AN ALGEBRAIC OBSTRUCTION TO ISOMORPHISM OF MARKOV SHIFTS WITH GROUP ALPHABETS

T. B. Ward

Final version, to appear in Bull. London Math. Soc.

Abstract. Given a compact group G, a standard construction of a $\mathbb{Z}^2$ Markov shift Σ_G with alphabet G is described. The cardinality of G (if G is finite) or the topological dimension of G (if G is a torus) is shown to be an invariant of measurable isomorphism for Σ_G. We show that if G is sufficiently non–abelian (for instance A_5, $PSL_2(\mathbb{F}_7)$ or a Suzuki simple group) and H is any abelian group with $|H| = |G|$, then Σ_G and Σ_H are not isomorphic. Thus the cardinality of G is seen to be necessary but not sufficient to determine the measurable structure of Σ_G.

1991 *Mathematics Subject Classification.* 22D40, 28D20.
Supported in part by N.S.F. grant No. DMS–91–03056 at the Ohio State University

§1: Introduction

Let G be a compact group with normalised Haar measure μ_G. Let

$$X_G = \{x \in G^{\mathbb{Z}^2} \mid x_{(i,j)} = x_{(i,j-1)} \cdot x_{(i+1,j-1)} \text{ for all } i, j \in \mathbb{Z}\}. \tag{1}$$

An element x of X_G is determined by specifying the coordinates $x_{(n,0)}$ and $x_{(0,m)}$ for $n \in \mathbb{Z}$ and $m \in \mathbb{N}_{>0}$, so Haar measure $\mu_G^{\mathbb{Z}} \otimes \mu_G^{\mathbb{N}}$ on the compact group $G^{\mathbb{Z}} \times G^{\mathbb{N}}$ determines a probability measure λ_G on X_G, defined on the class of subsets $\mathcal{B}_G$ of X_G determined by measurable subsets of $G^{\mathbb{Z}} \times G^{\mathbb{N}}$. If G is abelian, then X_G is a subgroup of $G^{\mathbb{Z}^2}$ and in this case λ_G is Haar measure on the group X_G.

The probability space $(X_G, \mathcal{B}_G, \lambda_G)$ supports a natural representation α^G of $\mathbb{Z}^2$ by λ_G–preserving transformations of X_G via the shift action

$$(\alpha^G_{(n,m)} x)_{(i,j)} = x_{(n+i,m+j)}. \tag{2}$$

The dynamical system $\Sigma_G = (\alpha^G, X_G)$ is, to within a trivial change, a generalisation of the "3–dot" or "1+x+y" system considered with various possible choices of G in [5], [6], [7], [9], [13] and [14]. We summarize the most important properties here.

If $G = \mathbb{T}$, the circle group, then X_G is a connected compact group, and the dynamical system Σ_G is an action by automorphisms with the Descending Chain Condition [5, Defn. 3.1]. It follows that the periodic points in Σ_G are dense [5, Thm. 7.2]. The action α_G has completely positive entropy [9, Thm. 6.5] and is therefore mixing of all orders [3, Thm. 2]. In fact Σ_G is measurably isomorphic to a $\mathbb{Z}^2$ Bernoulli shift [13, Thm. 2.4].

If $G = \{0, 1\}$, the group with two elements, then Σ_G again has the Descending Chain Condition (equivalently, α_G acts expansively – see [5, Thm. 5.2]) and dense periodic points ([5, Thm. 11.6]). This example (and other related actions) was shown by Ledrappier in 1978 to be a zero–entropy Markov shift which is mixing but not 2–fold mixing [7]. The periodic points are not uniformly distributed: along certain sequences of periods, the periodic points are uniformly distributed with respect to Haar measure, while along other sequences of periods there is only one periodic point for each period [14, Ex.3.3]. The shape $\{(0,0),(1,0),(0,1)\}$ is a minimal non–mixing shape [11, Ex.7.13] in the sense of [6] (see also §3). The failure of 2–fold mixing and the bad distribution of periodic points are manifestations of the same phenomenon: Σ_G does not have any specification properties.

