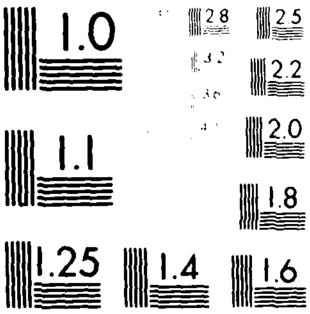
AD-A109 663 STANFORD UNIV CA DEPT OF STATISTICS F/G 12/1
FACTORING PROBABILITIES ON COMPACT GROUPS.(U)
DEC 81 P DIACONIS, M SHASHAHANI N00014-76-C-0475
UNCLASSIFIED TR-312 NL

1 OF 1
AD A
109663

END
DATE
FILMED
02-82
DTIC



MICROCOPY RESOLUTION TEST CHART

NATIONAL BUREAU OF STANDARDS-1963-A

FACTORING PROBABILITIES ON COMPACT GROUPS

By

PERSI DIACONIS AND MEHRDAD SHASHAHANI

TECHNICAL REPORT NO. 312

DECEMBER 2, 1981

Prepared Under Contract
N00014-76-C-0475 (NR-042-267)
For the Office of Naval Research

Herbert Solomon, Project Director

DEPARTMENT OF STATISTICS
STANFORD UNIVERSITY
STANFORD, CALIFORNIA

FACTORING PROBABILITIES ON COMPACT GROUPS

by

Persi Diaconis and Mehrdad Shashahani
Department of Statistics, Stanford University

Abstract

When can a probability P be factored as $P_1 * P_2$? This problem arises in efficient generation of pseudo random integers and permutations. It is thus natural to think of P defined on a group. We show that any strictly positive measure can be factored. The uniform distribution can be factored in a non-trivial way for any compact group having more than three elements. If it is required that $U = P * P$, then factorization is possible if and only if the group is not Abelian or the product of the quarternions and a finite number of two element groups.

1. Introduction

Let P be a probability measure on the Borel sets of a locally compact topological group. Following Levy (1953), we say that P is decomposable if P can be written as a convolution $P = P_1 * P_2$ with P_i not fixed at a point. The study of decomposable probability arises naturally in applied problems.

These problems include computer generation of pseudo-random uniform variables on a finite group such as the integers (mod n) or the permutations. Application is also made to the study of the distribution of nonparametric measures of correlation. Applications are discussed in Section 2. In Section 3 we show that any positive measure on a compact group is decomposable.

The uniform distribution U on a compact group requires special treatment because of the trivial factorization $U = U * P$, for any P. We say that U is semi-decomposable if $U = P_1 * P_2$ with P_i not uniform. In Section 3 we show that U on any compact polish group is semi-decomposable unless the group has two or three elements.

If restrictions are put on P_i, then factorization may not be possible. For example, if $\tilde{P}(A) = P(A^{-1})$, then $U = P * \tilde{P}$ is never possible. The factorization $U = P * P$ is never possible on Abelian groups, but is possible on most non-Abelian groups. Indeed, it is shown that $U = P * P$ for all groups different from a product of the quarternions and a finite number of two element groups. We also study the possibility of factorization when P is restricted to be spherically symmetric with respect to a subgroup forming a Gelfand pair.

A motivated introduction to probability on groups is in Grenander (1963). For a comprehensive treatment see Heyer (1977) or Hewitt and Ross (1963), (1970). A nice discussion of factorization on $\mathbb{R}$ is in Chapter 6 of Lukas (1970).

2. Some Applications

This section describes some applied problems in which factorization plays a role.

Example 1. Generating random permutations.

For generating random bridge hands, Monte Carlo investigation of rank tests in statistics, and other applications, a source of pseudo-random permutations of n objects is useful. If n is small, a useful approach is to set up a 1-1 correspondence between the integers from 1 to $n!$ and permutations and then use a source of pseudo random integers. The factorial number system is sometimes used for this purpose, see page 64 and 192 of Knuth (1981). For larger n, like 52, the most frequently used algorithm involves a factorization of the uniform distribution. Informally, at the ith stage a random integer J_i between i and n is chosen and i and J_i are transposed. Call the probability distribution at the ith stage P_i, it will be shown below that $P_1 * P_2, \ldots, * P_{n-1}$ is a factorization of the uniform distribution. Further discussion of this algorithm is on pp. 139-141 of Knuth (1981). The factorization has recently been applied in the theoretical problem of finding the order of a random permutation by Bovey (1980). It also forms the basis of fast algorithms for manipulating permutations. See Furst et al. (1980). The following algorithm abstracts the idea to any finite group.

