*Functiones et Approximatio*
*60.2 (2019), 263–275*
*doi: 10.7169/facm/1755*

# A DIRICHLET APPROXIMATION THEOREM FOR GROUP ACTIONS

Clayton Petsche, Jeffrey D. Vaaler

**Abstract:** If $G$ is a compact group acting continuously on a compact metric space $(X, m)$, we prove two results that generalize Dirichlet's classical theorem on Diophantine approximation. If $G$ is a noncommutative compact group of isometries, we obtain a noncommutative form of Dirichlet's theorem. We apply our general result to the special case of the unitary group $U(N)$ acting on the complex unit sphere, and obtain a noncommutative result in this setting.

**Keywords:** unitary group, continuous group actions.

## 1. Introduction

Let $G$ be a compact topological group that acts continuously and faithfully on a compact metric space $\{X, m\}$. If $\mathcal{A} \subseteq G$ is a finite subset containing at least two points, we prove two results that establish the existence of a nonidentity element in the difference set

$$\left\{ab^{-1} : a \in \mathcal{A},\ b \in \mathcal{A},\ \text{and } a \neq b\right\}$$

that moves the points of $X$ minimally. In the special case of the group $G = (\mathbb{R}/\mathbb{Z})^N$ acting on $X = (\mathbb{R}/\mathbb{Z})^N$ by translation, our results reproduce Dirichlet's classical theorem on Diophantine approximation. If $G$ acts continuously as a group of isometries on $\{X, m\}$, we obtain a noncommutative form of Dirichlet's theorem.

Before developing the general setting in which we formulate our results, we consider the special case of the unitary group $G = U(N)$ of $N \times N$ unitary matrices. The group $U(N)$ acts continuously and faithfully on the set

$$X = \{\boldsymbol{x} \in \mathbb{C}^N : |\boldsymbol{x}|_2 = 1\}, \tag{1.1}$$

where

$$|\boldsymbol{x}|_2 = \left(|x_1|^2 + |x_2|^2 + \cdots + |x_N|^2\right)^{\frac{1}{2}}$$

This research was supported by NSA grant, H98230-12-1-0254.

**2010 Mathematics Subject Classification:** primary: 11J25; secondary: 37B05, 22F10

is the standard Hermitian norm on (column) vectors $\boldsymbol{x}$ in $\mathbb{C}^N$. If $\boldsymbol{x}$ and $\boldsymbol{y}$ are points of $X$, we use the metric $m$ given by

$$m(\boldsymbol{x}, \boldsymbol{y}) = |\boldsymbol{x} - \boldsymbol{y}|_2.$$

Then a unitary matrix $A$ in $U(N)$ acts on vectors $\boldsymbol{x}$ in $X$ by $(A, \boldsymbol{x}) \mapsto A\boldsymbol{x}$, and it is easy to verify that this action is an isometry. We define a function $\varphi : U(N) \to [0, \infty)$ by

$$\varphi(A) = \sup\big\{|A\boldsymbol{x} - \boldsymbol{x}|_2 : \boldsymbol{x} \in X\big\}, \tag{1.2}$$

so that $\varphi(A)$ measures the maximum distance that $A$ moves a point $\boldsymbol{x}$ in $X$. It is instructive to observe that the map $(A, B) \mapsto \varphi\big(AB^{-1}\big)$ defines a metric on the compact group $U(N)$, and this metric induces its group topology.

**Theorem 1.** *Let $\mathcal{A} \subseteq U(N)$ be a finite subset of cardinality $|\mathcal{A}| \geqslant 2$. If*

$$\delta(\mathcal{A}) = \min\big\{\varphi\big(AB^{-1}\big) : A \in \mathcal{A},\ B \in \mathcal{A},\ \text{and } A \neq B\big\}, \tag{1.3}$$

*then we have*

$$\delta(\mathcal{A}) \leqslant 2\pi|\mathcal{A}|^{-1/N^2}. \tag{1.4}$$

As an application of Theorem 1, we obtain the following noncommutative form of Dirichlet's theorem.

**Theorem 2.** *Let $A$ and $B$ be matrices in the unitary group $U(N)$, and let $J$ and $K$ be positive integers. If*

$$\delta_{J,K}(A, B) = \min\big\{\varphi\big(A^j B^k\big) : |j| \leqslant J,\ |k| \leqslant K,\ \text{and } (j, k) \neq (0, 0)\big\}, \tag{1.5}$$

*then*

$$\delta_{J,K}(A, B) \leqslant 2\pi(J + 1)^{-1/N^2}(K + 1)^{-1/N^2}. \tag{1.6}$$

If $A$, $B$, and $C$, are three matrices in $U(N)$, and $J$, $K$, and $L$ are positive integers, we can form the nonnegative number

$$\delta_{J,K,L}(A, B, C) = \min\big\{\varphi\big(A^j B^k C^\ell\big) : |j| \leqslant J,\ |k| \leqslant K,\ |\ell| \leqslant L, \\ \text{and } (j, k, \ell) \neq (0, 0, 0)\big\}.$$

It would be of interest to give an upper bound for this quantity that is analogous to (1.6). But such a generalization is not obvious using the methods developed here.