If G is finite, then the measure λ_G may be described very easily on cylinder sets defined on contiguous sets. If $E \subset \mathbb{Z}^2$ is a finite contiguous set of positions, define an E–cylinder set by

$$A_E = \{x \in X_G \mid x_{(n,m)} = a_{(n,m)} \text{ for } (n,m) \in E\}$$

where $\{a_{(n,m)} \mid (n,m) \in E\}$ is an allowed word satisfying (1). Let $n(E)$ denote the number of positions in E at which we may choose the value of x independently: that is, the $(n(E)+1)^{\text{th}}$ position is the first one to be determined by the preceding $n(E)$ positions. Then $\lambda_G(A_E) = 1/|G|^{n(E)}$. For instance, if $E = \{(0,0),(0,1),(1,0),(1,1)\}$ then $n(E) = 3$ because we can only choose three positions in E independently. If E is not contiguous, positions may be partially determined and the measure of a cylinder set is then obtained by counting the allowed words on E.

In this note we show that the internal algebraic properties of the group G influence the measurable dynamics of Σ_G. It is clear from entropy considerations that the cardinality of G is an invariant of measurable isomorphism; what we show here is that mixing shape considerations involve more detailed attributes of G as a group rather than a set. Since it is cancellation in the alphabet group that leads to the breakdown of higher–order mixing in $\mathbb{Z}^2$ Markov groups, it is natural to expect more mixing as the alphabet group becomes less abelian, and this is an initial attempt to quantify this phenomenon.

If G is a finite group, let $G^{com} = \{ghg^{-1}h^{-1} \mid g, h \in G\}$ denote the set of commutators in G, and let G' denote the subgroup of G generated by the set G^{com}. Recall that G is said to be *perfect* if $G = G'$. We shall say that G is *entirely perfect* if $G = G^{com}$. Notice that an entirely perfect group is not solvable and therefore has even order. There are perfect groups that are not entirely perfect: in fact for any $r > 0$ there is a finite perfect group G with the property that some $g \in G$ cannot be written as a product of r commutators (see Lemma 2.1.10 in [1]). There are of course perfect groups that are not simple (for instance, $SL_2(\mathbb{F}_5)$) and for certain orders there are both simple and composite perfect groups of that order (this first occurs at order 20,160 – see [1], pp.260–264). There are many entirely perfect groups and we mention a few of them here.

(1) The alternating group A_n, for $n \geq 5$, is entirely perfect. This is stated in [10, Thm. 7]; detailed proofs are given in [2] and [4, Thm. 1]. What is proved in [10] is the *a priori* weaker statement that every element of the commutator subgroup in the symmetric group S_n is itself a commutator.

(2) The projective unimodular group $PSL_2(k)$ is entirely perfect if k is a finite field other than $\mathbb{F}_2$, $\mathbb{F}_3$ [4, Thm. 2].

(3) The Suzuki simple group $G(q)$, of order $q^2(q-1)(q^2+1)$, $q = 2^{2n+1}$, is entirely perfect [4, Thm. 3].

The dynamical systems Σ_G and Σ_H are isomorphic, written $\Sigma_G \cong \Sigma_H$, if there is an invertible measurable map $\theta : X_G \to X_H$ which has $\lambda_G\big(\theta^{-1}(A)\big) = \lambda_H(A)$ for every measurable $A \subset X_H$ and $\theta\alpha^G_{(n,m)} = \alpha^H_{(n,m)}\theta$ almost everywhere for every $(n, m) \in \mathbb{Z}^2$. An attribute $p(G)$ of G will be called an invariant (of measurable isomorphism) if $\Sigma_G \cong \Sigma_H$ implies $p(G) = p(H)$.

Questions about the mixing properties of systems of the form Σ_G and related problems have been attributed to H. Furstenberg, though I heard about them from K. Schmidt. The C.B.M.S. lecture notes [11, §§5–7] describe what little is known about higher dimensional Markov shifts and Markov groups; the examples considered here are discussed there in [11, Ex. 5.1(6)]. I would like to thank Doug Brozovic for several helpful conversations about finite groups, and an anonymous referee for suggestions leading to a strengthening of Theorem 2 and a simplification of the proof of Theorem 3.

After this note was written, K. Schmidt brought to my attention the preprint of M.