Subgroup algorithm. Let G be a finite group. Let $G_0 = G \supset G_1 \supset \ldots \supset G_r$ be a nested chain of subgroups, not necessarily normal. Let C_i be coset representatives for G_{i+1} in G_i, $0 \leq i < r$. Clearly G can be represented as $G \cong C_0 \times C_1 \times \ldots \times C_{r-1} \times G_r$ in the sense that each $g \in G$ has a unique representation as $g_0 g_1 \ldots g_{r-1} g_r$ with $g_i \in C_i$ and $g_r \in G_r$.

Let P_i be the uniform distribution on C_i and G_r respectively. The convolution $P_1 * P_2 * \ldots * P_r$ is then a factorization of the uniform distribution on G.

Specializing to the symmetric group, consider the chain $S_n \supset S_{n-1} \supset S_{n-2} \supset \ldots \supset \{id\}$. Here S_{n-i} is represented as the set of permutations of n letters that fix the first i letters. Then, coset representatives C_i can be chosen as the set of transpositions transposing i and letters larger than i. The subgroup algorithm suggests a class of algorithms that interpolate between the factorial number system and random transpositions: Let $S_n \supset S_{n_1} \supset \ldots \supset S_{n_r}$ with $n > n_1 > \ldots > n_r$. Here the size of the cosets C_i are allowed to get large and a variant of the factorial number system permits choice of a random coset element from a random integer. For example, consider the chain $S_n \supset S_{n-2} \supset S_{n-4} \supset \ldots \supset \{id\}$. Coset representatives for $S_{n-2(i+1)}$ in S_{n-2i} are permutations bringing a pair of elements between $i+1$ and n into positions $i+1$ and $i+2$. These permutations may be ordered lexographically, setting up a 1-1 correspondence between them and numbers $1, 2, \ldots, (n-i)(n-i-1)$. An advantage of this method is that it requires fewer calls to the random number generator.

The subgroup algorithm can be used to generate random positions in the currently popular Rubick's cube puzzle.

A different application of the factorization suggested by the subgroup algorithm is to computer generation of pseudo-random integers (mod N). Given two sources of pseudo-random integers X and Y, computer scientists sometimes form a new sequence $Z = X+Y \pmod N$. Knuth (1981, p. 631) contains a discussion of work by Marsaglia and others. Solomon and Brown (1980) show that this procedure brings Z closer to uniform. Marshall and Olkin (1980,

p. 383) generalize this to any finite group. It is natural to seek distributions of X and Y such that Z is exactly uniform. The subgroup algorithm does this when N is composite. For N prime, see Lemma 2 in Section 3.

Example 2. Nonparametric measures of association.

A wide variety of nonparametric measures of association arise from metrics ρ on the permutation group S_n. Typical choices are $\rho(\pi',\pi) = \{\Sigma(\pi'(i) - \pi(n))^2\}^{\frac{1}{2}}$ (Spearman's rank correlation), or the minimum number of pairwise adjacent transpositions it takes to bring π to π' (Kendall's tau). For a survey, see Diaconis and Graham (1977). Most naturally occurring metrics are right invariant:

$$\rho(\pi'\eta, \pi\eta) = \rho(\pi', \pi) = \rho(id, \pi'\pi^{-1}) .$$

If π' and π are chosen uniformly from S_n , then the distribution of $\rho(\pi',\pi)$ is the same as the distribution of $\rho(id,U)$, where U is a random permutation. It is natural to ask if $\pi'\pi^{-1}$ can be uniform under other assumptions on the distribution of (π',π). For example, if π', π are chosen independently from the same non-uniform distribution, it is shown in Theorem 3 of Section 4 that $\pi'\pi^{-1}$ is not uniform. The subgroup algorithm, or Theorem 5 in Section 4, show that $\pi'\pi^{-1}$ can be uniform if π' and π are merely independent.

3. Decomposable and Semi-decomposable Probabilities

Decomposable probabilities.