In Section 2 we describe the setting in which we prove our general results. This will be familiar to researchers on continuous group actions. We include it mainly for convenience and to establish notation. In Section 3 we prove our general form of Dirichlet's theorem stated as Theorem 3. And in Section 4 we prove a noncommutative version of this result which we state as Theorem 4. In Section 5 we show that Theorem 3 does in fact reproduce Dirichlet's classical theorem in Diophantine approximation when $G = (\mathbb{R}/\mathbb{Z})^N$ acts on $X = (\mathbb{R}/\mathbb{Z})^N$ by translation. The final section contains proofs of Theorem 1 and Theorem 2 for the unitary group.

## 2. Continuous actions of compact groups

Let $G$ be a compact topological group and write $e$ for the identity element in $G$. Let $\{X, m\}$ be a compact metric space, and assume that $G \times X \to X$ is a faithful, continuous action of $G$ on $X$, which we denote by $(g, x) \mapsto gx$. As the maps $(g, x) \mapsto gx$ and $(g, x) \mapsto x$ are both continuous, it follows that $(g, x) \mapsto (gx, x)$ is a continuous map from $G \times X$ into $X \times X$. Then

$$(g, x) \mapsto m(gx, x)$$

is a continuous map from $G \times X$ into $[0, \infty)$. Since $X$ is compact,

$$\varphi(g) = \sup\{m(gx, x) : x \in X\} \tag{2.1}$$

is finite, and therefore (2.1) defines a map $\varphi : G \to [0, \infty)$. The map $\varphi$ will play a basic role in this work.

We derive some elementary properties of the map $\varphi$. If $g$ and $h$ are in $G$, we have

$$\varphi(g^{-1}) = \sup\{m(g^{-1}x, x) : x \in X\} = \sup\{m(x, gx) : x \in X\} = \varphi(g), \tag{2.2}$$

and

$$\begin{aligned} \varphi(gh^{-1}) &= \sup\{m(gh^{-1}x, x) : x \in X\} \\ &= \sup\{m(gx, hx) : x \in X\} \\ &\leqslant \sup\{m(gx, x) + m(x, hx) : x \in X\} \\ &\leqslant \sup\{m(gx, x) : x \in X\} + \sup\{m(y, hy) : y \in X\} \\ &= \varphi(g) + \varphi(h). \end{aligned} \tag{2.3}$$

If the metric $m$ is nonarchimedean, that is, if $m$ satisfies the strong triangle inequality

$$m(x, y) \leqslant \max\{m(x, z), m(z, y)\}$$

for all $x$, $y$, and $z$ in $X$, then we get the corresponding nonarchimedean inequality

$$\varphi(gh^{-1}) \leqslant \max\{\varphi(g), \varphi(h)\}. \tag{2.4}$$

Using (2.2) and (2.3) we find that

$$\varphi(g) = \varphi(gh^{-1}h) \leqslant \varphi(gh^{-1}) + \varphi(h),$$

and similarly

$$\varphi(h) = \varphi(hg^{-1}g) \leqslant \varphi(hg^{-1}) + \varphi(g) = \varphi(gh^{-1}) + \varphi(g).$$

Hence we get

$$\big|\varphi(g) - \varphi(h)\big| \leqslant \varphi(gh^{-1}). \tag{2.5}$$

Let $\rho : G \times G \to [0, \infty)$ be defined by $\rho(g, h) = \varphi(gh^{-1})$. Because $G$ acts faithfully, $\rho(g, h) = 0$ if and only if $g = h$. The identity (2.2) shows that $\rho(g, h) = \rho(h, g)$. If $g$, $h$ and $k$ are elements of $G$ then using (2.3) we get

$$\rho(g, h) = \varphi\big(gk^{-1}(hk^{-1})^{-1}\big) \leqslant \varphi(gk^{-1}) + \varphi(hk^{-1}) = \rho(g, k) + \rho(k, h).$$

This shows that $\rho$ is a metric on $G$ that is induced by the metric $m$ on $X$. If $m$ is nonarchimedean, then it follows using (2.4) that $\rho$ is also nonarchimedean.

Of course, the metric $\rho$ does not necessarily induce the group topology in $G$. We would like to work in a situation where $\rho$ induces a metric topology in which every $\rho$-open set is also open in the group topology of $G$. That is, $\rho$ induces a topology in $G$ that is weaker than the group topology. In order for this to happen it is necessary and sufficient that $\varphi$ be a continuous map. This follows from the following general principle.

