ON SQUARE ROOTS OF THE UNIFORM DISTRIBUTION ON COMPACT GROUPS

PERSI DIACONIS AND MEHRDAD SHAHSHAHANI

Abstract. Let $G$ be a compact separable topological group. When does there exist a probability $P$ such that $P \ast P = U$, where $U$ is Haar measure and $P \neq U$? We show that such square roots exist if and only if $G$ is not abelian, nor the product of the quaternions and a product of two element groups. In the course of proving this we classify compact groups with the property that every closed subgroup is normal.

1. Introduction. Let $G$ be a compact separable topological group. When does there exist a probability $P$ such that $P \ast P = U$ where $U$ is Haar measure and $P \neq U$? Our main result is

Theorem 1. There is a probability $P$ such that $P \ast P = U$ if and only if $G$ is a nonabelian group which is not isomorphic to a product $H \times E$ with $H$ the eight element group of quaternions and $E$ a product of two element groups.

A proof of Theorem 1 appears in §2. The proof depends on the following result which is proved in §3.

Theorem 2. Let $G$ be a compact, separable group with the property that every closed subgroup is normal. Then $G = H \times E \times O$ where $H$ is the eight element group of quaternions, $E$ is a product of two element groups, and $O$ is a compact abelian group with Pontryagin dual a torsion group in which every element has odd order. The converse is also true.

Remark 1. Recall that a group is called Hamiltonian if every subgroup is normal. Dedekind and Baer characterized Hamiltonian groups as groups which can be represented as $H \times E \times \hat{O}$ with $H$ and $E$ as in Theorem 2, and $\hat{O}$ a torsion group in which every element has odd order. Thus there is a 1-1 correspondence between Hamiltonian groups with $E$ a countable product of two element groups and $O$ countable, and compact separable groups with every subgroup normal.

The countable torsion groups $\hat{O}$ can be classified by using results in Kaplansky (1952). First, any torsion group is a direct sum of primary groups, and $\hat{O}$ can have no 2-primary part. Then, Ulm's theorem gives a complete characterization of the other possible primary parts.
Remark 2. The problem studied here arose in a statistical context. One common method for generating uniform random variables on groups involves factoring the uniform distribution. Discussion and examples are in Chapter 4 of Diaconis (1982). Theorem 1 represents a first step in understanding such factorizations.

Theorem 1 is also related to problems of estimating the speed of convergence of random walks to Haar measure. Let $G$ be a finite group of cardinality $|G|$. For $P$ a probability on $G$, and $U$ the uniform distribution, define the variation distance between $P$ and $U$ as

$$\|P - U\| = \sum |P(g) - U(g)|.$$ 

Aldous and Diaconis have shown that for most probabilities $P$ (in the sense of the uniform distribution on the $|G|$ simplex) $\|P * P - U\| = o(1)$ as $|G|$ tends to infinity.

2. Proof of Theorem 1. We first introduce some notation and definitions. By a representation of a compact group $G$ we mean a continuous homomorphism $\rho$ of $G$ into the group of invertible linear operators on a complex vector space $V$ of dimension $d_\rho$. A representation $\rho$ is irreducible if the only proper invariant subspace of $V$ is $\{0\}$. Without loss of generality we assume throughout that all the irreducible representations are given by unitary matrices. For a representation $\rho$, its contragredient $\bar{\rho}$ is defined by

$$\bar{\rho}(g) = \rho(g^{-1})'$$

where $'$ denotes transpose. Then

$$\bar{\rho}(g) = \overline{\rho(g)}.$$ 

The Fourier transform of a measure $P$ on $G$ is defined by

$$\rho(P) = \int_G \rho(g) P(\text{d}g).$$ 

Similarly, one defines the Fourier transform of a continuous function $f$ on $G$. Then we have the Fourier inversion formula

$$f(g) = \sum_{\rho \in \hat{G}} d_\rho \text{Tr}(\rho(g)^* \rho(f)).$$

Where $*$ denotes transpose of complex conjugate, $\hat{G}$ is the set of irreducible representations of $G$, and Haar measure on $G$ is normalized so that $G$ has total mass 1.

