Distributions with Fixed Marginals and Related Topics
IMS Lecture Notes – Monograph Series Vol. 28, 1996

DOUBLY STOCHASTIC MEASURES: THREE VIGNETTES

BY DAVID FELDMAN
University of New Hampshire

The first section contains a nonstandard analysis proof of Strassen's theorem. The second section contains a uniqueness theorem for doubly stochastic measures on a family of supports that give rise in a natural way to certain dynamical systems. In the final section, we consider the action of $SL_2(\mathbb{Z})$ on $C(G \times G)^*$, G a compact abelian group, and study those orbits that consist entirely of stochastic or doubly stochastic measures.

0. Introduction. Our present state of knowledge concerning extreme doubly stochastic measures on $I \times I$ ($I = [0,1]$) and doubly stochastic measures with prescribed support is meager compared with the the situation for doubly stochastic finite matrices.

Recall that according to the Birkhoff-von Neumann Theorem, Birkhoff (1946), the extreme doubly stochastic $n \times n$-matrices are precisely the $n \times n$-permutation matrices. This being so, a set $S \subseteq \mathbf{n} \times \mathbf{n}$ ($\mathbf{n} = \{1, \ldots, n\}$) contains the support of a doubly stochastic matrix iff S contains the support of a permutation matrix iff the bipartite graph whose incidence relation S describes admits a perfect matching. P. Hall's theorem, Lovasz and Plummer (1986), tells us that S fails to admit a perfect matching iff S is disjoint from a set of the form $A \times B$, $A, B \subseteq \mathbf{n}$, $|A| + |B| > n$. With the availability of highly efficient algorithms for bipartite matching, Lovasz and Plummer (1986), our understanding of doubly stochastic finite matrices may be considered quite satisfactory.

One measure-theoretic analogue for the permutation matrices might be the class of doubly stochastic measures supported on graphs of measure preserving transformations. Alas, these form merely a proper subclass of the extreme doubly stochastic measures, so the most straightforward generalization of the Birkhoff-von Neumann Theorem is false. Indeed, extreme doubly

AMS 1991 Subject Classification: 15A51, 11F06, 28E05, 34C35

Key words and phrases: Doubly stochastic measure, Strassen's theorem, irrational rotation, $SL_2(\mathbb{Z})$.

stochastic measures may be quite pathological, Feldman (1992), Losert (1982), and the determination of whether a given set, even of simple form, supports a doubly stochastic measure can be a delicate matter, Kamiński et al. (1988), Sherwood and Taylor (1988).

This paper explores some ways in which the study of doubly stochastic measures interacts with diverse branches of mathematics, including logic, group theory, Fourier analysis, topological dynamics and ergodic theory. The three sections of the body of the paper are independent aside from certain comments.

The first section contains a proof by nonstandard analysis of an old theorem of Strassen, Strassen (1965), characterizing closed subsets S of $I \times I$ which support doubly stochastic measures: A closed set $S \subset I \times I$ *fails* to support a doubly stochastic measure iff S is disjoint from a set of the form $A \times B$ (A, B Borel subsets of I) where $m(A) + m(B) > 1$ (m is Lebesgue measure). The statement about finite matrices that Strassen's theorem generalizes is actually a consequence of the Birkhoff-von Neumann Theorem and P. Hall's Theorem together and does not mention permutation matrices. The nonstandard viewpoint offers a conceptual handle on why it should be this statement that generalizes. No previous knowledge of nonstandard analysis is assumed of the reader as we derive whatever we need from the most basic theorems of mathematical logic. Our proof of Strassen's theorem suggests an experimental approach to investigating whether a particular S supports a doubly stochastic measure.

In Section 2 we give a uniqueness theorem concerning doubly stochastic measures by using ideas from topological dynamics and ergodic theory. In particular, these examples illustrate how small perturbations in a set S may or may not affect the uniqueness of doubly stochastic measures supported on S. This sensitivity is indicative of the limitations of the experimental approach discussed in Section 1.

Section 3 discusses measure-theoretic analogues of "magic squares." Let $\mathbb{Z}/\langle p \rangle$ be the finite field with p elements. Let f be a real (or complex) valued function on $\mathbb{Z}/\langle p \rangle \times \mathbb{Z}/\langle p \rangle$ and assume that the values of f sum to 1 over every affine 1-dimensional subspace of $\mathbb{Z}/\langle p \rangle \times \mathbb{Z}/\langle p \rangle$. Then it is known that f must be a constant function always taking the value $1/p$. We formulate some measure-theoretic analogues of this statement featuring the modular group and some of its subgroups.

It is my pleasure to thank Professors D. Hadwin, R. Shortt and A. Wilce for discussions or criticisms that improved this paper.