**Lemma 1.** *Assume that $Y$ is a locally compact Hausdorff space, $Z$ is a compact Hausdorff space, and $f : Y \times Z \to \mathbb{R}$ is a continuous map. Then the function $g : Y \to \mathbb{R}$ defined by*

$$g(y) = \sup\{f(y, z) : z \in Z\}$$

*is continuous.*

**Proof.** Let $y$ be a point in $Y$. By local compactness there exists an open neighborhood $U$ of $y$ and a compact set $K$ such that $U \subseteq K \subseteq Y$. Then it suffices to show that the restriction of $g$ to $K$ is continuous.

Let $\epsilon > 0$ and for each point $(k, z)$ in $K \times Z$ let

$$B(k, z) = \{(\alpha, \beta) \in K \times Z : |f(k, z) - f(\alpha, \beta)| < \epsilon\}.$$

Then $B(k, z)$ is an open neighborhood of $(k, z)$. Let $U(k)$ be an open neighborhood of $k$ and let $V(z)$ be an open neighborhood of $z$ such that $U(k) \times V(z) \subseteq B(k, z)$. The collection of open sets

$$\big\{U(k) \times V(z) : (k, z) \in K \times Z\big\}$$

covers the compact space $K \times Z$, and so there exists a finite subcover

$$\big\{U(k_n) \times V(z_n) : (k_n, z_n) \in K \times Z \text{ and } n = 1, 2, \ldots, N\big\}.$$

Define a continuous function $h : K \to \mathbb{R}$ by

$$h(k) = \max\{f(k, z_n) : n = 1, 2, \ldots, N\}.$$

Since $Z$ is compact, at each point $k$ in $K$ there exists a point $\zeta = \zeta(k)$ in $Z$ such that $g(k) = f(k, \zeta)$. Then there exists an integer $m$ with $1 \leqslant m \leqslant N$ such that $(k, \zeta)$ belongs to $U(k_m) \times V(z_m)$. It follows that

$$\begin{aligned} 0 &\leqslant g(k) - h(k) \\ &\leqslant f(k, \zeta) - f(k, z_m) \\ &\leqslant |f(k, \zeta) - f(k_m, z_m)| + |f(k_m, z_m) - f(k, z_m)| < 2\epsilon. \end{aligned}$$

Since $h$ is continuous and $\epsilon > 0$ is arbitrary, it follows that $g$ restricted to $K$ is continuous. ∎

**Corollary 1.** *The map $\varphi : G \to [0, \infty)$ defined by* (2.1) *is continuous.*

**Proof.** In Lemma 1, take the map $f : G \times X \to [0, \infty)$ given by $f(g, x) = m(gx, x)$. ∎

Our assumption that the $G$-action on $X$ is faithful is not restrictive. Indeed, if the action were not faithful, then we could replace $G$ by $G/K$, where

$$K = \{g \in G : \varphi(g) = 0\},$$

which is easily seen to be a closed, normal subgroup of $G$. Indeed, $k$ is in $K$ if and only if $kx = x$ for all $x$ in $X$. If $g$ is in $G$ and $k$ is in $K$ then

$$m(gkg^{-1}x, x) = m(gg^{-1}x, x) = m(x, x) = 0,$$

and therefore $K$ is normal in $G$. If $gh^{-1}$ belongs to $K$ then (2.5) implies that $\varphi(g) = \varphi(h)$. In particular, $\varphi$ is constant on each coset $hK$. Thus $\varphi$ induces a map $\overline{\varphi} : G/K \to [0, \infty)$ by defining $\overline{\varphi}(hK) = \varphi(h)$, and $G/K$ acts faithfully on $X$.

## 3. A generalization of Dirichlet's theorem

Let $\mu$ denote a Haar measure on the Borel subsets of $G$ normalized so that $\mu(G) = 1$. We recall that for a compact group the Haar measure $\mu$ is both left and right invariant. That is, if $E \subseteq G$ is a Borel set and $g$ is in $G$, then $\mu(E) = \mu(gE) = \mu(Eg)$. For $0 \leqslant t$ we define the distribution function

$$\Phi(t) = \mu\{g \in G : \varphi(g) < t\}. \tag{3.1}$$

Clearly $\Phi(0) = 0$, and $t \mapsto \Phi(t)$ is nondecreasing. If $0 < t$ then

$$\{g \in G : \varphi(g) < t\}$$

is a nonempty open set, and therefore it has positive Haar measure. If $\lim_{t \to 0+} \varphi(t) > 0$ then it follows that $\{e\}$ is an open set and $G$ has the discrete topology. As $G$ is assumed to be compact, we find that $G$ is finite in this case.

Next we prove the following result which is inspired by Blichfeldt's theorem [1] in the geometry of numbers (see also [3, Chapter III.2, Theorem I].)