On a compact abelian group the factorization $U = P * P$ is impossible unless $P = U$. This follows because all irreducible representations are one dimensional and, for nontrivial $\rho$,

$$0 = \rho(U) = \rho(P * P) = \rho(P)^2$$

implies $\rho(P) = 0$.

For nonabelian groups, the proof requires some preliminary lemmas.

Lemma 1. Let $\mu$ be a bounded measure on a compact group $G$. Then $\mu$ is real if and only if for every irreducible representation $\rho$ of $G$, $\bar{\rho}(\mu) = \overline{\rho(\mu)}$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Proof. If \( \mu \) is real, then

\[
\overline{\rho_{ij}(\mu)} = \int \overline{\rho_{ij}(g)} \, \mu(dg) = \overline{\rho_{ij}(\mu)}.
\]

Conversely, suppose \( \mu \) is a measure such that \( \rho(\mu) = \overline{\rho(\mu)} \). This means

\[
0 = \int \rho_{ij}(g) \, \mu(dg) = -\int \overline{\rho_{ij}(g)} \, \mu(dg)
\]

or

\[
0 = \int \rho_{ij}(g) \, \mu(dg) - \int \rho_{ij}(g) \, \mu(dg).
\]

Since this holds for every irreducible \( \rho \), the Peter-Weyl theorem implies that the set function \( \overline{\mu} - \mu \) is zero, so \( \mu \) is real. \( \square \)

Lemma 2. Let \( G \) be a compact noncommutative group. Then the following conditions are equivalent:

(a) There is a probability measure \( P \neq U \) such that \( P \ast P = U \).

(b) There is an irreducible (complex) representation \( \rho \) of \( G \) such that the algebra

\[
\mathcal{R}_\rho = \left\{ \sum_{g \in G} \mathbb{C} \rho(g) \right\}
\]

contains nilpotent elements.

Proof. If \( U = P \ast P \) then \( \rho(P)^2 = 0 \) and \( \rho(P) \neq 0 \) for some \( \rho \) because \( P \neq U \). It is easy to see that \( \rho(P) \in \mathcal{R}_\rho \) and so \( \mathcal{R}_\rho \) contains nilpotent elements. Conversely, let \( \gamma_1 \in \mathcal{R}_\rho \) be nilpotent. If \( \gamma_n = 0 \) and \( n \) is smallest such power, then set \( \gamma = \gamma_n^{-1} \). This is nonzero and \( \gamma^2 = 0 \). Define a continuous \( f \) on \( G \) as follows: Set for every irreducible representation \( \pi \) of \( G \)

\[
\begin{cases}
\pi(f) = 0 & \text{if } \pi \neq \rho \text{ or } \tilde{\rho}, \\
\rho(f) = \gamma, \\
\tilde{\rho}(f) = \overline{\gamma} & \text{if } \tilde{\rho} \text{ is not equivalent to } \rho.
\end{cases}
\]

This defines a nonzero continuous function by the Fourier inversion theorem. By Lemma 1, \( f \) is real. Notice that if \( \rho \) is equivalent to \( \tilde{\rho} \), say \( \tilde{\rho}(g) = \overline{\rho(g)} = T \rho(g) T^{-1} \) (\( T \) is unitary), then

\[
\tilde{\rho}(f) = T \rho(f) T^{-1} = \sum c_g \overline{\rho(g)} = \overline{\gamma}
\]

and the hypothesis of Lemma 1 is satisfied. Clearly \( \pi(f)^2 = 0 \) for every irreducible representation \( \pi \) of \( G \). It follows that for \( \varepsilon > 0 \) sufficiently small \( P = (1 + \varepsilon f(g)) \, dg \) is a probability measure satisfying \( P \ast P = U \). \( \square \)

Remark. The relation between the existence of nilpotent elements and commutativity of the group has been investigated by M. Behncke (1971).