Throughout, P is a probability on the Borel sets of a compact topological group. The probability P is decomposable if P can be decomposed as a convolution $P = P_1 * P_2$ with P_i not fixed at a point. This definition rules out the trivial decomposition $P = P_1 * \delta_g$ with δ_g a point mass at group element g and $P_1 = P * \delta_{g^{-1}}$. Levy (1953) gave a nice example of a measure which is not decomposable: Take the group as S_3, fix p in $(0,1)$ and let P put mass p on the identity and mass $(1-p)$ on a 3-cycle. It is not hard to show that the set S of support points of P is not of the form $S = S_1S_2$ with S_i of cardinality 2 or more, so P is not decomposable. The following result shows that if $P << dg$ with a positive continuous density, then P is decomposable.

<u>Theorem 1</u>. Let G be compact; let $P = fdg$ with $f > \varepsilon > 0$. Then P is decomposable.

<u>Proof</u>. Suppose $f > \varepsilon > 0$. Let probability measures P_i be defined by

$$P_1 = \frac{1}{1+\varepsilon_1}\{f + \varepsilon_1\}dg \ , \quad P_2 = \frac{1}{1+\varepsilon_2}\{\delta_{id} + \varepsilon_2 dg\} \ ,$$

with ε_i chosen so $\varepsilon_1 + \varepsilon_2 + \varepsilon_1\varepsilon_2 = 0$; e.g., $\varepsilon_1 = -\varepsilon_2/(1+\varepsilon_2)$ and ε_2 chosen positive but so small that $P_i \geq 0$. Then

$$P_1 * P_2 = fdg + \{\varepsilon_1 + \varepsilon_2 + \varepsilon_1\varepsilon_2\}dg = fdg \ . \qquad \square$$

<u>Remarks</u>. In the case of finite groups, this gives an easy proof of a theorem of P. J. Cohen (1959). Cohen showed that if the density f is continuous, then the measures P_i can be chosen to have densities. Note that in our construction P_2 is not absolutely continuous with respect to dg when G is infinite. Cohen gives an example of a probability density on a compact subset of $\mathbb{R}$ which cannot be written as a convolution of two probabilities with densities. An earlier example of Levy and a review of the literature on $\mathbb{R}$ appear in

chapter 6 of Lukacs (1970). Lewis (1967) shows that the uniform distribution on [0,1] cannot be written as a convolution of two probabilities with densities. It is well known that the convolution of singular measures can have a density. See Rubin (1967) and Hewitt and Zukerman (1966) for some examples.

Semi-decomposable probabilities.

Turn now to decomposing the uniform distribution U on a compact group. The subgroup algorithm of Section 2 gives any easy method for decomposing the uniform distribution on a finite group. Consideration of the circle group and the subgroup of kth roots of unity suggests that the result generalizes:

Lemma 1. Let G be a compact, Polish group with a closed subgroup H. Then, the uniform distribution is semi-decomposable.

Proof. Let $\pi : G \to G/H$ be the cannonical map. Let Q be the image of the uniform distribution under π. Take a measurable inverse $\phi : G/H \to G$ with the property that $\pi\, \phi\{gH\} = \{gH\}$. The existence of ϕ under our hypothesis follows from Theorem 1 in Bondar (1976). Let P_1 be the image of Q under ϕ. Let P_2 be the uniform distribution on H. To prove that $P_1 * P_2$ is uniform, consider any continuous function f on G. By definition

$$\int_G f(g)\ P_1 * P_2(dg) = \int_G \int_G f(g_1 g_2)\ P_1(dg_1)P_2(dg_2) = \int_{\phi(G/H)} \int_H f(g_1 g_2)\ P_1(dg_1)P_2(dg_2)$$

$$= \int_G f(g)\ U(dg)\ .$$

The final equality in the display follows from Theorem 2 in Bondar (1976). □

We next show how to decompose the uniform distribution on groups with no proper subgroups: the integers mod a prime. It is easy to see that the uniform distribution is not semi-decomposable on Z_2 or Z_3. One approach uses the fact that $1+z$ and $1+z+z^2$ are irreducible over the reals factorization of U leads would lead to a factorization of the associated polynomial.

Lemma 2. Let $p \geq 5$ be prime. Let Z_p be the integers mod p. Then the uniform distribution is semi-decomposable.