**Theorem 3.** *Let $\mathcal{A} \subseteq G$ be a finite, nonempty set. Write $|\mathcal{A}|$ for the cardinality of $\mathcal{A}$, and define*

$$\delta(\mathcal{A}) = \min\{\varphi(ab^{-1}) : a \in \mathcal{A},\ b \in \mathcal{A},\ \text{and } a \neq b\}. \tag{3.2}$$

*Then we have*

$$\Phi\big(\tfrac{1}{2}\delta(\mathcal{A})\big) \leqslant |\mathcal{A}|^{-1}. \tag{3.3}$$

*If the metric $m$ is nonarchimedean then*

$$\Phi\big(\delta(\mathcal{A})\big) \leqslant |\mathcal{A}|^{-1}. \tag{3.4}$$

**Proof.** As $\varphi(g) = 0$ if and only if $g = e$, we may assume that $\delta(\mathcal{A})$ is positive. Let $V \subseteq G$ be the nonempty open set

$$V = \big\{g \in G : \varphi(g) < \tfrac{1}{2}\delta(\mathcal{A})\big\}.$$

For each point $a$ in $\mathcal{A}$ we have

$$Va = \big\{ga \in G : \varphi(g) < \tfrac{1}{2}\delta(\mathcal{A})\big\} = \big\{g \in G : \varphi(ga^{-1}) < \tfrac{1}{2}\delta(\mathcal{A})\big\}. \tag{3.5}$$

Assume that $a$ and $b$ are distinct points in $\mathcal{A}$ such that $Va \cap Vb$ contains a point $h$. In view of (3.5) we have

$$\varphi(ha^{-1}) < \tfrac{1}{2}\delta(\mathcal{A}) \qquad \text{and} \qquad \varphi(hb^{-1}) < \tfrac{1}{2}\delta(\mathcal{A}).$$

Using (2.2) and (2.3) we also get

$$\begin{aligned}\varphi(ab^{-1}) &= \varphi(ah^{-1}hb^{-1}) \\ &\leqslant \varphi(ha^{-1}) + \varphi(hb^{-1}) \\ &< \tfrac{1}{2}\delta(\mathcal{A}) + \tfrac{1}{2}\delta(\mathcal{A}),\end{aligned}$$

which is impossible. It follows that the subsets $Va$ with $a \in \mathcal{A}$ are disjoint. Using the right translation invariance of Haar measure we find that

$$\sum_{a \in \mathcal{A}} \mu(Va) = |\mathcal{A}|\mu(V) = |\mathcal{A}|\Phi\big(\tfrac{1}{2}\delta(\mathcal{A})\big) \leqslant 1,$$

and this verifies (3.3).

If $m$ is nonarchimedean then $\varphi$ also satisfies the nonarchimedean inequality (2.4). Arguing as before, we are led to the inequality (3.4). ∎

**Corollary 2.** *Let $a$ be an element of the compact group $G$ and define*

$$\delta_N(a) = \min\{\varphi(a^n) : 1 \leqslant n \leqslant N\}. \tag{3.6}$$

*Then we have*

$$\Phi\big(\tfrac{1}{2}\delta(a)\big) \leqslant (N+1)^{-1}. \tag{3.7}$$

*If $m$ is nonarchimedean then*

$$\Phi\big(\delta(a)\big) \leqslant (N+1)^{-1}. \tag{3.8}$$

**Proof.** Apply the Theorem with $\mathcal{A} = \{a^n : n = 0, 1, 2, \ldots, N\}$, and use the fact that $\varphi(a^{-n}) = \varphi(a^n)$. ∎

Given an element $a \in G$ of infinite order, we could also consider the closure $H$ of $\langle a \rangle$ in $G$, which is a compact subgroup ([5], 6.26). Then we can apply the above corollary to $H$. Of course, the normalized Haar measure on $H$ is not necessarily the restriction to $H$ of a Haar measure on $G$.

## 4. $G$ is a group of isometries

Using the metric $m$ on $X$, we may define the closed subgroup

$$I = \{g \in G : m(gx, gy) = m(x, y) \text{ for all } (x, y) \in X \times X\} \tag{4.1}$$

of all isometries in $G$. If $g$ and $h$ are elements of $G$ which do not commute, then in general we do not expect to have $\varphi(gh) = \varphi(hg)$. However, if either $g$ or $h$ is an element of the closed subgroup $I$ of all isometries in $G$, then we do have

$$\varphi(gh) = \varphi(hg). \tag{4.2}$$

For example, if $g$ is an isometry then

$$\begin{aligned} \varphi(gh) &= \sup\{m(ghx, x) : x \in X\} \\ &= \sup\{m(ghx, gg^{-1}x) : x \in X\} \\ &= \sup\{m(hx, g^{-1}x) : x \in X\} \\ &= \sup\{m(hgx, x) : x \in X\} \\ &= \varphi(hg). \end{aligned} \tag{4.3}$$

Alternatively, if $g$ is an isometry then

$$\varphi(ghg^{-1}) = \varphi(h) \tag{4.4}$$

for all $h$ in $G$. In particular, if $G = I$ is a group of isometries, then $\varphi : G \to [0, \infty)$ is constant on conjugacy classes. In this case we may derive the following noncommutative form of Dirichlet's theorem on Diophantine approximation.