1. A Nonstandard Approach to Strassen's Theorem.

THEOREM 1 (Strassen). *Let S be a closed subset of $I \times I$. Let m be Lebesgue measure on I. Then the following statements are equivalent:*

(I) There exists a doubly stochastic measure μ on $I \times I$ such that $\mu(S) = 1$.

(II) If $A, B \subset I$ are Borel sets such that $(A \times B) \cap S = \emptyset$, then $m(A) + m(B) \leq 1$.

PROOF. The easy direction is (I) implies (II). Indeed, if $(A \times B) \cap S = \emptyset$ and μ is a doubly stochastic measure with $\mu(S) = 1$, then $\mu(A \times B) = 0$. Thus

$$m(A) = \mu(A \times I) = \mu(A \times B^c) \leq m(I \times B^c) = 1 - m(B) \ .$$

The idea behind our proof that (II) implies (I) is to associate doubly stochastic measures μ satisfying $\mu(S) = 1$ with models of a certain first order theory $\mathcal{T}$.

Suppose S satisfies (II).

Let $C = \{0,1\}^\omega$ be the Cantor set. Let $f : C = \{0,1\}^\omega \to I$ be the usual map which regards 0–1 sequences as binary expansions, i.e. $f(\langle a_i \rangle_{i \in \mathbb{N}}) = \sum_{i=1}^{\infty} a_i 2^{-i}$. We write m for both Lebesgue measure on I and its unique lifting along f to C. Write $S_C = (f \times f)^{-1}(S)$.

We will actually prove the existence of a doubly stochastic measure μ_C on $C \times C$ such that $\mu_C(S_C) = 1$. Any doubly stochastic measure μ_C on $C \times C$ can be pushed forward along $f \times f : C \times C \to I \times I$ to a doubly stochastic measure μ on $I \times I$, so this will be sufficient. In fact, where there is no possibility of confusion, we will refer to S_C simply as S and μ_C simply as μ.

We are now ready to describe the first-order theory $\mathcal{T}$. Take note that the theory $\mathcal{T}$ has an uncountable language and uncountably many axioms.

Begin with your favorite first order axiomatization of the real numbers.

Introduce a constant symbol c_r for each (standard) real number r (not just for 0 and 1 as is usual). The intended interpretation of c_r is r, so adopt whatever axioms are necessary to insure that these constants behave arithmetically like the reals that index them, e.g. $c_2 + c_2 = c_4$, $c_3 > c_2$ and $c_0 = 0$.

Let $\mathcal{F}$ be the field of subsets of $C \times C$ generated by sets of the form $A \times B$ where A and B are finitely determined cylinder sets of C. For each $T \in \mathcal{F}$, introduce a constant symbol c_T and take as axioms statements of the form $c_T \geq 0$. The intended interpretation of c_T is $\mu(T)$ where μ is a positive measure.

For each disjoint finite family $T_1, \ldots, T_n$ of sets in $\mathcal{F}$, introduce the axiom

$$c_{T_1} + \ldots + c_{T_n} = c_{T_1 \cup \ldots \cup T_n} .$$

For each set in $\mathcal{F}$ of the form $A \times I$ (resp. $I \times B$), introduce the axiom

$$c_{A\times I} = c_{m(A)} \quad (\text{resp.} \quad c_{I\times B} = c_{m(B)}).$$

For each $T \in \mathcal{F}$ satisfying $S \subset T$, introduce the axiom $c_T = 1$.

A model M of $\mathcal{T}$ determines a doubly stochastic measure μ on $C \times C$ as follows. The underlying set of M is *a priori* a nonstandard extension of the reals, but passing to the standard parts of the values c_T determines a finitely additive measure on the field of sets $\mathcal{F}$. Because C is totally disconnected and the field $\mathcal{F}$ consists of clopen sets, this is actually a countably additive measure on $\mathcal{F}$. The σ-field generated by $\mathcal{F}$ is the Borel field on $C \times C$ and the Caratheodory extension theorem gives us a unique Borel measure μ on $C \times C$. (It is also true that a doubly stochastic measure μ on $I \times I$ with $\mu(S) = 1$ determines a model of $\mathcal{T}$, but we do not use this fact here.)

Suppose now, for contradiction, that there is no doubly stochastic measure μ such that $\mu(S) = 1$. We must find Borel sets $A, B \subset C$ such that $(A \times B) \cap S = \emptyset$ and $m(A) + m(B) > 1$.

Since there is no such μ, the theory $\mathcal{T}$ has no model. By the compactness theorem for first-order logic, some finite subset $\mathcal{T}_f$ of the axioms constituting $\mathcal{T}$ already fail to have a model. The axioms in $\mathcal{T}_f$ involve only finitely many of the constant symbols, and, in particular, only finitely many of the form c_T, $T \in \mathcal{F}$, say $c_{T_1}, \ldots, c_{T_n}$.