It was argued above that abelian groups do not admit a nontrivial square root of the uniform distribution. In light of Lemma 2, the nonabelian compact separable groups with the property that \( \mathcal{R}_\rho(G) \) has no nilpotents must be classified.
Let $M(G)$ denote the algebra, under convolution, of real measures on $G$. The following lemma has been abstracted from Sehgal (1975):

**Lemma 3.** If $M(G)$ has no nilpotent elements then every closed subgroup of $G$ is normal.

**Proof.** Observe first that if $R$ is any ring with unit and no nilpotents, then an idempotent $e = e^2$ in $R$ commutes with every element $r \in R$. In fact, the equation $[e(r(1-e))]^2 = 0$ implies $e(r(1-e)) = 0$, so $er = ere$. Similarly, $re = ere = er$. Now let $R = M(G)$, let $H$ be a closed subgroup of $G$, and let $e$ be Haar measure on $H$ normalized so that $\text{vol}(H) = 1$. Then $e$ is an idempotent in $M(G)$. For $g \in G$ let $\delta_g$ be a point mass at $g$. Then $\delta_g * e * \delta^{-1}_g = e$ which implies $H$ is normal. $\square$

To complete the proof of Theorem 1, map $M(G)$ into $R^p(G)$ by $\mu \mapsto p(\mu)$. From the Peter-Weyl theory, the map

$$M(G) \to \prod_\rho R^p(G), \quad \mu \to \prod_\rho \rho(\mu)$$

is injective. Since $R^p(G)$ contains no nilpotent elements, neither does $M(G)$ and by Lemma 3, $G$ is of the form given by Theorem 2. If $O$ is not trivial, choose a character $\chi$ taking at least one nonreal value. Let $\rho$ be the irreducible representation of $H$ given by

$$i \to \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \quad \text{and} \quad j \to \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Then $\chi \otimes 1 \otimes \rho$ is an irreducible two-dimensional representation, and $R_{\chi \otimes 1 \otimes \rho}(G)$ is the full $2 \times 2$ complex matrix algebra, which contains nilpotent elements. This completes the proof of Theorem 1.

3. Proof of Theorem 2.

**Definition.** A topological group is Hamiltonian if every closed subgroup is normal.

Recall that a finite group $G$ is Hamiltonian if and only if it is of the form $G = H \times F$ where $F$ is a finite abelian group with no element of order 4 (see Hall (1959)).

**Lemma 4.** Closed subgroups and quotient groups of Hamiltonian groups are Hamiltonian.

**Proof.** Clear.

**Lemma 5.** A compact noncommutative Lie group of dim $\geq 1$ is not Hamiltonian.

**Proof.** Let $G^0$ be a connected component of the identity in $G$. If $G$ is Hamiltonian then so is $G^0$. If $G^0$ is not abelian then it contains closed nonnormal subgroups, e.g. a maximal torus. So we may assume $G^0$ is a torus $T$, and $G/T$ is finite. Hence we have the exact sequence

$$0 \to T \to G \to H \times F \to (1)$$
where $F$ is a finite abelian group with no element of order 4. Let $G' = \eta^{-1}(H)$. Then we have the exact sequence

\[ 0 \rightarrow T \rightarrow G' \rightarrow H \rightarrow \{1\}. \]

Let $c \in H^2(H, T)$ be the cocycle defining the extension (1). Since $H$ has order 8, $8c = 0$ in $H^2(H, T)$ (see e.g. Mac Lane (1975)). This means there is $f: H \rightarrow T$ such that $8\bar{c} - \delta f = 0$ where $\delta$ is the coboundary operator for nonhomogeneous cochains and $\bar{c}: H \times H \rightarrow T$ is a representative for the cocycle $c$. Clearly there is $\phi: H \rightarrow T$ such that $8\phi = f$. Now the cochain $c' = \bar{c} - 8\phi$ is also a representative for $c$ and $8c' = 0$, i.e., $c'$ takes values in the subgroup $\mathcal{S}$ of elements of orders dividing 8 in $T$. Therefore we have the commutative, row and column exact diagram

\[
\begin{array}{c}
0 & \rightarrow & T & \rightarrow & G' & \rightarrow & H & \rightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \rightarrow & \mathcal{S} & \rightarrow & K & \rightarrow & H & \rightarrow & 0 \\
\end{array}
\]

where $K$ is defined by the cocycle $c'$. The subgroup $K$ is finite, therefore a closed subgroup of $G'$. From the finite case, $K$ and therefore $G'$ and so $G$ cannot be Hamiltonian. $\square$

For a separable compact group $G$, the Peter-Weyl theorem implies there is a sequence of finite dimensional representations $\rho_n (n \in \mathbb{N})$ such that

\[ \bigcap_n \text{Ker} \rho_n = \{ e \} \quad \text{and} \quad \text{Ker} \rho_n \supset \text{Ker} \rho_{n+1}. \]

**LEMMA 6.** If $G$ is a compact separable Hamiltonian group, then $\rho_n(G)$ is finite and $G = \lim_n \rho_n(G)$ where the projective limit is taken relative to the system $\{\rho_n(G)\}$ with the obvious maps $\rho_{n+1}(G) \rightarrow \rho_n(G)$.