**Theorem 4.** *Assume that $G = I$, and let $a$ and $b$ belong to $G$. For positive integers $M$ and $N$ define*

$$\delta_{M,N}(a, b) = \min\big\{\varphi\big(a^m b^n\big) : |m| \leqslant M, |n| \leqslant N, \text{ and } (m, n) \neq (0, 0)\big\}. \tag{4.5}$$

*Then we have*

$$\Phi\big(\tfrac{1}{2}\delta_{M,N}(a, b)\big) \leqslant (M + 1)^{-1}(N + 1)^{-1}. \tag{4.6}$$

*If the metric $m$ is nonarchimedean, then*

$$\Phi\big(\delta_{M,N}(a, b)\big) \leqslant (M + 1)^{-1}(N + 1)^{-1}. \tag{4.7}$$

**Proof.** If there exist integers $k$ and $l$, not both zero, such that $|k| \leqslant M$, $|l| \leqslant N$ and $a^k b^l = e$, then we have $\delta_{M,N}(a, b) = 0$ and the result is obvious. Therefore we define

$$\mathcal{A} = \{a^k b^l : 0 \leqslant k \leqslant M \text{ and } 0 \leqslant l \leqslant N\},$$

and we assume that $|\mathcal{A}| = (M+1)(N+1)$. If $a^{k_1} b^{l_1}$ and $a^{k_2} b^{l_2}$ are distinct elements of $\mathcal{A}$ then, making use of (4.2), we have

$$\begin{aligned} \varphi\big(a^{k_1} b^{l_1} \big(a^{k_2} b^{l_2}\big)^{-1}\big) &= \varphi\big(a^{k_1} b^{l_1 - l_2} a^{-k_2}\big) \\ &= \varphi\big(a^{k_1 - k_2} b^{l_1 - l_2}\big). \end{aligned}$$

This shows that $\delta_{M,N}(a, b)$ as defined by (4.5) is equal to $\delta(\mathcal{A})$ as defined by (3.2). Hence the inequalities (4.6) and (4.7) both follow from Theorem 3. ∎

## 5. The classical case of Dirichlet's Theorem

Let $\| \ \| : \mathbb{R} \to [0, \frac{1}{2}]$ be defined by

$$\|x\| = \min\{|x - n| : n \in \mathbb{Z}\},$$

so that $\|x\|$ is the distance from the real number $x$ to the nearest integer. Clearly $x \mapsto \|x\|$ is constant on each coset of the quotient group $\mathbb{R}/\mathbb{Z}$, and so we have $\| \ \| : \mathbb{R}/\mathbb{Z} \to [0, \frac{1}{2}]$. Then $(x, y) \mapsto \|x - y\|$ is a metric on $\mathbb{R}/\mathbb{Z}$ which induces its quotient topology. More generally,

$$(\boldsymbol{x}, \boldsymbol{y}) \mapsto \max\{\|x_l - y_l\| : 1 \leqslant l \leqslant L\} \tag{5.1}$$

is a metric on the product $(\mathbb{R}/\mathbb{Z})^L$ which induces its product topology.

Now suppose that $G = (\mathbb{R}/\mathbb{Z})^L$. Let $X = (\mathbb{R}/\mathbb{Z})^L$ with metric defined by (5.1), and let $G$ act on $X$ by translation. Here the group is naturally written using additive notation, so that the action is given by $(\boldsymbol{g}, \boldsymbol{x}) \mapsto \boldsymbol{g} + \boldsymbol{x}$. It is trivial that this action is continuous. In this case we find that

$$\begin{aligned} \varphi(\boldsymbol{g}) &= \sup\big\{ \max\{\|g_l + x_l - x_l\|; 1 \leqslant l \leqslant L\} : \boldsymbol{x} \in X\big\} \\ &= \max\{\|g_l\| : 1 \leqslant l \leqslant L\}. \end{aligned} \tag{5.2}$$

And for $0 \leqslant t \leqslant \frac{1}{2}$ we get

$$\Phi(t) = \mu\{\boldsymbol{g} \in G : \varphi(\boldsymbol{g}) < t\} = (2t)^L. \tag{5.3}$$

Let $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_M$ be nonzero points in $G$, and let $K_1, K_2, \dots, K_M$ be positive integers. Then define

$$\mathcal{A} = \big\{k_1\boldsymbol{\alpha}_1 + k_2\boldsymbol{\alpha}_2 + \cdots + k_M\boldsymbol{\alpha}_M : 0 \leqslant k_m \leqslant K_m\big\}.$$