Now let us write $\pi_k : C \to \{0,1\}^k$ for the projection onto the first k coordinates. Let $\mathcal{F}_k$ be the (finite) subfield of $\mathcal{F}$ generated by sets of the form $(\pi_k \times \pi_k)^{-1}(a)$, $a \in \{0,1\}^k \times \{0,1\}^k$. Choose k large enough so that all the sets $T_1, \ldots, T_n$ belong to $\mathcal{F}_k$.

Observe that since measures on the field $\mathcal{F}_k$ are determined by their values on the atoms $\mathcal{F}_k$, they are essentially $2^k \times 2^k$ matrices.

Let S' be the smallest subset of $\{0,1\}^k \times \{0,1\}^k$ such that $S \subset \bigcup_{a\in S'} (\pi_k \times \pi_k)^{-1}(a)$. There can be no $2^k \times 2^k$ doubly stochastic matrix (rows and columns indexed by $\{0,1\}^k$) which is 0 outside of S', because $\mathcal{T}_f$ has no model. By Birkhoff-von Neumann and P. Hall, there must be sets $P, Q \subset \{0,1\}^k$ such that $P \times Q$ is disjoint from S' and $|P| + |Q| > 2^k$. Finally, setting $A = \pi_k^{-1}(P)$ and $B = \pi_k^{-1}(Q)$ gives us the desired contradiction. ∎

The referee has kindly observed that the construction underlying the proof above is essentially Loeb's extension trick, Cutland (1988).

Note that this proof is easily modified to yield Strassen's more precise result:

THEOREM 2. *Let S be a closed subset of $I \times I$. Let m be Lebesgue measure on I. Then the following statements are equivalent:*

(I) There exists a doubly stochastic measure μ on $I \times I$ such that $\mu(S) = 1-\epsilon$.

(II) If $A, B \subset I$ are Borel sets such that $(A \times B) \cap S = \emptyset$, then $m(A)+m(B) \leq 1+\epsilon$.

What makes our nonstandard proof of Strassen's theorem work is the fact that the property of being a doubly stochastic measure with support in a closed set S is *finitely refutable*, in the sense that if μ is *not* such a measure, then this is already evident upon examining the values of μ on finitely many sets. For example, we may either exhibit a vertical or or horizontal strip where μ does not have the correct measure, or a set on which the measure of μ is negative, or a set disjoint from S on which the measure of μ is positive.

This suggests many problems. For example, let $\mathcal{D}$ (resp. $\mathcal{D}'$) be the closed convex hull of the set of extreme doubly stochastic measures which are symmetric about the diagonal $x = y$ of $I \times I$ (resp. symmetric about the diagonal $x = y$ of $I \times I$ and supported off of it). (Note that the symmetric extreme doubly stochastic measures are a subset of the extreme symmetric doubly stochastic measures.) Is $\mathcal{D}$ finitely refutable? This question is a natural one in light of the analogy to finite combinatorics. Strassen's theorem may be regarded as a measure-theoretic analogue for the matching theory of bipartite graphs. One might regard a criterion for whether a closed set S supports a measure in $\mathcal{D}$, or what amounts to the same, whether S supports a symmetric extreme doubly stochastic measure, as a measure-theoretic analogue for the matching theory of arbitrary graphs. For the basic matching theory of arbitrary graphs, especially Tutte's theorem, Gallai's Lemma and Berge's Formula, see Chapter 3 of Lovasz and Plummer (1986). For the Matching Polytope and Perfect Matching Polytope, the matrix analogues of $\mathcal{D}$ and $\mathcal{D}'$, and for Edmonds Theorem, see Chapter 7.

Some interesting examples of finitely refutable closed convex sets of doubly stochastic measures appear in Section 3.

2. Dynamics and Doubly Stochastic Measures. We turn now to a theorem concerning the uniqueness, when they exist, of doubly stochastic measures on a certain family of supports in the square $I \times I$. The supports of these measures will be simple closed curves Θ satisfying three conditions. The first two conditions are:

(I) Θ meets the interior of each side of the square once;

(II) Θ meets every other vertical or horizontal line in the square exactly twice.

Observe that Θ is the union of two graphs, but is never a hairpin in the sense of Kamiński et al. (1988),Sherwood and Taylor (1988) since Θ avoids the corners of the square. We shall write l, r, t and b for the unique points where Θ meets the left, right, top and bottom edges of the square.

To state the third condition, we need some terminology. Associated to a curve Θ satisfying (I) and (II) are two natural orientation-reversing involutive self-homeomorphisms, vertical exchange V and horizontal exchange H. In detail, $V(x) = y$ (resp. $H(x) = y$) iff either x and y are distinct points on Θ on the same vertical (resp. horizontal) line or $x = y = l$ or r (resp. $x = y = t$ or b). The composition VH is then an orientation-preserving fixed-point-free self-homeomorphism of Θ. The third condition on Θ is:

(III) There exists a homeomorphism $\phi : \Theta \to R/\mathbb{Z}$ such that $\phi VH\phi^{-1}(x) = x + q$ where q is irrational.