Shereshevsky, [12]. I am grateful to M. Shereshevsky for providing me with this preprint. Since [12] deals with the case of a finite abelian group alphabet (in which case Σ_G is itself a group), it is complementary to this note. We briefly describe the main results of [12] here. Firstly, Shereshevsky proves that if G_1 and G_2 are abelian p–groups with $E(G_1) \neq E(G_2)$ then Σ_{G_1} and Σ_{G_2} are non–isomorphic, where $E(G)$ is the least common multiple of the orders of the elements of G. This shows at once that the collection of two–dimensional Markov shifts $\{\Sigma_G \mid |G| = 2^n\}$ contains at least n measurably distinct shifts. He also addresses the question of topological conjugacy and provides a complete solution for G finite and abelian: Σ_G and Σ_H are topologically conjugate if and only if G and H are isomorphic. It is to be hoped that an extension of the ideas of [12] and this note may eventually produce a complete understanding of the measurable structure of Σ_G for G a finite group.

§2: The cardinality of G is an invariant

Each $\alpha^G_{(n,m)}$ is an invertible measure preserving transformation, and it is clear that isomorphism of $\mathbb{Z}^2$ actions implies isomorphism of each element of the actions.

The observations made in this section are a small application of the very extensive theory of directional and global entropies for $\mathbb{Z}^d$ actions developed in [9] and [6].

Theorem 1. *If $\Sigma_G \cong \Sigma_H$ then*

(1) *if G is finite, H is too, and $|G| = |H|$;*
(2) *if G is infinite, H is too;*
(3) *if G and H are tori, they are of the same dimension.*

Proof. (1) The map $\alpha^G_{(1,0)}$ is isomorphic to the full shift with alphabet G; it follows that $h(\alpha^G_{(1,0)}) = \log |G|$ if G is finite, and $h(\alpha^G_{(1,0)}) = \infty$ if G is infinite. Thus the two full shifts $\alpha^G_{(1,0)}$ and $\alpha^H_{(1,0)}$ are isomorphic if and only if $|G| = |H|$ for G finite.
(2) Follows from (1): if G is infinite, then $h(\alpha^H_{(1,0)}) = \infty$ so H cannot be finite.
(3) If $G = \mathbb{T}^k$, then $h(\alpha^G_{(n,m)}) = \infty$ for $(n,m) \neq (0,0)$ so the directional entropies are not helpful. However, the joint entropy of $\alpha^{\mathbb{T}}$ as a $\mathbb{Z}^2$ action is computed in [9, Ex.5.1], and is finite and positive. Since $\alpha^G \cong (\alpha^{\mathbb{T}})^k$, $h(\alpha^G) = k \cdot h(\alpha^{\mathbb{T}}) = \dim(H) \cdot h(\alpha^{\mathbb{T}})$, so $\dim(H) = k$. If $G = \mathbb{T}^\infty$, then $\Sigma_G \cong (\Sigma_{\mathbb{T}})^\infty$ so Σ_G is an infinite entropy $\mathbb{Z}^2$ Bernoulli shift by [13, Thm. 2.4]: it follows that the torus H cannot have finite dimension. □

§3: The cardinality of G is not a complete invariant

A sequence $\{(a_n,b_n),(c_n,d_n)\}_{n\in\mathbb{N}}$ in $\mathbb{Z}^2\times\mathbb{Z}^2$ will be called 2–fold mixing for α^G if

$$\lim_{n\to\infty}\lambda_G\big(A\cap\alpha^G_{(a_n,b_n)}(B)\cap\alpha^G_{(c_n,d_n)}(C)\big)=\lambda_G(A)\lambda_G(B)\lambda_G(C) \tag{3}$$

for all measurable sets $A,B,C\subset X_G$.

A 2–fold mixing sequence is clearly an invariant of measurable isomorphism. In this section we use this to show that the cardinality of the group G is not sufficient to determine the measurable structure of Σ_G, although it is sufficient to determine the measurable structure of each element $\alpha^G_{(n,m)}$ of the action. If the alphabet group is abelian, then each $\alpha^G_{(n,m)}$ is an ergodic group automorphism and is therefore isomorphic to a Bernoulli shift (see [8]) whose entropy depends only on (n,m) and $|G|$. In general, a re–coding of Σ_G allows $\alpha^G_{(n,m)}$ to be written as a full shift on some power of G, the power depending only on (n,m).

It should be emphasised that the assumption of entire perfectness in Theorem 3 is sufficient to give the 2–fold mixing property, but no comment is made on necessary algebraic conditions – other than that the alphabet group be non–abelian by Theorem 2.