**PROOF.** If $G$ is Hamiltonian, then $\rho_n(G)$ is a Hamiltonian compact Lie group, and therefore finite. We have the inverse system of exact sequences:

\[ (1) \rightarrow K_n \rightarrow G \rightarrow \rho_n(G) \rightarrow (1) \]

\[ (1) \rightarrow K_m \rightarrow G \rightarrow \rho_m(G) \rightarrow (1) \]

for $n \leq m$ where $K_m = \text{Ker} \rho_m \rightarrow K_n$ is the inclusion etc. Since in the category of compact groups $\lim$ of inverse systems of exact sequences is exact (Eilenberg-Steenrod (1952, Chapter 8)), we have the exact sequence

\[ (1) \rightarrow \bigcap_n K_n \rightarrow G \rightarrow \lim_n \rho_n(G) \rightarrow (1). \]

The hypothesis on $\rho_n$ implies $\bigcap K_n = \{ e \}$. $\square$

It is no loss of generality to assume $\rho_1(G) = H$. So we have the exact sequence

\[ (2) \rightarrow K_1 \rightarrow G \rightarrow \rho_1(H) \rightarrow (1), \]

when we have identified $\rho_1(G)$ with $H$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Lemma 7. Let $G$ be a compact separable Hamiltonian group, and $\pi_{mn}$ ($m \geq n$) be
the natural projection $\pi_{mn}: \rho_m(G) \rightarrow \rho_n(G)$. Then we can choose a splitting $\rho_n(G) = H \times F''_n \times F'_n$ when $F''_n$ is a product of $\mathbb{Z}_2$'s and $F'_n$ is an abelian group of odd order in such a way that $\pi_{mn}|_H = \text{id}$.

Proof. We construct the splitting inductively. The case $n = 1$ being obvious, we assume the splitting has been constructed up to $n$. Consider the canonical homomorphism

$$\pi_{n+1}: \rho_{n+1}(G) \rightarrow \rho_n(G) = H \times F''_n \times F'_n$$

and any decomposition

$$\rho_{n+1}(G) \cong H' \times F''_{n+1} \times F'_{n+1}$$

where $H' = H$, $F''_{n+1}$ is a product of $\mathbb{Z}_2$'s and $F'_{n+1}$ is a finite abelian group of odd order. Choose $(q_\alpha, \eta_\alpha, 0) \in H' \times F''_{n+1} \times F'_{n+1}$ ($\alpha = 1, 2$) such that

$$\pi_{n+1}(q_1, \eta_1, 0) = (i, 0, 0), \quad \pi_{n+1}(q_2, \eta_2, 0) = (j, 0, 0).$$

Set $q_3 = q_1 q_2$, $\eta_3 = \eta_1 \eta_2$, then $\pi_{n+1}(q_3, \eta_3, 0) = (k, 0, 0)$. Now define a homomorphism

$$\Phi_{n+1}: H \rightarrow H' \times F''_{n+1} \times F'_{n+1}$$

by

$$\Phi_{n+1}(\pm 1) = (\pm e, 0, 0), \quad \Phi_{n+1}(\pm i) = (\pm q_1, \eta_1, 0),$$
$$\Phi_{n+1}(\pm j) = (\pm q_2, \eta_2, 0), \quad \Phi_{n+1}(\pm k) = (\pm q_3, \eta_3, 0).$$

The fact that $\Phi_{n+1}$ is a homomorphism can be checked by straightforward verification, e.g., let us show

(3) $\Phi_{n+1}(j) = \Phi_{n+1}(ki)$.