In other words, VH is conjugate to an irrational rotation.

THEOREM 3. *A curve Θ satisfying conditions (I), (II) and (III) supports at most one doubly stochastic measure.*

In particular, if such a curve does support a doubly stochastic measure, the measure must be extreme.

PROOF. We shall need the following

LEMMA 1. *Let τ_1, τ_2 be orientation-reversing self-homeomorphisms of $S^1 = R/\mathbb{Z}$. Assume that $\tau_1^2 = \tau_2^2 = \mathrm{id}$, the identity map, and that $\tau_1\tau_2 = \rho$ is an irrational rotation, that is $\rho(x) = x + q \pmod 1$, where q is irrational. Then τ_1 and τ_2 are reflections.*

PROOF. Lift τ_1 to a map $\tilde{\tau}_1 : R \to R$ and define $\tilde{\rho}(x) := x + q$ for $x \in R$. Now set $\tilde{\tau}_2 = \tilde{\tau}_1\tilde{\rho}$; then $\tilde{\tau}_2$ is a lift of τ_2. Since τ_2 is an orientation-reversing homeomorphism, the lift $\tilde{\tau}_2$ satisfies $\tilde{\tau}_2(x+1) = \tilde{\tau}_2(x) - 1$, so by the Intermediate Value Theorem $\tilde{\tau}_2$ must have a fixed point. Thus we have

$$\tilde{\tau_2}^2 = \tilde{\tau}_1\tilde{\rho}\tilde{\tau}_1\tilde{\rho} = \mathrm{id},$$

not just modulo 1, but exactly! Similarly, $\tilde{\tau_1}^2 = \mathrm{id}$, so we obtain $\tilde{\rho}\tilde{\tau}_1\tilde{\rho} = \tilde{\tau}_1$. Now define $u(x) := -\tilde{\tau}_1(x+q) - x$. Since

$$\tilde{\tau}_1(x+q) + q = \tilde{\tau}_1(x)$$

we obtain $u(x+q) = u(x)$. Since $\tilde{\tau}_1$ is the also the lift of an orientation reversing homeomorphism, $\tilde{\tau}_1(x+1) = \tilde{\tau}_1(x) - 1$ and thus $u(x+1) = u(x)$. So $u(x)$ is a continuous function with two irrationally related periods, hence a constant function. From the definition of u we see that τ_1 is a reflection, and so likewise τ_2. ∎

(Observe how the irrationality of q in Lemma 1 is essential.)

If Θ satisfies (I), (II) and (III), then by the lemma, we may choose ϕ so that $\phi V \phi^{-1}(x) = -x$ and $\phi H \phi^{-1}(x) = q - x$. Without loss of generality, we may assume that $\phi(l) = 0$ and $\phi(b) = q/2$, both modulo 1.

We write $\pi_i : I \times I \to I$ for projection onto the i^{th} coordinate.

Now suppose that μ is a doubly stochastic measure stochastic on Θ. Let $\tilde{\mu}$ be the Borel measure on $R/\mathbb{Z}$ determined by the condition that $\tilde{\mu}(B) = \mu(\phi^{-1}(B))$ for all Borel sets $B \subseteq R/\mathbb{Z}$.

If $x \mapsto \psi(x)$ defines a self-homeomorphism of $R/\mathbb{Z}$, we shall write $\tilde{\mu}_{\psi(x)}$ for the result of pushing $\tilde{\mu}$ along ψ. The double stochasticity of μ may now be expressed in terms of $\tilde{\mu}$ as follows:

$$\tilde{\mu}_x + \tilde{\mu}_{-x} = \nu_1$$

and

$$\tilde{\mu}_x + \tilde{\mu}_{q-x} = \nu_2$$

where the measures ν_1 and ν_2 depend only on ϕ, not on μ. For example, for $0 \leq a \leq 1$, $\nu_1([0,a]) = \pi_1 \phi^{-1}(a)$ and $\nu_2([0,a]) = \pi_2 \phi^{-1}(a)$. Combining these equations shows that $\tilde{\mu}$ satisfies the inhomogeneous difference equation

$$\tilde{\mu}_{q-x} - \tilde{\mu}_{-x} = \nu_2 - \nu_1 \,. \tag{$*$}$$

Suppose μ' were a distinct doubly stochastic measure supported on Θ. Then $\tilde{\mu}'$ would be a distinct solution of the inhomomogenous difference equation $(*)$, and the signed measure $\xi = \tilde{\mu}' - \tilde{\mu}$ would satisfy the homogenous difference equation

$$\xi_{q-x} - \xi_{-x} = 0$$

or $\xi_{q+x} = \xi_x$. Since irrotational rotations are ergodic maps, the Radon-Nikodym derivative of ξ with respect Lebesgue measure must be constant, and indeed must be 0 since $\xi(R/\mathbb{Z}) = 0$. Thus $\tilde{\mu} = \tilde{\mu}'$ and $\mu = \mu'$. ∎

Using Fourier techniques, one may obtain at least a formal expression for the Fourier series of the measure $\tilde{\mu}$ (exclusive of the constant term which one knows anyway) in terms of the Fourier series of $\nu_2 - \nu_1$. On the other hand, the question of whether the Fourier series one obtains is the Fourier series of even just a signed measure depends in a delicate way on the Fourier series of $\nu_2 - \nu_1$ and on the diophantine approximation of q by rationals.