Proof. For $i = 1, 2, \ldots, \frac{p-1}{2}$, let a_i, b_i be determined by

$$a_i + 2b_i = 1 \ , \quad a_i + 2b_i \cos\left(\frac{2\,\pi\, i^2}{p}\right) = 0$$

Noting that $\cos\left(\frac{2\,\pi\, i^2}{p}\right) \neq 1$ for i in the indicated range;

$$b_i = \left\{2\left(1 - \cos\frac{2\,\pi\, i^2}{p}\right)\right\}^{-1} , \quad a_i = -\cos\left(\frac{2\,\pi\, i^2}{p}\right) \Big/ \left(1 - \cos\frac{2\,\pi\, i^2}{p}\right) \ .$$

Define signed measures Q_i on Z_p by

$$Q_i(0) = a_i \ , \quad Q_i(i) = Q_i(-i) = b_i \ , \quad Q_i(j) = 0 \text{ otherwise} \ .$$

The argument depends on the discrete Fourier transform of a measure. If P is a measure on Z_p and $k \in Z_p$, define

$$\rho_k(P) = \frac{1}{p} \sum_{j=0}^{p-1} P(j) e^{2\pi ijk/p} \ .$$

For the uniform distribution,

$$\rho_k(U) = \begin{cases} 1 & \text{if } k = 0 \\ 0 & \text{otherwise} \end{cases} \ .$$

It is easy to check that for $k \neq 0$, $\rho_{\pm k}(Q_k) = 0$, $\rho_0(Q_k) = 1$. Now let signed measures R_1 and R_2 be defined by

$$R_1 = \mathop{*}_{i=1}^{a} Q_i \; , \quad R_2 = \mathop{*}_{i=a+1}^{(p-1)/2} Q_i \quad \text{for fixed } 1 \leq a \leq (p-1)/2 \; .$$

Finally, for sufficiently small ε the measures $U + \varepsilon R_1$ and $U + \varepsilon R_2$ are positive measures and can be normed to be probabilities, say P_1 and P_2. We claim $U = P_1 * P_2$. Indeed, for $k \neq 0$, $\rho_k(P_1 * P_2) = \rho_k(P_1)\,\rho_k(P_2) = 0$. To show that the decomposition is non-trivial, it suffices to show that R_i are non-zero, $i = 1, 2$. This follows from the fact that for $k \neq j$, $\rho_j(Q_k) \neq 0$. Indeed,

$$\rho_j(Q_k) = a_k + 2b_k \cos\left(\frac{2\,\pi\, jk}{p}\right)$$

$$= \frac{1}{1 - \cos(2\,\pi\, k^2)} \left\{ -\cos\left(\frac{2\,\pi\, k^2}{p}\right) + \cos\left(\frac{2\,\pi\, jk}{p}\right) \right\}$$

This is zero if and only if $j = k$. □

<u>Remarks</u>. Factoring the uniform distribution on Z_p is sufficiently close to some classical factorization results to warrant discussion. A well known elementary probability problem argues that it is impossible to load two dice so that the sum is uniform. More generally, Dudewicz and Dann (1972) show that it is impossible to find probabilities P_1 and P_2 on the set $\{1, 2, \ldots, n\}$ such that $P_1 * P_2$ is the uniform distribution on $\{2, \ldots, 2n\}$. A related result asks for a decomposition of the uniform distribution on the set $0, 1, 2, \ldots, N$. Lukacs (1970), pp. 182-183, reviews the literature on this problem. He shows factorization is possible when, and only when, N is

prime. The difference between the three results is this: In Lemma 2, and in the subgroup factorization, addition is (mod N). In the dice result, both factors must be supported on $\{1, \ldots, n\}$ while the uniform distribution is on $\{2, \ldots, n\}$. In the results reported in Lukacs, the factors are permitted to have arbitrary support.

The results above can be combined into the following.

Theorem 2. The uniform distribution on a compact Polish group G is semi-decomposable unless G is Z_2 or Z_3.

Proof. For finite groups, Lemma 2 and the subgroup algorithm prove the claim, since a finite group with no proper subgroups is the residues of a prime. We now argue that every infinite compact group contains a closed non-trivial subgroup. A topological group has no small subgroups (NSS) if there exists a neighborhood U of the identity such that the only subgroup in U is $\{id\}$. Clearly, a group which has small subgroups contains non-trivial closed subgroups. A famous theorem of Gleason (1952) implies that a group with NSS is a Lie group. The structure of compact Lie groups is well known; see, for example, Chapter 11 of Pontryagin (1966): If G is Abelian, then the connected component of the identity is a finite dimensional torus which certainly has non-trivial closed subgroups, hence G does. If G is not Abelian, then its maximal torus is a non-trivial closed subgroup. □

4. Restricted Factorizations

The results in Section 3 show that in most cases, the uniform distribution can be factored. In this section the factors are restricted in some way. The first result introduces material on representations which will be used throughout this section.

