrm{Fix}_n(\alpha_S) = I(n) \times J(n) \times K(n).$$

A simple argument using the p–adic logarithm shows that

$$\frac{1}{n} \ll |2^n - 1|_p \le 1$$

for every rational prime p (see Appendix). It follows that for any fixed finite set T of primes,

$$|2^n - 1| \times \prod_{p \in T} |2^n - 1|_p \gg \frac{2^n}{n^a}$$

for some constant a, so

$$\lim_{n\to\infty} \frac{1}{n} \log J(n) = 0.$$

It is clear that

$$\lim_{n\to\infty} \frac{1}{n} \log I(n) = \log 2.$$

Now along the sequence (r_v), primes appearing in $P'(r_v)$ are cancelled, but we might not cancel out from $2^{r_v}-1$ primes appearing in S_0, so

$$1 \le I(r_v) \times J(r_v) \times K(r_v) = \left(\prod_{p \in S_0 \setminus S} |2^{r_v} - 1|_p \right)^{-1} \le \frac{1}{J(r_v)}.$$

Along the sequence (t_v) we can only cancel primes appearing in S_0, so

$$|2^{t_v}-1| \times J(t_v) \le I(t_v) \times J(t_v) \times K(t_v) = |2^{t-v}-1| \times \left(\prod_{p \in S_0 \cap S} |2^{t_v} - 1|_p \right) \le |2^{t_v}-1|.$$

It follows that

$$\lim_{v \to \infty} \frac{1}{r_v} \log \mathrm{Fix}_{r_v}(\alpha_S) = 0$$

and

$$\lim_{v \to \infty} \frac{1}{t_v} \log \mathrm{Fix}_{t_v}(\alpha_S) = \log 2.$$

That is, $p^+(\alpha_S) = \log 2$ and $p^-(\alpha_S) = 0$ almost surely.

The distribution of periodic point measures follows by the argument used in (e) above.

Appendix

Periodic points. *The number of periodic points of α_S is given by*

$$\mathrm{Fix}_n(\alpha_S) = |2^n - 1| \times \prod_{p \in S} |2^n - 1|_p.$$

Proof. First notice that the set $F_n = \{x \in X_S \mid \alpha_S^n(x) = x\}$ is a closed subgroup of X_S. By standard character theory, it follows that there is an isomorphism between the dual group of F_n and the quotient $R_S/F_n^\perp$, where $F_n^\perp$ is the subgroup of characters on X_S that are trivial on F_n. From the definition of F_n, we have that

$$F_n^\perp = (2^n - 1) \cdot R_S.$$

Moreover, if G is any finite abelian group, the dual group of G has the same number of elements as G. It follows that

$$\mathrm{Fix}_n(\alpha_S) = |R_S/(2^n-1)R_S|$$

if the right–hand side is finite.

Fix n and let $m = 2^n - 1$, and $S = \{q_1, q_2, \dots\}$. Since $\mathbb{Z} \subset R_S$, the set $\{0, 1, 2, \dots, m-1\}$ is a complete set of coset representatives for mR_S in R_S. It follows that $|R_S/mR_S| \le m$.

Now consider the first prime q_1. Write $m = q_1^{e_1} d_1$ (with e_1 maximal, $d_1 \in \mathbb{N}$). Since $m \cdot q_1^{-e_1} = d_1 \in R_S$, the cosets $a + mR_S$ and $b + mR_S$ are equal if d_1 divides $(a-b)$. So a complete set of coset representatives is given by $\{0, 1, 2, \dots, d_1 - 1\}$. It follows that $|R_S/mR_S| \le m \times |m|_{q_1} = d_1$.

Continue with the next prime: write $d_1 = q_2^{e_2} d_2$ (with e_2 maximal, $d_2 \in \mathbb{N}$). Since $m \cdot q_2^{-e_2} \cdot q_1^{-e_1} = d_2 \in R_S$, the cosets $a + mR_S$ and $b + mR_S$ are equal if d_2 divides $(a-b)$. So a complete set of coset representatives is given by $\{0, 1, 2, \dots, d_2 - 1\}$. It follows that $|R_S/mR_S| \le m \times |m|_{q_1} \times |m|_{q_2} = d_2$.

This continues for the finitely many primes in S that divide m, showing that $|R_S/mR_S| \le m \times \prod_{p \in S} |m|_p$. On the other hand, the remaining coset representatives $\{0, 1, \dots, d_s - 1\}$ say, all determine distinct cosets since their differences do not lie in mR_S. □

This calculation also follows from a more general result in [.chothi everest ward periodic points.], where an adelic covering space is used to calculate the periodic points.

The next result is used in (f) above, and appears in [.chothi everest ward periodic points.]. Write $A \ll B$ to mean there is a constant $C > 0$ for which $A \cdot C < B$.

Logarithm estimate. *There is a bound from below on the p–adic size of $2^n - 1$ of the form $\frac{1}{n} \ll |2^n - 1|_p \le 1$.*

Proof. The upper bound is clear. Assume that $p > 2$ and that $|2^n - 1|_p < 1$. Use the Euclidean algorithm to write $n = s(p-1) + r$ with $0 \le r < p - 1$. Let Ω_ν denote the smallest field which contains $\mathbb{Q}$ and is both algebraically closed and complete with respect to the valuation $|\cdot|_\nu$ extending $|\cdot|_p$. The ν–adic logarithm is defined for all $x \in \Omega_\nu$ with $|x|_\nu < 1$ by

$$\log_\nu(x+1) = \sum_{j=1}^{\infty} \frac{(-1)^{j+1} x^j}{j}.$$

It follows that

$$\log_\nu(2^n) = (2^n - 1) - \frac{(2^n-1)^2}{2} + \frac{(2^n-1)^3}{3} - \dots$$

so $|\log_p(2^n)|_p = |2^n - 1|_p$. Now

$$\begin{aligned} |2^n - 1|_p &= |\log_p\left(2^{(s(p-1)+r)}\right)|_\nu \\ &= |(s(p-1)+r)\log_p(2)|_\nu \\ &= |s + \tfrac{r}{p-1}|_p \cdot C, \end{aligned}$$

where $C = |\log_p(2)|_p > 0$. Expand s p–adically to obtain

$$s = a_0 + a_1 p + a_2 p^2 + \dots + a_m p^m,$$

where each $a_i \in \mathbb{F}_p$ and $a_m \ne 0$. Now $p^m \le s < p^{m+1}$, so

$$\frac{C}{n} \le \frac{C}{s} \le \frac{C}{p^m} \le |s + \tfrac{r}{p-1}|_p \cdot C = |2^n - 1|_p,$$

which is the required estimate. □

Problems

There is a large gap between (d) and the conjectural (e), (f) above: what is the true typical behaviour? It is shown in [.chothi everest ward periodic.] and [.chothi thesis.] by different methods that "standard" conjectures in number theory imply the existence of infinite sets S with $p^{+}(\alpha_S) = p^{-}(\alpha_S) = \log 2$. For the hypothesis of (f), all that seems to be known is that a recurrence sequence with a bounded number of prime divisors for ALL n can have only finitely many distinct primes dividing any term of the sequence, and must therefore be highly degenerate (see [.methfessel.]). Does the dynamical zeta function have poles dense in the interval $[\frac{1}{2}, 1]$ almost surely? Are any of the maps α_S finitarily equivalent to $\alpha_\emptyset$?

.[]

References

School of Mathematics, University of East Anglia, Norwich NR4 7TJ, U.K.