PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 98, Number 2, October 1986

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 $P * P = U$, 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 $P * P = U$ where U is Haar measure and $P \neq U$? Our main result is

THEOREM 1. *There is a probability P such that $P * P = U$ if and only if G is a nonabelian group which is not isomorphic to a product $\mathbf{H} \times E$ with $\mathbf{H}$ 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 $G \simeq \mathbf{H} \times E \times O$ where $\mathbf{H}$ 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 Hamitonian groups as groups which can be represented as $\mathbf{H} \times E \times \tilde{O}$ with $\mathbf{H}$ and E as in Theorem 2, and $\tilde{O}$ 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 $\tilde{O}$ countable, and compact separable groups with every subgroup normal.

The countable torsion groups $\tilde{O}$ can be classified by using results in Kaplansky (1952). First, any torsion group is a direct sum of primary groups, and $\tilde{O}$ can have no 2-primary part. Then, Ulm's theorem gives a complete characterization of the other possible primary parts.

Received by the editors August 5, 1985.
1980 *Mathematics Subject Classification*. Primary 22C05; Secondary 60B15.
Key words and phrases. Compact groups, factorization, Haar measure, normality of closed subgroups.

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 ρ of G into the group of invertible linear operators on a complex vector space V of dimension d_ρ. A representation ρ 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 ρ, its contragredient $\tilde{\rho}$ is defined by

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

where $'$ denotes transpose. Then

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

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

$$\rho(P) = \int_G \rho(g) P(dg).$$

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

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

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 ρ,

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

implies $\rho(P) = 0$.

For nonabelian groups, the proof requires some preliminary lemmas.

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

PROOF. If μ is real, then

$$\tilde{\rho}_{ij}(\mu) = \int \bar{\rho}_{ij}(g)\,\mu(dg) = \overline{\rho_{ij}(\mu)}\,.$$

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

$$0 = \int \bar{\rho}_{ij}(g)\,\mu(dg) = -\int \bar{\rho}_{ij}(g)\,\bar{\mu}(dg)$$

or

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

Since this holds for every irreducible ρ, the Peter-Weyl theorem implies that the set function $\bar{\mu} - \mu$ is zero, so μ is real. □

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 $P * P = U$.*

(b) *There is an irreducible (complex) representation ρ of G such that the algebra*

$$R_\rho = \left\{ \sum_{g \in G} \mathbf{R}\rho(g) \right\}$$

contains nilpotent elements.

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

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

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

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

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

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 $R_\rho(G)$ 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 $[er(1 - e)]^2 = 0$ implies $er(1 - e) = 0$, 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 $\mathrm{vol}(H) = 1$. Then e is an idempotent in $M(G)$. For $g \in G$ let δ_g be a point mass at g. Then $\delta_g * e * \delta_{g^{-1}} = e$ which implies H is normal. □

To complete the proof of Theorem 1, map $M(G)$ into $R_\rho(G)$ by $\mu \to \rho(\mu)$. From the Peter-Weyl theory, the map

$$M(G) \to \prod_\rho R_\rho(G), \qquad \mu \to \prod_\rho (\rho(\mu))$$

is injective. Since $R_\rho(G)$ 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 χ taking at least one nonreal value. Let ρ 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 2×2 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 $G = \mathbf{H} \times F$ 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* $\dim \geqslant 1$ *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

$$0 \to T \to G \xrightarrow{\eta} \mathbf{H} \times F \to (1)$$

where F is a finite abelian group with no element of order 4. Let $G' = \eta^{-1}(\mathbf{H})$. Then we have the exact sequence

$$(1) \qquad 0 \to T \to G' \to \mathbf{H} \to \{1\}.$$

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

$$\begin{array}{ccccccccc} & & 0 & & 0 & & & & \\ & & \downarrow & & \downarrow & & & & \\ 0 & \to & \mathscr{E} & \to & K & \to & \mathbf{H} & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow \text{id} & & \\ 0 & \to & T & \to & G' & \to & \mathbf{H} & \to & 0 \end{array}$$

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. □

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

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

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

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:

$$\begin{array}{ccccccccc} (1) & \to & K_n & \to & G & \to & \rho_n(G) & \to & (1) \\ & & \uparrow & & \uparrow \text{id} & & \uparrow & & \\ (1) & \to & K_m & \to & G & \to & \rho_m(G) & \to & (1) \end{array}$$

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

$$(1) \to \bigcap_n K_n \to G \to \varprojlim \rho_n(G) \to (1).$$

The hypothesis on ρ_n implies $\bigcap K_n = \{e\}$. □

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

$$(2) \qquad (1) \to K_1 \to G \overset{\rho_1}{\to} \mathbf{H} \to (1),$$

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

LEMMA 7. *Let G be a compact separable Hamiltonian group, and π_{mn} $(m \geqslant n)$ be the natural projection π_{mn}: $\rho_m(G) \to \rho_n(G)$. Then we can choose a splitting $\rho_n(G) = \mathbf{H} \times F_n'' \times F_n'$ when F_n'' is a product of $\mathbf{Z}_2$'s and F_n' is an abelian group of odd order in such a way that $\pi_{mn}|_{\mathbf{H}} = \mathrm{id}$.*