Difference distributions.

Let P be a probability on a group. Let $\tilde{P}(A) \equiv P(A^{-1})$. Example 2 of Section 2 gives some motivation for considering factorizations of the form $P * \tilde{P}$.

Theorem 3. On a compact group, if $U = P * \tilde{P}$, then $P = U$.

Proof. The argument uses the basic facts about representations of compact groups. See Chapter 4 of Serre (1977) for a review. We need the following facts. A representation ρ is a continuous map from G into $GL_{d_\rho}(V)$ for a complex vector space V of dimension d_ρ. The matrices $\rho(g)$ can all be chosen as unitary: $\rho(g)\ \rho(g)^* = \text{id}$, where the $*$ means conjugate transpose. A representation is irreducible if the matrices $\{\rho(g)\}_{g \in G}$ leave no non-trivial subspace of V invariant. The transform of a probability P on G at representation ρ is $\rho(P) = \int_G \rho(g)\ P(dg)$. The matrices $\{\rho(P)\}_{P \in G}$, as ρ ranges over the finite dimensional irreducible representations, determine P. If ρ is non-trivial, $\rho(U) = 0$. With these facts, the proof is easy. For a unitary representation $\rho(g^{-1}) = \rho(g)^{-1} = \rho(g)^*$. Thus $\rho(\tilde{P}) = \rho(P)^*$. If $P * \tilde{P} = U$, then $0 = \rho(U) = \rho(P * \tilde{P}) = \rho(P)\ \rho(\tilde{P}) = \rho(P)\ \rho(P)^*$. Thus $\rho(P) = 0$ for all non-trivial irreducible representations, so $P = U$. □

Square roots.

On a compact Abelian group the factorization $U = P * P$ is impossible unless P is uniform. This follows because all irreducible representations are one-dimensional and $0 = \rho(U) = \rho(P * P) = \rho(P)^2$ implies $\rho(P) = 0$. For non-Abelian groups, things are more complex.

Example 3. On S_3 a square root P of U can be defined as follows: using cycle notation for permutations let

$P(id) = \frac{1}{6}$, $P(12) = \frac{1}{6}$, $P(23) = \frac{1}{6}+h$, $P(31) = \frac{1}{6}-h$, $P(123) = \frac{1}{6}-h$, $P(132) = \frac{1}{6}+h$, for any h with $0 \leq h \leq \frac{1}{6}$.

To motivate Theorem 4, let us explain how this example was found. We seek a probability P on S_3 such that $\rho(P)^2 = 0$ for each non-trivial irreducible representation ρ. Let us find a function f on S_3 such that $\rho(f) = 0$ for all irreducible ρ and then $P(\pi) = \frac{1}{6} + \varepsilon f(\pi)$, with ε chosen small enough that $P(\pi) \geq 0$ will do the job. There are three irreducible representations of S_3, the trivial representation ρ_t, the alternating representation ρ_a, and a two-dimensional representation ρ_2. If $\rho_2(f)$ is a non-zero nilpotent matrix $\rho_2(f) = \begin{pmatrix} 0 & * \\ 0 & 0 \end{pmatrix}$ and $\rho_t(f) = \rho_a(f) = 0$, then $\rho^2(f) \equiv 0$. This gives five linear relations for the six numbers $f(\pi)$. The example above resulted from solving these equations. The following theorem gives a generalization.

Theorem 4. Let G be a compact, non-commutative group. The following conditions are equivalent.

a) There is a probability measure $P \neq U$ such that $P * P = U$.

b) There is an irreducible representation ρ of G such that the algebra $R_\rho = \{\Sigma_{g\epsilon G} \mathbb{R}\, \rho(g)\}$ contains nilpotent elements.

Remark. The quaternions ± 1, $\pm i$, $\pm j$, $\pm k$ form a finite non-commutative group such that the uniform distribution does not have a non-trivial square root. This follows from Theorem 5 below which identifies all finite groups satisfying condition b).