If

$$|\mathcal{A}| < \prod_{m=1}^{M} (K_m + 1),$$

then it is trivial that there exists a nonzero integer vector $\boldsymbol{j}$ in $\mathbb{Z}^M$ such that

$$j_1\boldsymbol{\alpha}_1 + j_2\boldsymbol{\alpha}_2 + \cdots + j_M\boldsymbol{\alpha}_M = \boldsymbol{0},$$

and $|j_m| \leqslant K_m$ for each $m = 1, 2, \dots, M$. Thus we assume that

$$|\mathcal{A}| = \prod_{m=1}^{M} (K_m + 1).$$

As in the statement of Theorem 3, let

$$\delta(\mathcal{A}) = \min\big\{\varphi(j_1\boldsymbol{\alpha}_1 + j_2\boldsymbol{\alpha}_2 + \cdots + j_M\boldsymbol{\alpha}_M) : \boldsymbol{j} \neq \boldsymbol{0}, \text{ and } |j_m| \leqslant K_m + 1\big\}.$$

Then the inequality (3.3) and (5.3) imply that

$$\delta(\mathcal{A})^L \leqslant \prod_{m=1}^{M} (K_m + 1)^{-1}. \tag{5.4}$$

This is a slight generalization of Theorem VI in [2, Chapter 1], and includes Dirichlet's basic theorem on Diophantine approximation.

## 6. Proof of Theorem 1 and Theorem 2

Throughout this section we write $\mu$ for Haar measure on the Borel subsets of the unitary group $U(N)$ normalized so that $\mu\big(U(N)\big) = 1$. We let $X$ denote the surface (1.1) of the complex unit ball, and let

$$\varphi : U(N) \to [0, 2]$$

denote the function defined by (1.2). We write

$$\Phi(t) = \mu\big\{A \in U(N) : \varphi(A) < t\big\} \tag{6.1}$$

for the corresponding distribution function.

**Lemma 2.** *Let $A$ be a matrix in the group $U(N)$. If*

$$\{\alpha_n : n = 1, 2, \ldots, N\} \subseteq \mathbb{T}$$

*are the eigenvalues of $A$, then*

$$\varphi(A)^2 = 2 - 2\min\{\Re(\alpha_n) : n = 1, 2, \ldots, N\}. \tag{6.2}$$

**Proof.** At each (column) vector $\boldsymbol{x}$ in $X$, we have $|\boldsymbol{x}|_2 = |A\boldsymbol{x}|_2 = 1$. It follows that

$$|A\boldsymbol{x} - \boldsymbol{x}|_2^2 = \langle A\boldsymbol{x} - \boldsymbol{x}, A\boldsymbol{x} - \boldsymbol{x}\rangle = 2 - \boldsymbol{x}^*(A^* + A)\boldsymbol{x},$$

where $\boldsymbol{x}^*$ is the complex conjugate transpose of $\boldsymbol{x}$, and similarly for $A^*$. The matrix $A^* + A$ is self-adjoint. Therefore, by the spectral theorem, there exists an $N \times N$ unitary matrix $V$, and an $N \times N$ real diagonal matrix $D$, such that

$$A^* + A = V^* D V, \qquad \text{and} \qquad D = [\omega_n],$$

where

$$\{\omega_n : n = 1, 2, \ldots, N\} = \{2\Re(\alpha_n) : n = 1, 2, \ldots, N\}$$

are the eigenvalues of $A^* + A$. Setting $\boldsymbol{y} = V\boldsymbol{x}$ we find that $|\boldsymbol{y}|_2^2 = |\boldsymbol{x}|_2^2 = 1$, and

$$\begin{aligned} |A\boldsymbol{x} - \boldsymbol{x}|_2^2 &= 2 - \boldsymbol{y}^* D \boldsymbol{y} \\ &= 2 - \sum_{n=1}^{N} \omega_n |y_n|^2 \\ &\leqslant 2 - 2\min\{\Re(\alpha_n) : n = 1, 2, \ldots, N\}. \end{aligned} \tag{6.3}$$

If

$$\omega_m = \min\{\omega_n : n = 1, 2, \dots, N\},$$

then there is equality in the inequality (6.3) when $\boldsymbol{y} = \boldsymbol{e}_m$ is the $m$th standard basis vector. As the vector $V^*\boldsymbol{e}_m$ belongs to $X$, the identity (6.2) follows. ∎

If $z$ is a complex number we write $e(z) = e^{2\pi i z}$.