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

$$\pi_{n+1\,n}\colon \rho_{n+1}(G) \to \rho_n(G) = \mathbf{H} \times F_n'' \times F_n'$$

and any decomposition

$$\rho_{n+1}(G) \simeq \mathbf{H}' \times F_{n+1}'' \times F_{n+1}'$$

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

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

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

$$\Phi_{n+1}\colon \mathbf{H} \to \mathbf{H}' \times F_{n+1}'' \times F_{n+1}'$$

by

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

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

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

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

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

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

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

Now notice that the projection $\pi_{n+1\,n}|_{\mathbf{H}''}$ 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 $G \simeq \mathbf{H} \times K_1$ 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 $\mathbf{H}$ which is not a direct product, then $\mathbf{H}$ would be a closed subgroup which is not normal. To prove that (2) splits, we have to construct a homomorphism

$$\beta\colon \mathbf{H} \to G = \varprojlim \rho_n(G)$$

such that $\rho_1 \circ \beta = \mathrm{id}_{\mathbf{H}}$. To do this it suffices to construct $\beta_n\colon \mathbf{H} \to \rho_n(G)$ such that

$$(4) \qquad \begin{array}{ccc} & & \rho_n(G) \\ & \beta_n \nearrow & \\ H & & \uparrow \pi_{mn} \qquad m \geqslant n \\ & \beta_m \searrow & \\ & & \rho_m(G) \end{array}$$

commutes and $\beta_1 = \mathrm{id}$. We define $\beta_1 = \mathrm{id}$. Consider the decomposition $\rho_n(G) = \mathbf{H} \times F_n'' \times F_n'$ 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 $\pi_{n+1\,n}(F'_{n+1}) \subset F'_n$ and $\pi_{n+1\,n}(\mathbf{H} \times F''_{n+1}) \subset \mathbf{H} \times F''_n$. Hence

$$G = \varprojlim\left(\mathbf{H} \times F_n''\right) \times \varprojlim\left(F_n'\right).$$

It remains to show

$$(5) \qquad \varprojlim\left(\mathbf{H} \times F_n''\right) = \mathbf{H} \times \varprojlim\left(F_n''\right)$$

where limits are taken with respect to the obvious maps. By definition

$$\varprojlim\left(\mathbf{H} \times F_n''\right) = \left\{\left((q,f_1),(q,f_2),\dots\right) \middle| \pi_{mn}((q,f_m)) = (q,f_n)\right\}.$$

Now $\pi_{mn}(q,0) = (q,0)$, hence if $((q,f_1),(q,f_2),\dots) \in \varprojlim(\mathbf{H} \times F_n'')$ we have

$$(6) \qquad \pi_{mn}(e,f_m) = (e,f_n).$$

Conversely, if (6) holds then $((q,f_1),(q,f_2),\dots) \in \varprojlim(\mathbf{H} \times F_n'')$. 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, $\mathbf{H} \times \prod \mathbf{Z}_p$ ($\mathbf{Z}_p$ = integers mod prime p) is Hamiltonian in our sense, however, the cyclic subgroup generated by $(i,1,1,1,\dots)$ is not normal.

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

References

H. Behncke, (1971), *Nilpotent elements in group algebras*, Bull. Acad. Polon. Ser. Math. **19** (1971), 197–198.

P. Diaconis, (1982), *On the use of group representations in probability and statistics*, Typed Lecture Notes, Department of Statistics, Institute of Mathematical Statistics, Harvard University (to appear).

S. Eilenberg and N. Steenrod, (1952), *Foundations of algebraic topology*, Princeton Univ. Press, Princeton, N.J., 1952.

M. Hall, (1959), *The theory of groups*, Macmillan, New York, 1959.

E. Hewitt and K. Ross, (1963), *Abstract harmonic analysis*. I, Springer-Verlag, Berlin, 1963.

______, (1970), *Abstract harmonic analysis*. II, Springer-Verlag, Berlin, 1970.

I. Kaplansky, (1952), *Infinite abelian groups*, Univ. of Michigan Press, Ann Arbor, Michigan, 1952.

S. Mac Lane, (1975), *Homology theory*, Springer-Verlag, Berlin, 1975.

J. Pascaud, (1973), *Anneaux de groups reduits*, C. R. Acad. Sci. Paris Ser. A **277** (1973), 719–722.

S. Shatz, (1972), *Profinite groups, arithmetic, and geometry*, Princeton Univ. Press, Princeton, N.J., 1972.

S. K. Sehgal, (1975), *Nilpotent elements in group rings*, Manuscripta Math. **15** (1975), 65–80.

DEPARTMENT OF STATISTICS, STANFORD UNIVERSITY, STANFORD, CALIFORNIA 94305

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