The proof of Theorem 4 requires some notation. Throughout we assume that all irreducible representations are given by unitary matrices. If ρ is a representation, let $\bar{\rho}(g)$ be defined as $\bar{\rho}(g) = \rho(g^{-1})'$. The following lemma is used in the proof of Theorem 4.

Lemma 3. Let μ be a bounded measure on a compact group G. Then μ is real if and only if $\tilde{\rho}(\mu) = \overline{\rho(\mu)}$ for every irredicuble ρ.

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 $\bar{\rho}(\mu) = \overline{\rho(\mu)}$. 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. □

Proof of Theorem 4. If $U = P * P$, then $\rho(P)^2 = 0$ and $\rho(P) \neq 0$ for some ρ^* because $P \neq U$. Thus $R_{\rho*}$ has nilpotents. Conversely, let $\gamma_1 \in R_{\rho*}$ be nilpotent. If $\gamma_1^n = 0$ and n is the smallest such power, then set $\gamma = \gamma_1^{n-1}$. This is non-zero and $\gamma^2 = 0$. Define a continuous function f on G as follows. Set $\rho(f) = 0$ if $\rho \neq \rho*$ or $\tilde{\rho}*$, $\rho*(f) = \gamma$, and if $\rho*$ is not equivalent to $\tilde{\rho}$, $\tilde{\rho}*(f) = \bar{\gamma}$. This defines a non-zero continuous function f through the Peter-Weyl theorem. Because of Lemma 3, f is real. Clearly, $\rho(f)^2 = 0$ for all irreducible ρ. It follows that for ε suitably small, $P = (1+\varepsilon f(g))dg$ is a probability satisfying $P * P = U$. □

A sufficient condition for Theorem 4 is that G have a real representation of dimension 2 or greater: If $\rho*$ is an n-dimensional real representation, let $f(g) = \varepsilon\ \rho^*_{1n}(g)$. Then by the Schur orthogonality relations, for any $\rho \neq \rho^*$, $\rho(f) = 0$. Also, Schur's relations imply $\rho^*(f)$ is an $n \times n$ matrix which is zero except that the $1, n$ entry is $\varepsilon \int \rho_{1n}^2 \, dg > 0$. Thus $\rho^*(f)^2 = 0$. Let a probability P be defined by $P = (1+\varepsilon f)dg$, with ε chosen so that P is positive. Then $\rho(P * P) = \rho(U)$ for all irreducible representations. As an example, the adjoint representation of a compact simple lie group has a basis with respect to which it is real orthogonal. Thus, the group $SO(n)$ of proper notations for $n = 3$, and $n \geq 5$ admits a square root of U.

The next result classifies all finite groups such that the uniform distribution is semi-decomposable.

Theorem 5. The uniform distribution on a finite group G is semi-decomposable if and only if G is not Abelian or the product of the quarternions and a finite number of two-element groups.

Proof. It was argued above that Abelian groups do not admit a non-trivial square-root of the uniform distribution. In light of Theorem 4, the non-Abelian groups with the property that $R_\rho(G)$ has no nilpotents must be classified. We will use a lemma of Sehgal (1975). Some notation is needed. Let $\mathbb{Q}$ denote the rational numbers, and let $\mathbb{Q}(G)$, the rational group ring denote the set of formal linear combinations of elements of G with rational coefficients. A non-Abelian group in which every subgroup is normal is called Hamiltonian. Theorem 12.5.4 of Hall (1959) shows that every Hamiltonian group is of the form $G = A \times B \times H$, where A is an Abelian group of odd order, B is a product of a finite number of two-element groups, and H is the eight element group of quarternions $\{\pm 1, \pm i, \pm j, \pm k\}$. The following lemma has been abstracted from Sehgal (1975). The result also appears in Pascaud (1973).

Lemma 3 (Sehgal). If $\mathbb{Q}(G)$ has no nilpotents, then G is Hamiltonian.