**Lemma 3.** *Let $w$, $x$ and $y$ be real numbers such that $|w| \leqslant \frac{1}{2}$, $|x| \leqslant \frac{1}{2}$, and $|y| \leqslant \frac{1}{2}$. Then we have*

$$(2w)^2\big|e(x) - e(y)\big|^2 \leqslant \big|e(2wx) - e(2wy)\big|^2. \tag{6.4}$$

**Proof.** If $u$ and $v$ are real numbers such that $0 \leqslant |u| \leqslant |v| \leqslant 1$, then it follows from the convergent infinite product

$$\left(\frac{\sin \pi z}{\pi z}\right) = \prod_{n=1}^{\infty}\left(1 - \frac{z^2}{n^2}\right), \tag{6.5}$$

that

$$0 \leqslant \left(\frac{\sin \pi v}{\pi v}\right) \leqslant \left(\frac{\sin \pi u}{\pi u}\right).$$

By hypothesis,

$$0 \leqslant |2wx - 2wy| \leqslant |x - y| \leqslant 1.$$

Therefore we get

$$0 \leqslant \left(\frac{\sin \pi(x-y)}{\pi(x-y)}\right) \leqslant \left(\frac{\sin \pi(2wx - 2wy)}{\pi(2wx - 2wy)}\right),$$

and

$$(2w)^2\big(\sin \pi(x-y)\big)^2 \leqslant \big(\sin \pi(2wx - 2wy)\big)^2. \tag{6.6}$$

Then (6.6) is equivalent to (6.4). ∎

**Lemma 4.** *If $0 < t \leqslant 2$ then the distribution function $\Phi$ defined by* (6.1)*, satisfies the inequality*

$$\left(\frac{t}{\pi}\right)^{N^2} \leqslant \Phi(t). \tag{6.7}$$

**Proof.** Let $\boldsymbol{x}$ be a (column) vector in $\mathbb{R}^N$ with coordinates $x_1, x_2, \dots, x_N$, and let $E : \mathbb{R}^N \to \mathbb{C}$ be defined by the Vandermonde determinant

$$E(\boldsymbol{x}) = \det\big(e\big((n-1)x_m\big)\big) = \prod_{1 \leqslant m < n \leqslant N}\big(e(x_n) - e(x_m)\big).$$

As each function $x \mapsto e(x)$ is periodic with period 1, the function $E$ is well defined on the compact quotient group $(\mathbb{R}/\mathbb{Z})^N$. Let $\nu$ denote Haar measure on $(\mathbb{R}/\mathbb{Z})^N$

normalized so that $\nu\big((\mathbb{R}/\mathbb{Z})^N\big) = 1$. Using the determinant representation for $E(\boldsymbol{x})$, we get the Fourier expansion

$$E(\boldsymbol{x}) = \sum_{\sigma \in S_N} \operatorname{sgn}(\sigma) \prod_{m=1}^{N} e\big((\sigma(m) - 1)x_m\big),$$

where the sum is over the collection of all permutations

$$\sigma : \{1, 2, \ldots, N\} \to \{1, 2, \ldots, N\}$$

in the symmetric group $S_N$. Then using Parseval's identity we find that

$$\frac{1}{N!} \int_{(\mathbb{R}/\mathbb{Z})^N} |E(\boldsymbol{x})|^2 \, \mathrm{d}\nu(\boldsymbol{x}) = 1. \tag{6.8}$$

Let $F : U(N) \to \mathbb{C}$ be an integrable function with respect to the Haar measure $\mu$. Assume that $F$ is constant on conjugacy classes, so that

$$F\big(B^{-1}AB\big) = F(A)$$

for all $A$ and $B$ in $U(N)$. We recall that $F$ is constant on conjugacy classes if and only if $F(A)$ depends only on the eigenvalues of $A$. Let $A$ be a matrix in $U(N)$ with eigenvalues

$$\{\alpha_n : n = 1, 2, \ldots, N\} \subseteq \mathbb{T}.$$

Let $\boldsymbol{x} = (x_n)$ be the unique point in $(\mathbb{R}/\mathbb{Z})^N$ such that $\alpha_n = e(x_n)$. If $F : U(N) \to \mathbb{C}$ is constant on conjugacy classes, then $F$ induces a function $\widetilde{F} : (\mathbb{R}/\mathbb{Z})^N \to \mathbb{C}$, by $F(A) = \widetilde{F}(\boldsymbol{x})$. Moveover, the function $\widetilde{F}$ is integrable with respect to Haar measure $\nu$, and by the Weyl integration formula (see [4, Chapter 5]) we have

$$\int_{U(N)} F(A) \, \mathrm{d}\mu(A) = \frac{1}{N!} \int_{(\mathbb{R}/\mathbb{Z})^N} \widetilde{F}(\boldsymbol{x}) |E(\boldsymbol{x})|^2 \, \mathrm{d}\nu(\boldsymbol{x}). \tag{6.9}$$

Again let $A$ be a matrix in $U(N)$ with eigenvalues

$$\{\alpha_n : n = 1, 2, \ldots, N\} \subseteq \mathbb{T},$$

and let $\boldsymbol{x} = (x_n)$ be the point in $(\mathbb{R}/\mathbb{Z})^N$ such that $\alpha_n = e(x_n)$. By Lemma 2 the inequality $\varphi(A) < t$ holds if and only if

$$1 - \tfrac{1}{2}t^2 < \Re(\alpha_n) = \cos 2\pi x_n$$

for each $n = 1, 2, \ldots, N$. Therefore, if

$$K(t) = \big\{\boldsymbol{x} \in (\mathbb{R}/\mathbb{Z})^N : 1 - \tfrac{1}{2}t^2 < \cos 2\pi x_n\big\},$$

then by Lemma 2 and the Weyl integration formula (6.9), we have

$$\Phi(t) = \mu\big\{A \in U(N) : \varphi(A) < t\big\} = \frac{1}{N!} \int_{K(t)} |E(\boldsymbol{x})|^2 \, \mathrm{d}\nu(\boldsymbol{x}).$$

