HOUSTON JOURNAL OF MATHEMATICS

Volume 25, No. 4, 1999

ON EXPANDING ENDOMORPHISMS OF THE CIRCLE II

R. COWEN AND P.H. FISHER
Communicated by the editors

ABSTRACT. In this paper we give sufficient conditions for weak isomorphism of Lebesgue measure-preserving expanding endomorphisms of S^1.

1. Introduction

In [2] the first author gave necessary and sufficient conditions for two real analytic Lebesgue measure-preserving expanding endomorphisms of the circle to be isomorphic upto a phase factor. This was a partial answer to the problem of finding complete measure theoretic invariants for isomorphisms posed by Shub and Sullivan in [5]. In this paper it is shown that the condition given in [2] is sufficient for weak-isomorphism.

For $i = 1, 2$ let f_i be endomorphisms of the Lebesgue spaces $(X_i, \mathcal{B}_i, \mu_i)$. We say that the two systems $(X_1, \mathcal{B}_1, \mu_1, f_1)$ and $(X_2, \mathcal{B}_2, \mu_2, f_2)$ are *isomorphic* if there are sets of measure zero $A_1 \subset X_1, A_2 \subset X_2$ and a one-to-one onto map $\phi : X_1 \setminus A_1 \to X_2 \setminus A_2$ such that $\phi f_1 = f_2 \phi$ on $X_1 \setminus A_1$ and $\mu_1(\phi^{-1}E) = \mu_2(E)$ for all measurable $E \subset X_2 \setminus A_2$. The classification problem in ergodic theory is to determine when two given endomorphisms are isomorphic. As usual in measure theory, we do not distinguish between functions which coincide almost everywhere.

Let $1 \leq r \leq \omega$ and $f : S^1 \to S^1$ be a C^r Lebesgue measure-preserving endomorphism. Then if Df denotes the derivative of f we say that f is *expanding* if there exists $\lambda \in R$ such that $|Df(z)| > \lambda > 1$ for all $z \in S^1$.

Countable-to-one positively measurable non-singular maps have Jacobian derivatives (see [3,4,6] for details) which we denote by $|D|$. For C^1 Lebesgue measure-preserving endomorphisms the Jacobian derivative is simply the absolute value of the derivative of the endomorphism. We say that the Jacobian derivatives $|Df|$ and $|Dg|$ are *isomorphic* if there is a Lebesgue measure-preserving automorphism ϕ of S^1 such that $|Df| = |Dg|\phi$. If ϕ is a Lebesgue measure-preserving automorphism of S^1 then $|D\phi| = 1$. Therefore, if ϕ is an isomorphism between f and g, we have by the chain rule that $|Df| = |Dg|\phi$ and so the Jacobians will be isomorphic. When our endomorphisms are real analytic and expanding, the following theorem of Shub and Sullivan shows that this invariant is nearly complete.

Theorem 1 (cf. [5])**.** *Let f and g be real analytic expanding endomorphisms of S^1 which preserve Lebesgue measure. Suppose that the Jacobian derivatives of f and g are isomorphic; then there are isometries R_1 and R_2 of S^1 such that $R_1^{-1}gR_1 = R_2 f$.*

2. The phase group

In [2] the first author introduced a certain group that can be associated with a continuous surjection $f : S^1 \to S^1$. More precisely, for such an f, let

$G_f = \{\alpha \in S^1 : \exists\ \beta \in S^1 \text{ such that } f(\alpha z) = \beta f(z)\ \forall z \in S^1\}$;

then G_f is a group, where the multiplication of group elements is given by normal multiplication of complex numbers. We call G_f a *phase group*; G_f is never empty since $1 \in G_f$ and as G_f is a closed subgroup of S^1 it is either all of S^1 or the pth roots of unity for some integer $p \geq 1$.

Examples were given of real analytic expanding Lebesgue measure-preserving endomorphisms of the circle with degree d whose phase group has order m for any integers $d \geq 2$ and $m \geq 1$. The following two lemmas were also proved:

Lemma 1 (cf. [2])**.** *If $f : S^1 \to S^1$ is a continuous surjection with degree d then $f(z) = cz^d$ for some constant $c \in S^1$ if and only if $G_f = S^1$.*

Lemma 2 (cf. [2])**.** *Suppose that $f : S^1 \to S^1$ is a continuous surjection with degree d; then if $\alpha \in G_f$, we have that $f(\alpha z) = \alpha^d f(z)$ for all $z \in S^1$.*

Let f^n denote the n-fold composition of f. The main result of [2] was to give complete measure theoretic invariants for f and αg to be isomorphic, where (in the non-trivial case) α is an element of the finite group G_g :

Theorem 2 (cf. [2])**.** *Let f, g be real analytic Lebesgue measure-preserving expanding endomorphisms of S^1 with the same degree. Then there exists an $\alpha \in G_g$*

such that f is isomorphic αg, if and only if there exists a Lebesgue measure-preserving automorphism $\phi of S^1$ such that $|Df|(z) = |Dg|(\phi(z))$ and $|Df^2|(z) = |Dg^2|(\phi(z))$.