By construction $\Phi_{n+1}(j) = (q_2, \eta_2, 0)$,

$$\Phi_{n+1}(k)\Phi_{n+1}(i) = (q_3 q_1, \eta_3 \eta_1, 0)$$

and $\eta_3 \eta_1 = \eta_2$. Also

$$\pi_{n+1}(q_2, \eta_2, 0) = (j, 0, 0) = \pi_{n+1}(q_3 q_1, \eta_2, 0).$$

Hence $(q_3 q_1 q_2^{-1}, 0, 0) \in \text{Ker} \pi_{n+1}$. If $q_3 q_1 q_2^{-1} \neq e$ then $\text{Ker} \pi_{n+1}|_{H'} \neq \{e\}$ and then $\text{im} \pi_{n+1}$ would be abelian. This proves (3). Let $H'' = \text{im} \Phi_{n+1}$. We have the decomposition

$$\rho_{n+1}(G) = H'' \times F''_{n+1} \times F'_{n+1}.$$ 

Now notice that the projection $\pi_{n+1}|_{H''}$ is simply the identity map after possibly relabelling. □

Lemma 8. Let $G$ be a compact separable Hamiltonian group. Then the exact sequence (2) splits and furthermore $G = H \times K_1$ as a direct product.

Proof. It suffices to prove the first assertion since if the sequence (2) splits and $G$ is a semidirect product of $K_1$ and $H$ which is not a direct product, then $H$ would be a closed subgroup which is not normal. To prove that (2) splits, we have to construct
a homomorphism
\[ \beta: H \to G = \lim\rho_n(G) \]
such that \( \rho_1 \circ \beta = \text{id}_H \). To do this it suffices to construct \( \beta_n: H \rightarrow \rho_n(G) \) such that
\[ \rho_n(G) \\
\beta_n \uparrow \\
\pi_{mn} \downarrow m \geq n \]
commutes and \( \beta_1 = \text{id} \). We define \( \beta_1 = \text{id} \). Consider the decomposition \( \rho_n(G) = H \times F'_n \times F''_n \) provided by Lemma 7. Define
\[ \beta_n(i) = (i, 0, 0), \quad \beta_n(j) = (j, 0, 0), \quad \text{etc.} \]
By Lemma 7, the commutativity condition (4) is satisfied.

We now complete the proof of Theorem 2. We necessarily have \( \pi_{n+1,n}(F'_{n+1}) \subseteq F'_n \) and \( \pi_{n+1,n}(H \times F''_{n+1}) \subseteq H \times F''_n \). Hence
\[ G = \lim (H \times F'') \times \lim (F''_n). \]
It remains to show
\[ \lim (H \times F'') = H \times \lim (F''_n) \]
where limits are taken with respect to the obvious maps. By definition
\[ \lim (H \times F'') = \{(q, f_1), (q, f_2), \ldots \} | \pi_{mn}((q, f_m)) = (q, f_n) \}. \]
Now \( \pi_{mn}(q, 0) = (q, 0) \), hence if \( ((q, f_1), (q, f_2), \ldots) \in \lim (H \times F'') \) we have
\[ \pi_{mn}(e, f_m) = (e, f_n). \]
Conversely, if (6) holds then \( ((q, f_1), (q, f_2), \ldots) \in \lim (H \times F''). \) This proves (5) and Theorem 2 with \( O \) presented as an abelian profinite group. Shatz (1972, p. 10) shows that an abelian group is profinite if and only if its dual is a torsion group.

In conclusion we note that a compact Hamiltonian group does not necessarily have the property that every subgroup is normal. In fact, \( H \times \prod \mathbb{Z}_p \) (\( \mathbb{Z}_p = \) integers mod prime \( p \)) is Hamiltonian in our sense, however, the cyclic subgroup generated by \( (i, 1, 1, 1, \ldots) \) is not normal.

ACKNOWLEDGMENT. We thank Irving Kaplansky for helping us make the transition from finite to compact in Theorem 1.

REFERENCES


DEPARTMENT OF STATISTICS, STANFORD UNIVERSITY, STANFORD, CALIFORNIA 94305

JET PROPULSION LABORATORY, CALIFORNIA INSTITUTE OF TECHNOLOGY, PASADENA, CALIFORNIA 91109