Theorem 2. *If G is a finite abelian group and p is a rational prime dividing $|G|$, then the sequence $\{(p^n,0),(0,p^n)\}_{n\in\mathbb{N}}$ is not 2–fold mixing for α^G.*

Theorem 3. *If G is entirely perfect then the sequence $\{(2^n,0),(0,2^n)\}_{n\in\mathbb{N}}$ is 2–fold mixing for α^G.*

Corollary 4. *If G is an entirely perfect group, and H is an abelian group with $|G|=|H|$, then Σ_G is not isomorphic to Σ_H.*

Proof of Theorem 2. This follows from the method used for $G=\{0,1\}$ in [6] or [7]. We give a proof here for completeness and to clarify the rôle played by commutativity in the alphabet group. The group G has a factor group isomorphic to $\mathbb{Z}/p\mathbb{Z}$; let $\pi:G\to\mathbb{Z}/p\mathbb{Z}$ be the factor map. Define $\bar\pi:\Sigma_G\to\Sigma_{\mathbb{Z}/p\mathbb{Z}}$ by $(\bar\pi(x))_{(n,m)}=\pi(x_{(n,m)})$ for all $n,m\in\mathbb{Z}$. It is clear that $\alpha^{\mathbb{Z}/p\mathbb{Z}}_{(n,m)}\bar\pi=\bar\pi\alpha^G_{(n,m)}$ for all $n,m\in\mathbb{Z}$, so $\Sigma_{\mathbb{Z}/p\mathbb{Z}}$ is a factor of Σ_G. It is therefore enough to show that $\{(p^n,0),(0,p^n)\}$ is not 2–fold mixing for $\alpha^{\mathbb{Z}/p\mathbb{Z}}$.

Consider $X_{\mathbb{Z}/p\mathbb{Z}}$. If the positions $(0,0),(1,0),\dots,(n,0)$ have values $a_0,\dots,a_n$ respectively, then we must have

$$x_{(0,n)}=\sum_{j=0}^{n}\binom{n}{j}a_j \tag{4}$$

This may be proved by induction: if $n=2$, then the values are:

$$\begin{array}{ccccc} a_0+2a_1+a_2 & & & & \\ & a_0+a_1 & & a_1+a_2 & \\ & a_0 & & a_1 & \quad a_2. \end{array} \tag{5}$$

Now assume the formula for a string of $n+1$ symbols, recorded in the array

$$\begin{array}{cccc} \sum_{j=0}^{n}\binom{n}{j}a_j & \sum_{j=0}^{n}\binom{n}{j}a_{j+1} & & \\ \vdots & \vdots & & \\ a_0 & a_1 & \dots & a_n \end{array} \tag{6}$$

where $a_{n+1}=0$. If we change a_{n+1} from zero, the effect is to add a diagonal line of a_{n+1}'s along the right hand side of the array (6), giving

$$x_{(0,n+1)} = \sum_{j=0}^{n}\binom{n}{j}a_j + \sum_{j=0}^{n}\binom{n}{j}a_{j+1} = \sum_{j=0}^{n+1}[\binom{n}{j}+\binom{n}{j-1}]a_j = \sum_{j=0}^{n+1}\binom{n+1}{j}a_j$$

which shows (4).

Let $A=B=C=\{x\in X_{\mathbb{Z}/p\mathbb{Z}} \mid x_{(0,0)}=0\}$, so $\lambda_{\mathbb{Z}/p\mathbb{Z}}(A)=\frac{1}{p}$. Since p is prime, $\binom{p^k}{j}g=0$ for any $g\in\mathbb{Z}/p\mathbb{Z}$ and $j=1,\dots,p^k-1$. It follows that

$$x_{(0,p^k)} = [x_{(0,0)}+x_{(p^k,0)}] \tag{7}$$

by (4), so

$$\lambda_{\mathbb{Z}/p\mathbb{Z}}\big(A\cap\alpha^{\mathbb{Z}/p\mathbb{Z}}_{(0,p^k)}(A)\cap\alpha^{\mathbb{Z}/p\mathbb{Z}}_{(p^k,0)}(A)\big) = \frac{1}{p^2} > \frac{1}{p^3} = \lambda_{\mathbb{Z}/p\mathbb{Z}}\big(A\big)^3,$$

showing that the sequence $\{(p^n,0),(0,p^n)\}_{n\in\mathbb{N}}$ is not 2–fold mixing. □

Proof of Theorem 3. It will be convenient in this argument to identify positions in $\mathbb{Z}^2$ with their corresponding projections onto the alphabet G, so "the position (a,b) is determined" means "the value of $x_{(a,b)}$ in G is determined".