In [5] it was shown that this isomorphism is an isometry. We say that f and g are *weakly isomorphic* if there exists $n \in N$ such that f^n and g^n are isomorphic. In this paper we show that the condition of Theorem 2 is sufficient for weak-isomorphism:

Theorem 3. *Let f, g be real analytic Lebesgue measure-preserving expanding endomorphisms of S^1 with the same degree. If there exists a Lebesgue measure-preserving automorphism ϕ, of S^1 such that $|Df|(z) = |Dg|(\phi(z))$ and $|Df^2|(z) = |Dg^2|(\phi(z))$ then f and g are weakly isomorphic.*

To investigate examples of endomorphisms that satisfy the hypothesis of Theorem 3, but are not isomorphic, one needs to look at functional equations formed by m-fold covers of the restriction to the circle of certain Blaschke products. This will be contained in a forthcoming paper.

3. Some Number Theory

The proof of Theorem 3 relies on a sequence of mostly number theoretic lemmas. In what follows, unless otherwise stated, we let m and d be positive integers where $m > 1$ and $d > 2$. We denote the greatest common divisor of two integers, a and b by (a, b). Let $(m, d-1) = e$.

Lemma 3. *There exist integers $x \geq 1$ and $k \geq 0$ such that $e^k x \equiv 0 (mod m)$, where $(x, d-1) = 1$.*

Proof. If $(m, d-1) = 1$, set $k = 0$ and $m = x$. Otherwise let $m = ex_1$ and consider $(x_1, d-1)$. If $(x_1, d-1) = 1$, set $k = 1$ and $x_1 = x$. Otherwise $(x_1, d-1) = e_1$ and let $x_1 = e_1 x_2$. Repeating the above, since m is finite, the process eventually terminates in k steps.
Then $(x_k, d-1) = 1$ and $m = ee_1e_2 \dots e_{k-1}x_k$. Now since for $1 \leq i \leq k-1$, $m \equiv 0(\text{mod } e_i)$, $d-1 \equiv 0(\text{mod } e_i)$ and $(m, d-1) = e$ we have $e \equiv 0(\text{mod } e_i)$. Hence $e^k \equiv 0 \ (\text{mod } ee_1 \dots e_{k-1})$ where $x_{k-1} = x$. □

Lemma 4. *If $(x, d-1) = 1$, then for any integer $l \geq 1$, there exists an integer s such that $(s(d-1) + l) \equiv 0 (mod x)$.*

Proof. Since $(x, d-1) = 1$, we can find integers u and v with $ux + v(d-1) = 1$. Multiplying through by l we have $lux + lv(d-1) = l$. Hence $-lv(d-1) + l \equiv 0(\text{mod } x)$ and we can set $s = -lv$. □

We will need the following well known result:

Lemma 5. *Let $n \geq 2$ and $1 \leq r < n$ then* ${}^1C_r +^2 C_r + \ldots +^{n-1} C_r = \ {}^nC_{r+1}$.

Since $(m, d-1) = e$, there exists an integer y with $d = ey+1$. We next consider the sum $1 + d + d^2 + \ldots + d^n$ with $d = ey + 1$ and $n = e^k - 1$ for some integer $k \geq 1$.

Lemma 6. *In the expansion of* $1 + (ey + 1) + (ey + 1)^2 + \ldots + (ey + 1)^{e^k-1}$, *for* $1 \leq r < k$, *the coefficient of* $(ey)^r$ *is* ${}^{e^k}C_{r+1}$.

Proof. $1 + (ey + 1) + (ey + 1)^2 + \ldots + (ey + 1)^{e^{k-1}} =$

$$1 + \sum_{r=0}^{1} {}^1C_r(ey)^r + \sum_{r=0}^{2} {}^2C_r(ey)^r + \ldots + \sum_{r=0}^{e^k-1} {}^{e^k-1}C_r(ey)^r.$$

Thus the coefficient of $(ey)^r$ is ${}^1C_r +^2 C_r + \ldots +^{e^k-1} C_r$ which by Lemma 5 is equal to ${}^{e^k}C_{r+1}$. $\square$

Lemma 7 (cf.[1])**.** *Let $r + 1$ be a positive integer and p be a prime, then the exponent of the highest power of p that divides $(r + 1)!$ is*

$$\sum_{i=1}^{\infty} \left[\frac{r+1}{p^i}\right]$$

where the series is finite since $\left[\frac{r+1}{p^i}\right] = 0$ *for* $p^i r + 1$. *(here [ ] is the usual greatest integer function).*

Proposition 1. *Given $m > 1$ and $d > 2$ are positive integers there exists integers s and $n \geq 0$ such that for any l with $1 \leq l < m$,* $(s(d-1)+l)(1+d+\ldots+d^n) \equiv 0(mod m)$.