To see that the hypothesis that q is irrational is essential to Theorem 3, one need only consider the cases where Θ is a rectangle symmetric about the diagonal. Then q is rational if the ratio of the lengths of the sides are rational, and in that case one sees easily that Θ supports uncountably many distinct doubly stochastic measures.

It is also easy to see that the rotation number q does not, by itself determine the existence of a doubly stochastic measure supported on Θ. In particular, if $\zeta : I \times I \to I \times I$ is a homeomorphism of the the square of the form $\zeta(x, y) = (\zeta_1(x), \zeta_2(y))$, then the curve Θ' obtained by pulling Θ back along ζ has the same rotation number as Θ. On the other hand, we may choose ζ so that Θ' is entirely concentrated near the sides of $I \times I$. If Θ' is disjoint from, say $[1/5, 4/5] \times [1/5, 4/5]$, then Θ' cannot support a doubly stochastic measure, by the easy direction of Strassen's theorem above.

3. $SL_2(\mathbb{Z})$ Actions and Double Stochasticity. Let G be a compact abelian group. In this section we study a special class of doubly stochastic measures on $G \times G$.

We begin with notation. Haar measure on G, normalized as a probability measure, we denote by m_G. The Pontrayagin dual of G, the group of continuous complex characters, we write as $\widehat{G}$. If $\chi \in \widehat{G}$, then $\overline{\chi}$ is the complex conjugate of χ. When $g_1, \ldots, g_n$ are elements of a (discrete) group, $\langle g_1, \ldots, g_n \rangle$ is the subgroup they generate. If a and b are integers, $\mathrm{GCD}(a, b)$ is their greatest common divisor. If M is a matrix, M^T is its transpose. Where we distinguish between row vectors and column vectors, this notation appears frequently.

If X is a topological space, then $C(X)$ is the space of continuous complex-valued functions on X. The Riesz representation theorem provides a correspondence between complex regular Borel measures on X and $C(X)^*$, the bounded complex-valued linear functionals on $C(X)$. We shall systematically abuse notation by letting the same symbol, usually μ, stand at once for the measure, the associated functional on $C(X)$ and the extension of this functional to $L_1(\mu)$.

Let $\Gamma = SL_2(\mathbb{Z})$ denote the group of 2×2 matrices over the integers with determinant 1 or -1. We understand Γ to act on $G \times G$ on the left:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} g_1 \\ g_2 \end{pmatrix} = \begin{pmatrix} ag_2 + bg_2 \\ cg_1 + dg_2 \end{pmatrix}.$$

Then Γ also acts on $C(G \times G)$ by $(\gamma f)(g_1, g_2) = f(\gamma(g_1, g_2)^T)$ and on $C(G \times G)^*$ by $(\gamma\mu)f = \mu(\gamma f)$. The action of Γ on $\widehat{G \times G}$ is actually a special case of the action on $C(G \times G)$. Using the canonical isomorphism $\widehat{G \times G} = \widehat{G} \times \widehat{G}$ we can write $\chi \in \widehat{G \times G}$ as (χ_1, χ_2), $\chi_i \in \widehat{G}$, $i = 1, 2$, where $\chi(g_1, g_2) = \chi_1(g_1)\chi_2(g_2)$. Then $\gamma\chi = (\chi_1, \chi_2)\gamma^T$.

Let $\pi_i : G \times G \to G$ be projection onto the ith coordinate (i=1,2). A positive measure $\mu \in C(G \times G)^*$ is stochastic in the i^{th} variable if $\mu(h\pi_i) = m_G(h)$ for all $h \in C(G)$ and doubly stochastic if it is stochastic in both variables.