Let G be an entirely perfect group, and write the group operation in G multiplicatively with identity element e. Let $\mathcal{S}$ denote the semi–algebra of cylinder sets of the form

$$\{x\in X_G \mid x_{(i,0)}=a_i \text{ for } i=0,\dots,k-1\}. \tag{8}$$

In order to show that $\{(2^n,0),(0,2^n)\}$ is 2–fold mixing for α^G, it is enough to do this for sets of the form (8) for each $k\in\mathbb{N}$.

Let us first show that the cylinder set $A=\{x\in X_G \mid x_{(0,0)}=e\}$ does 2–fold mix along $\{(|G|n,0),(0,|G|n)\}_{n\in\mathbb{N}}$.

If $x_{(i,0)}=e$ for $i=0,\dots,|G|m$ then the entire triangle whose base extends from $(0,0)$ to $(|G|m,0)$ and whose apex is $(|G|m,0)$ must comprise e's. However, if

$$(x_{(0,0)},x_{(1,0)},x_{(2,0)},\dots,x_{(|G|m-2,0)},x_{(|G|m-1,0)},x_{(|G|m,0)}) = (a,g,e,\dots,e,h,b),$$

then the triangle is:

$$\begin{array}{cccccccc}
ag^{n-1}hgh^{n-1}b & & & & & & & \\
ag^{n-1}h & gh^{n-1}b & & & & & & \\
ag^{n-2} & gh & h^{n-2}b & & & & & \\
\vdots & \vdots & \vdots & \ddots & & & & \\
ag^3 & g & e & \dots\dots & h^3b & & & \\
ag^2 & g & e & \dots\dots & h & h^2b & & \\
ag & g & e & \dots\dots & e & h & hb & \\
a & g & e & \dots\dots & e & e & h & b
\end{array} \tag{9}$$

where $n = |G|m$. Thus $x_{(0,|G|m)} = ag^{|G|m-1}hgh^{|G|m-1}b = ag^{-1}hgh^{-1}b$, so by choosing g and h we may obtain any value for $x_{(0,|G|m)}$ if $m \geq 1$. This allows us to compute the number of allowed words on the set of positions $\{(0,0),(|G|m,0),(0,|G|m)\}$: a triple $(a,b,c) \in G^3$ is such an allowed word if there is an element $x \in X_G$ such that $x_{(0,0)} = a$, $x_{(|G|m,0)} = b$, and $x_{(0,|G|m)} = c$. By the above argument, any word is allowed, so the measure of the cylinder set determined by a word (a,b,c) is exactly $|G|^{-3}$. The set $A \cap \alpha^G_{(0,|G|m)}(A) \cap \alpha^G_{(|G|m,0)}(A)$ is such a set, corresponding to the word (e,e,e). It follows that

$$\lambda_G\big(A \cap \alpha^G_{(0,|G|m)}(A) \cap \alpha^G_{(|G|m,0)}(A)\big) = \frac{1}{|G|^3} = \lambda_G(A)^3, \tag{10}$$

so the set A does 2–fold mix along the sequence $\{(|G|n,0),(0,|G|n)\}_{n\in\mathbb{N}}$.

The general case, where we must establish property (3) for any $A,B,C \in \mathcal{S}$, may be seen as follows. Choose a fixed k in (8). Recall from (1) that $x = (x_{(n,m)}) \in X_G$ for $m \geq 0$ and all n, is determined by the values of $(x_{(n,0)})$, $n \in \mathbb{Z}$. There is an isomorphism θ between (X_{G^k}, α^{G^k}) and $(X_G, (\alpha^G)^k)$, defined by

$$\theta(\mathbf{x}_{(n,0)})_{(ki+j)} = x_i^{(j)} \tag{11}$$

where $\mathbf{x}_{(n,0)} = (x_n^{(1)},\dots,x_n^{(k)})$ is the $(n,0)$ element in X_{G^k} (the image of θ as in (11) only determines the $m \geq 0$ coordinates; requiring that θ intertwine α^{G^k} and $(\alpha^G)^k$ makes θ extend uniquely to an isomorphism.)