Proof. From Lemma 3 we can find integers $x \geq 1$ and $k \geq 0$ such that $e^k x \equiv 0(\text{mod } m)$ where $(x, d-1) = 1$. Then from Lemma $l \geq 1$ we can find an integer s such that $(s(d-1)+l) \equiv 0(\text{mod } x)$.
Again setting $d = ey+1$ and $n = e^k-1$ we want to show that $1+(ey+1)+\ldots+(ey+1)^{e^k-1} \equiv 0(mod e^k)$. Firstly we note that the constant term in the above sum is e^k and $(ey)^r e^k)$ for $r \geq k$. By Lemma 6, for $1 \leq r < k$, the coefficient of $(ey)^r$ in the sum is ${}^{e^k}C_{r+1}$. It then remains to show that for $1 \leq r < k$, ${}^{e^k}C_{r+1}(ey)^r \equiv 0(\text{mod } e^k)$.

Let $p \geq 2$ be a prime with $e \equiv 0(\text{mod } p)$, $(r+1) \equiv 0(\text{mod } p)$ and let λ be the exponent of the highest power of p th Then

$$\lambda < (r+1)\left(\frac{1}{p} + \frac{1}{p^2} + \dots\right)$$

and hence $\lambda < \frac{r+1}{p-1}$. Since $p \geq 2$ we then have $\lambda \leq r$. Now

$$^{e^k}C_{r+1} = \left(\frac{e^k(e^k-1)\dots(e^k-r)}{(r+1)!}\right),$$

so it follows that $e^r(e^k-1)\dots(e^k-r) \equiv 0(\text{mod } (r+1)!)$ and hence $^{e^k}C_{r+1}(ey)^r \equiv 0(\text{mod } e^k)$.

So finally we have found integers s and $n \geq 0$ such that for any $1 \leq l < m$ $(s(d-1)+l)(1+d+d^2+\dots+d^n) \equiv 0(\text{mod } e^k x)$ where $e^k x \equiv 0(\text{mod } m)$. □

4. Proof of Theorem 3

If the degree of f and g is 2 then Corollary 2.4 of [2] gives that the invariant is in fact a complete invariant for isomorphism. Hence, for the remainder of the proof, we will assume that the degree is strictly greater than 2.

Let the degree of f and g be d. Let the order of G_f be m. As the Jacobians are isomorphic, we have that the order of $G_g = m$ (c.f. Proposition 2 of [2]). From Theorem 2, there exists $1 \leq l \leq m$ such that f is isomorphic to $\alpha^l g$ where $\alpha = e^{\frac{2\pi i}{m}}$. If $l = m$ then f is isomorphic to g and the theorem is proved. Thus we can assume $1 \leq l < m$.

Let s and n be the integers given by Proposition 1. That is
$(s(d-1)+l)(1+d+\dots+d^n) \equiv 0(\text{mod } m)$.

From Theorem 1 there exists an isometry $R_1(z)$ such that $fR_1(z) = R_1\alpha^l g(z)$. Now let $R_2(z) = \alpha^s z$ and let $R(z) = R_1R_2(z)$. Then we have, by repeated use of Lemma 2 that

$f^{n+1}R(z) = f^{n+1}R_1R_2(z) = f^{n+1}R_1(\alpha^s z)$

$= f^{n+1}\alpha^{sk}R_1(z) = \alpha^{skd^{n+1}}f^{n+1}R_1(z)$

(where $k = 1$ if R_1 is orientation preserving and $k = -1$ if R_1 is orientation reversing)

$= \alpha^{skd^{n+1}}\alpha^{lk(1+d+\dots+d^n)}R_1g^{n+1} = \alpha^{skd^{n+1}+lk(1+d+\dots+d^n)}\alpha^{-sk}Rg^{n+1}$

$= \alpha^{sk(d^{n+1}-1)+lk(1+d+\dots+d^n)}Rg^{n+1} = \alpha^{k(s(d-1)+l)(1+d+\dots+d^n)}Rg^{n+1}$

$= Rg^{n+1}$.

Thus the theorem is proved.

References

[1] D. Burton, *Elementary number theory*, W. C. Brown Publishers, Iowa, 1994.

[2] R. Cowen, *On expanding endomorphisms of the circle*, J. London Math. Soc. (2) 41 (1990), 272-282.

[3] W. Parry, *Entropy and generators in ergodic theory*, W. A. Benjamin, New York, 1969.

[4] W. Parry and P. Walters, *Endomorphisms of a Lebesgue space*, Bull. Amer. Math. Soc. 78 (1972), 272-276.

[5] M. Shub and D. Sullivan, *Expanding endomorphisms of the circle revisited*, Ergod. Theory Dynam. Systems 5 (1985), 285-289.

[6] P. Walters, *Some results on the classification of some measure-preserving transformations*, Recent advances in topological dynamics, Lecture Notes in Mathematics 319, Springer Verlag, Berlin, 1973, 255-276.

Received September 29, 1998
Revised version received January 22, 1999

Department of Mathematics, University of Botswana, Private Bag 0022, Gaborone, Botswana.

E-mail address: cowenr@noka.ub.bw

E-mail address: fisherph@noka.ub.bw