LEMMA 2. *A positive measure $\mu \in C(G \times G)^*$ is stochastic in the ith variable if and only if $\mu(1) = 1$ and $\mu(\chi\pi_i) = 0$ for all nontrivial $\chi \in \widehat{G}$.*

PROOF. If $\mu \in C(G \times G)^*$ is stochastic in the ith variable, then $\mu(\chi\pi_i) = m_G(\chi)$ which is 1 or 0 according as χ is trivial or not. Conversely $\mu_i(h) = \mu(h\pi_i)$ defines a measure on G and such a measure is determined by its behavior on characters. If $\mu(1) = 1$ and $\mu(\chi\pi_i) = 0$, then we must have $\mu_i = m_G$. ∎

LEMMA 3. *Let H be an abelian group. Let Δ be a subgroup of Γ such that for any ordered pair of relatively prime integers (a, c), either $(a, c)^T$ or $(-a, -c)^T$ occurs as the first column of an element of Δ. Then following are equivalent:*

(I) Every finitely generated subgroup of H is cyclic;

(II) $H \times H = \{\gamma(h, 0)^T \mid \gamma \in \Delta, h \in H\}$;

(III) H is isomorphic either to a subgroup of $\mathbb{Q}$ or a subgroup of $\mathbb{Q}/\mathbb{Z}$.

PROOF.

(I) implies (II): If every finitely generated subgroup of H is cyclic, then given $(h_1, h_2)^T \in H \times H$, let h be a generator of $\langle h_1, h_2\rangle$. We may always choose h so as to write $(h_1, h_2)^T = (ah, ch)^T$, where a and c are relatively prime integers. Then there exists an element γ of Δ which has either the form $\left(\begin{smallmatrix} a & * \\ c & * \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} -a & * \\ -c & * \end{smallmatrix}\right)$. In the first case, we have immediately that $\gamma(h, 0)^T = (h_1, h_2)^T$; otherwise we must first replace h by $-h$.

(II) implies (I): Assume $H \times H = \{\gamma(h, 0)^T \mid \gamma \in \Delta, h \in H\}$. Given elements h_1 and h_2, we may write $(h_1, h_2)^T = \gamma(h, 0)^T$ for some $\gamma \in \Delta$. Thus $\langle h_1, h_2\rangle \subseteq \langle h\rangle$, so $\langle h_1, h_2\rangle$ is a cyclic group. By induction, if every pair of elements of H generates a cyclic subgroup, then every finitely generated subgroup of H is cyclic.

(I) implies (III): Assume that every finitely generated subgroup of H is cyclic. A pair consisting of a torsion element and nontorsion element can't generate a cyclic subgroup, so H must be either torsion or torsion-free.

If H is torsion free, pick any element $u \neq 0$ in H. Given v in H, let w be a generator of $\langle u, v\rangle$, so $(u, v) = (m_1 w, m_2 w)$ for integers m_1, m_2. Note that $m_1 \neq 0$. Define a function $\phi : H \to \mathbb{Q}$ by $\phi(v) = m_2/m_1$. One checks easily that ϕ is a well-defined injective homomorphism.

If H is a torsion group, choose a sequence of positive integers $n_1, n_2, \ldots$, such that

1) n_i is the order of some element of H;

2) n_i divides n_{i+1};

3) if m is the order of some v in H, m divides n_i for i sufficiently large.

Next, choose a sequence of elements $w_1, w_2, \ldots$ such that the order of w_i is n_i. Now we may inductively define a new sequence $w'_1, w'_2, \ldots$ such that $w_1 = w'_1$ and $w'_i = (n_{i+1}/n_i)w'_{i+1}$ by using the fact that $\langle w'_i, w_{i+1}\rangle = \langle w_{i+1}\rangle$ since both groups are cyclic of order n_{i+1}. Now mapping w'_i to $1/n_i$ defines a homomorphism from H to $\mathbb{Q}/\mathbb{Z}$.

(III) implies (I): Take common denominators. ∎

For any abelian group H, write $\mathcal{O}_H$ for the set $\{\gamma(h,0)^T \mid \gamma \in \Delta, h \in H\}$. The set $\mathcal{O}_H$ coincides with $\{(h_1,h_2)^T \mid \langle h_1, h_2\rangle \text{ is cyclic}\}$, as one sees from the proof of Lemma 3.

THEOREM 4. *Let G be a compact abelian group. Let Δ be a subgroup of Γ such that for any pair of relatively prime integers (a,b), either (a,b) or $(-a,-b)$ occurs as the first row of an element of Δ. Then the following are equivalent:*

(I) $\widehat{G}$ is isomorphic either to a subgroup of $\mathbb{Q}$ or a subgroup of $\mathbb{Q}/\mathbb{Z}$;

(II) If μ is a measure on $G \times G$ such that $\gamma\mu$ is stochastic in the first variable for all $\gamma \in \Delta$, then μ is Haar measure on $G \times G$.