Alternatively, let $w$ be the unique real number such that $0 < w \leqslant \frac{1}{2}$,

$$1 - \tfrac{1}{2}t^2 = \cos 2\pi w, \qquad \text{and} \qquad t = 2\sin \pi w.$$

We will use the unit cube

$$C_N = \{\boldsymbol{y} \in \mathbb{R}^N : |y_n| \leqslant \tfrac{1}{2}\}$$

as a fundamental domain for the quotient group $(\mathbb{R}/\mathbb{Z})^N$. Then we have

$$K(t) \cap C_N = \big\{\boldsymbol{y} \in \mathbb{R}^N : |y_n| < w\big\},$$

and

$$\Phi(t) = \frac{1}{N!} \int_{\{\boldsymbol{y}:|y_n|<w\}} |E(\boldsymbol{y})|^2 \, \mathrm{d}\boldsymbol{y}. \tag{6.10}$$

The inequality (6.4), implies that

$$\begin{aligned} (2w)^{N^2-N}|E(\boldsymbol{y})|^2 &= \prod_{1\leqslant m<n\leqslant N} (2w)^2\big|e(y_n) - e(y_m)\big|^2 \\ &\leqslant \prod_{1\leqslant m<n\leqslant N} \big|e(2wy_n) - e(2wy_m)\big|^2 \\ &= E(2w\boldsymbol{y}) \end{aligned} \tag{6.11}$$

at each point $\boldsymbol{y}$ in $C_N$. It follows that

$$\begin{aligned} (2w)^{N^2} &= \frac{(2w)^N}{N!} \int_{C_N} (2w)^{N^2-N}|E(\boldsymbol{y})|^2 \, \mathrm{d}\boldsymbol{y} \\ &\leqslant \frac{(2w)^N}{N!} \int_{C_N} |E(2w\boldsymbol{y})|^2 \, \mathrm{d}\boldsymbol{y} \\ &= \frac{1}{N!} \int_{\{\boldsymbol{x}:|x_n|<w\}} |E(\boldsymbol{x})|^2 \, \mathrm{d}\boldsymbol{x} \\ &= \Phi(t). \end{aligned} \tag{6.12}$$

To complete the proof we use the elementary inequality

$$t = 2\sin \pi w \leqslant 2\pi w. \tag{6.13}$$

The inequality (6.7) plainly follows from (6.12) and (6.13). ∎

Let $\mathcal{A} \subseteq U(N)$ be a finite, nonempty subset of cardinality $|\mathcal{A}| \geqslant 2$. Combining the inequalities (3.3) and (6.7), we conclude that

$$\left(\frac{\delta(\mathcal{A})}{2\pi}\right)^{N^2} \leqslant \Phi\big(\tfrac{1}{2}\delta(\mathcal{A})\big) \leqslant |\mathcal{A}|^{-1},$$

and this verifies Theorem 1.

Similarly, let $A$ and $B$ be elements of $U(N)$, and let $\delta_{J,K}(A,B)$ be defined by (1.5). Then (4.7) implies that

$$\left(\frac{\delta_{J,K}(A,B)}{2\pi}\right)^{N^2} \leqslant (J+1)^{-1}(K+1)^{-1},$$

and this proves the inequality (1.6) in the statement of Theorem 2.

## References

[1] H. F. Blichfeldt, *A new principle in the geometry of numbers with some applications*, Trans. Amer. Math. Soc. **15** (1914), 227–235.

[2] J. W. S. Cassels, *An Introduction to Diophantine Approximation*, Cambridge Tracts No. 45, Cambridge U. Press, 1965.

[3] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, Springer, New York, 1971.

[4] N. M. Katz and P. Sarnak, *Random Matrices, Frobenius Eigenvalues, and Monodromy,* AMS Colloquium Publications, Vol. 45, AMS Providence, RI, 1999.

[5] M. Stroppel, *Locally Compact Groups*, EMS Textbooks in Mathematics, European Mathematical Society (EMS), Zürich, 2006.

**Addresses:** C. Petsche: Department of Mathematics, Oregon State University, Corvallis, Oregon 97331 USA;
J. D. Vaaler: Department of Mathematics, University of Texas, Austin, Texas 78712 USA.

**E-mail:** petschec@math.oregonstate.edu, vaaler@math.utexas.edu

**Received:** 28 April 2017; **revised:** 12 June 2018