Apply the above argument to the system Σ_{G^k} to conclude that $\{(|G^k|n,0),(0,|G^k|n)\}_{n\in\mathbb{N}}$ is a 2–fold mixing sequence for α^{G^k} on the semi–algebra of cylinder sets in X_{G^k} defined on the $(0,0)$ coordinate. (Notice that G^k is an entirely perfect group if G is.) Applying the map θ allows us to conclude that if A, B, and C are three cylinder sets of the form (8), then, if n is sufficiently large,

$$\lambda_G\big(A \cap \alpha^G_{(nk|G^k|,0)}(B) \cap \alpha^G_{(0,nk|G^k|)}(C)\big) = \lambda_G(A)\lambda_G(B)\lambda_G(C). \tag{12}$$

For a fixed k, choose n so that (12) holds and let $N = nk|G^k|$. That is, there are $|G|^{3k}$ allowed words on the positions

$$\{(0,0),\dots,(k-1,0),(N,0),\dots,(N+k-1,0),(0,N),\dots,(k-1,N)\}.$$

It follows that there are $|G|^{3k}$ allowed words on the positions

$$\{(0,0),\dots,(k-1,0),(N+1,0),\dots,(N+k,0),(0,N+1),\dots,(k-1,N+1)\}.$$

So, if N exceeds $nk|G^k|$,

$$\lambda_G\big(A \cap \alpha^G_{(N,0)}(B) \cap \alpha^G_{(0,N)}(C)\big) = \lambda_G(A)\lambda_G(B)\lambda_G(C), \tag{13}$$

showing that $\{(N,0),(0,N)\}_{N\in\mathbb{N}}$ is 2–fold mixing for α^G. Theorem 3 follows at once. $\square$

References

[1] D. F. Holt and W. Plesken, *Perfect Groups*, Clarendon Press, Oxford, 1989.

[2] N. Ito, *A theorem on the alternating group* $\mathfrak{G}_n$ $(n \geq 5)$, Math. Japonicae **2** (1951), 59–60.

[3] B. Kamiński, *Mixing properties of two–dimensional dynamical systems with completely positive entropy*, Bull. de L'Acad. Polon. des Sci. **XXVIII** (1980), 453–463.

[4] T. K'en-ch'eng & H. Ch'eng-hao, *On the commutators of two classes of finite simple groups*, Shuxue Jinzhan (Chinese) **8** (1965), 202–208; MR **34**, #5938.

[5] B. Kitchens & K. Schmidt, *Automorphisms of compact groups*, Ergod. Th. & Dynam. Sys. **9** (1989), 691–735.

[6] ———, *Mixing sets and relative entropies*, Warwick University Preprint (1991).

[7] F. Ledrappier, *Un champ markovien peut être d'entropie nulle et melangeant*, Comptes Rendus Acad. Sci. Paris **Ser. A, 287** (1978), 561–562.

[8] D. Lind, *The structure of skew products with ergodic group automorphisms*, Israel J. of Math. **28** (1977), 205–248.

[9] D. Lind, K. Schmidt & T. Ward, *Mahler measure and entropy for commuting automorphisms of compact groups*, Inventiones mathematicæ **101** (1990), 593–629.

[10] O. Ore, *Some remarks on commutators*, Proc. Amer. Math. Soc. **2** (1951), 307–314.

[11] K. Schmidt, *Algebraic ideas in ergodic theory*, C.B.M.S. Reg. Conf. Ser. in Math. **76** (1990).

[12] M. A. Shereshevsky, *On the classification of some two–dimensional Markov shifts with group structure*, Warwick University Preprint (1991).

[13] T. Ward, *Almost block independence for the three dot* Z^2 *dynamical system*, Israel J. of Math, to appear.

[14] ———, *Periodic points for expansive actions of* Z^2 *on compact abelian groups*, Bull. London Math. Soc., to appear.

Department of Mathematics
Ohio State University
Columbus
OH 43210
USA.

(from June 1992) School of Mathematics
University of East Anglia
Norwich
NR4 7TJ