PROOF. Assume that $\widehat{G}$ is isomorphic either to a subgroup of $\mathbb{Q}$ or a subgroup of $\mathbb{Q}/\mathbb{Z}$. Assume further that μ is a measure on $G \times G$ such that $\gamma\mu$ is stochastic in the first variable for all $\gamma \in \Delta$. Clearly $\mu(1) = 1$, so to see that μ is Haar measure, it suffices to show that $\mu(\chi) = 0$ for every nontrivial character $\chi \in \widehat{G}$. Write $\chi = (\chi_1, \chi_2)$ as above. Then by the analogue of Lemma 3 for right actions, $\chi = (\chi_3, 0)\gamma^T$ for some nontrivial $\chi_3 \in \widehat{G}$ and some $\gamma \in \Delta$. Since $\gamma\mu$ is stochastic in the first variable,

$$0 = m_G(\chi_3) = (\gamma\mu)(\chi_3\pi_1) = (\gamma\mu)(\chi_3, 0) = \mu(\chi_3, 0)\gamma^T = \mu\chi \; .$$

Thus μ is Haar measure.

For the other direction, we observe that by Lemma 2, a positive measure μ satisfies the hypothesis of (II) provided that its Fourier coefficents are supported outside of $\mathcal{O}_{\widehat{G}}$. So, for example, if $\chi_1, \chi_2 \in \widehat{G}$ generate a noncyclic subgroup, let μ be the measure on $G \times G$ with Radon-Nikodym derivative

$$\frac{d\mu}{dm_{G\times G}}(g_1, g_2) = 1 + \epsilon(\chi_1(g_1)\chi_2(g_2) + \overline{\chi_1}(g_1)\overline{\chi_2}(g_2)).$$

Then μ is a real measure and positive if ϵ is sufficiently small, and $\gamma\mu$ will be stochastic in the first variable for every $\gamma \in \Delta$. ∎

The next theorem is a straightforward generalization of Lindenstrauss' characterization of extreme doubly stochastic measures, Lindenstrauss (1965). Combined with the previous theorem it yields an interesting corollary.

THEOREM 5. *Let G be a abelian compact group and Δ be a subgroup of $SL_2(\mathbb{Z})$. Let $\mathcal{M}$ be the convex set of all measures μ on $G \times G$ such that $\gamma\mu$ is stochastic in the first variable for every $\gamma \in \Delta$. Then μ is an extreme point of $\mathcal{M}$ if and only if $L_1(\mu)$ is the norm closure of the space spanned by functions of the form $(g_1, g_2) \mapsto h(ag_1 + cg_2)$ with $h \in L_1(m_G)$ and $(a, c)^T$ the first column of a matrix in Δ.*

PROOF. Suppose $\mu \in \mathcal{M}$. Recall that the dual of $L_1(\mu)$ is $L_\infty(\mu)$. For $k \in L_\infty(\mu)$, $\nu(h) = \mu(kh)$ defines a signed measure on $G \times G$ absolutely continuous with respect to μ, and the Radon-Nikodym theorem says that all such signed measures arise in this fashion.

So let V be the norm closure in $L_1(\mu)$ of the space spanned by all functions of the form $(g_1, g_2) \mapsto h(ag_1 + cg_2)$, where $h \in L_1(m_G)$ and $(a, c)^T$ is the first column of a matrix in Δ. Then $V = L_1(\mu)$ if and only if whenever $k \in L_\infty(\mu)$ satisfies $\mu(kh(ag_1 + cg_2)) = 0$ for all $h \in L_1(m_G)$, then $k = 0$.

Now suppose $\mu = (1/2)(\mu_1 + \mu_2)$ for $\mu_i \in \mathcal{M}$. Then $\nu = \mu - \mu_1$ is a signed measure satisfying $|\nu(A)| \leq \mu(A)$ for every Borel set $A \subseteq G \times G$. Then there is a $k \in L_\infty(\mu)$ with $||L||_\infty \leq 1$ such that $\nu(j) = \mu(kj)$ for all $j \in L_1(\mu)$. Moreover, for all $\gamma \in \Delta$ and $h \in L_1(m_G)$, we have

$$(\gamma\nu)(h\pi_1) = (\gamma\mu)(h\pi_1) - (\gamma\mu_1)(h\pi_1) = m_G(h) - m_G(h) = 0.$$

Thus

$$\mu(kh(ag_1 + cg_2)) = \mu(k\gamma h\pi_1) = \nu(\gamma h\pi_1) = (\gamma\nu)(h\pi_1) = 0.$$

Now if $V = L_1(\mu)$, then $k = 0$, $\nu = 0$, $\mu = \mu_1 = \mu_2$, so μ is an extreme point.

Conversely, if $V \neq L_1(\mu)$, then we can find a $k \in L_\infty(\mu)$ with $||L||_\infty \leq 1$ such that $\mu(kh(ag_1 + cg_2)) = 0$ for all $h \in L_1(m_G)$. Then k determines a signed measure ν satisfying $|\nu(A)| \leq \mu(A)$ for every Borel set $A \subseteq G \times G$, and the measures $\mu + \nu$ and $\mu - \nu$ belong to $\mathcal{M}$. So μ is not an extreme point. ∎

COROLLARY. *Let G be a abelian compact group such that every finitely generated subgroup of $\widehat{G}$ is cyclic. Then $L_1(m_{G\times G})$ is the norm closure of the space spanned by functions F of the form $(g_1, g_2) \mapsto h(ag_1 + cg_2)$ where $h \in L_1(m_G)$ and a and c are relatively prime.*

PROOF. If every finitely generated subgroup of $\widehat{G}$ is cyclic, then $\mathcal{M}$ contains just the single measure $m_{G\times G}$ which is then trivially extreme. ∎

The following theorem is a variation on Theorem 4:

THEOREM 6. *Let G be compact group. Let Δ be a subgroup of $SL_2(\mathbb{Z})$ with the property that given any pair of relatively prime integers (a, b), either*

(a,b) or $(-a,-b)$ occurs as one of the columns of some element of Δ. Then the following are equivalent:

(I) $\widehat{G}$ is isomorphic either to a subgroup of $\mathbb{Q}$ or a subgroup of $\mathbb{Q}/\mathbb{Z}$;

(II) If μ is a measure on $G \times G$ such that $\gamma\mu$ is doubly stochastic for all $\gamma \in \Delta$, then μ is Haar measure on $G \times G$. ∎

There are subgroups Δ of arbitrarily large index in $SL_2(\mathbb{Z})$ satsifying the hypothesis of this theorem. For example, fix a prime p and consider the subgroup $\Gamma_0(p)$ of $SL_2(\mathbb{Z})$ consisting of elements $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ where p divides c. The index of $\Gamma_0(p)$ is p^2. Given a relatively prime pair (a,b), find a matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ in $SL_2(\mathbb{Z})$. The other elements of $SL_2(\mathbb{Z})$ whose first row is (a,b) are $\begin{bmatrix} a & b \\ c+ka & d+kb \end{bmatrix}$. If a is not divisible by p, then we can choose k so that $c + ka$ is divisible by p. If a is divisible by p, then $\begin{bmatrix} -c & -d \\ a & b \end{bmatrix} \in \Gamma_0(p)$.

When the compact abelian group G has a measure-preserving Borel isomorphism to the unit interval, we can interpret these results in the context of measures on $I \times I$ in a straightforward if perhaps unnatural way. If G is a prime cyclic group, then we recover the well-known theorem about matrices to which we alluded in the introduction.

Given a compact abelian group G and a subgroup Δ of the $SL_2(\mathbb{Z})$, the set of measures μ such that $\gamma\mu$ is stochastic in the first variable for every $\gamma \in \Delta$ forms a convex set, let us call it $\mathcal{M}_{G,\Delta}$. So one may consider the problems of constructing and classifying the extreme points in $\mathcal{M}_{G,\Delta}$, and of deciding the existence of elements of $\mathcal{M}_{G,\Delta}$ with prescribed support. Actually each closed convex set $\mathcal{M}_{G,\Delta}$ is finitely refutable in the sense of Section 1, so one may hope for extensions of the techniques of that section.

More generally, given a compact abelian group G, and closed subsets $S_1 \subset G \times G$ and $S_2 \subset \widehat{G} \times \widehat{G}$, one may consider the existence of probability measures μ supported on S with $\widehat{\mu}$, the Fourier transform of μ, supported on S_2. (If, for example, S_2 contains the identity but not the rest of the "axes" then such a μ is automatically doubly stochastic.) Questions of this sort relate to the uncertainty principles of quantum mechanics. These questions should even be of interest even in the case of finite groups G, in which case one is dealing with matrices.

References

BIRKHOFF, G. (1946). Tres observaciones sobre el algebra lineal, *Rev. Univ. Nac. Tucumán, Series A.* **5**, 147—151.

CUTLAND, N. (1988). *Nonstandard Analysis and its Applications*, Cambridge University Press.

FELDMAN, D. V. (1992). Extreme doubly stochastic measures with full support. *Proc. Amer. Math. Soc.* **114**, Number 4, 919–922.

KAMIŃSKI, A., MIKUSIŃSKI, P., SHERWOOD, H. and TAYLOR, M. D. (1988). Properties of a special class of doubly stochastic measures, *Aequationes Math.* **36**, 212–229.

LINDENSTRAUSS, J. (1965). A remark on extreme doubly stochastic measures, *Amer. Math. Monthly* **12**, 379–382.

LOSERT, V. (1982). Counter-examples to some conjectures about doubly stochastic measures, *Pacific J. Math.* **99**, 387–397.

LOVÁSZ, L. AND PLUMMER, M. D. (1986). *Matching Theory*, North-Holland.

SHERWOOD, H. and TAYLOR, M. D. (1988). Doubly stochastic measures with hairpin support, *Probab. Theory Related Fields* **78**, 617–626.

STRASSEN, V. (1965). Probability measures with given marginals, *Ann. Math. Statist.* **36**, 423–439.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF NEW HAMPSHIRE
DURHAM, NH 03824
dvf@math.unh.edu