Proof. Observe first that if R is any ring with unit and no nilpotents, then an idempotent $e^2 = e$ in R commutes with every element of R. Indeed, the equation $0 = [er(1-e)]^2$ implies $er(1-e) = 0$, so $er = ere$. Similarly, $re = ere = er$. Now let $R = \mathbb{Q}(G)$, let H be a subgroup of G , and set $e = \frac{1}{|H|} \Sigma_{h \in H} h$. It follows that for each $g \in G$, $geg^{-1} = e$ and this implies that for each $h \in H$, $ghg^{-1} \in H$, so H is normal. □

Proof of Theorem 5. map $\mathbb{Q}(G)$ into $R_\rho(G)$ by mapping $g \mapsto \rho(g)$ and extending by linearity. This is an algebra homomorphism. We thus get a map from $\mathbb{Q}(G)$ into $\Pi_\rho R_\rho(G)$. From Proposition 10 of Serre (1977) this map is 1-1. Since no $R_\rho(G)$ has nilpotents, neither does $\mathbb{Q}(G)$. Lemma 3 implies that G has the form $G = A \times B \times H$ where A is an Abelian group of odd order. If A is not zero, choose a character χ taking at least one complex value. Let ρ be the irredicuble representation of H which sends $i \mapsto \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$ and $j \mapsto \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. Then $\chi \otimes \rho$ is an irreducible two-dimensional representation so $R_{\chi \otimes \rho}(G)$ consists of all 2×2 matrices, with complex entries, and so contains nilpotents. □

Spherical functions.

As Theorem 5 shows, the uniform distribution on many non-commutative groups has non-trivial square roots. We now show that if some symmetry restrictions are put on the factors, then roots do not exist. Let G be a compact group and H a closed subgroup. A probability μ on G is spherical if $\mu(h_1 A h_2) = \mu(A)$ for all measurable A in G and $h_1, h_2 \in H$. Spherical functions are the object of intensive study in modern harmonic analysis. See Dieudone (1978) for an extensive treatment. The pair (G,H) is called a Gelfand pair if the algebra of L_2 spherical functions is commutative. Many examples of Gelfand pairs in probability are discussed in a very useful survey by Letac (1981). Compact lie groups G and their maximal compact subgroups H form Gelfand pairs, so the proper rotations SO(3) and the rotations fixing a point are a concrete example. The group $G = S_n$ and subgroup S_{n-1} form a Gelfand pair. There is a well developed transform theory for Gelfand pairs based on zonal-spherical functions. These are spherical functions s on G with the property that

$$\int s(g)\, \mu_1 * \mu_2(dg) = \int s(g)\, \mu_1(dg) \int s(g)\, \mu_2(dg) ,$$

for any spherical probabilities μ_i. The theory shows that there are enough spherical functions to determine a measure and defines $\hat{\mu}(s) = \int s(g)\, \mu(dg)$. It now follows as in the Abelian case that the uniform distribution on a compact group G does not admit non-trivial square roots which are spherical with respect to a subgroup H such that (G,H) form a Gelfand pair.

References

Bondar, J. V. (1976). Borel cross-sections and maximal invariants. Ann. Statist. 4, 866-877.

Brown, M., and Solomon, H. (1979). On combining pseudo-random number generators. Ann. Statist. 7, 691-695.

Bovey, J. D. (1980). An approximate probability distribution for the order of elements of the symmetric group. Bull. London Math. Soc. 12, 41-46.

Cohen, P. J. (1959). Factorization in group algebras. Duke Math. J. 26, 199-205.

Diaconis, P., and Graham, R. L. (1977). Spearman's footrule as a measure of disarray. Jour. Roy. Statist. Soc. B 39, 262-268.

Dieudone, J. (1978). Treatise on Analysis VI. Academic Press: New York.

Dudewicz, E. J., and Dann, R. E. (1972). Equally likely dice sums do not exist. Amer. Statistician 26, #4, 41-42.

Furst, M., Hopcroft, J., and Luks , E. (1980). Polynomial time algorithms for permutation groups. Proc. 21st FOCS I, 36-41.

Gleason, A. (1952). Groups without small subgroups. Amer. Math. 56, 193-212.

Grenander, U. (1963). Probability on algebraic structures. Wiley: New York.

Hall, M. (1959). The Theory of Groups. Macmillan: New York.

Heyer, H. (1977). Probability Measures on Locally Compact Groups. Springer-Verlag: Berlin.

Hewitt, E., and Ross, K. (1963). Abstract Harmonic Analysis I. Springer-Verlag: Berlin.

Hewitt, E., and Ross, K. (1970). Abstract Harmonic Analysis II. Springer-Verlag: Berlin.

Hewitt, E., and Zukerman, H. (1966). Singular measures with absolutely continuous convolution squares. Proc. Camb. Phil. Soc. 62, 399-420.

Knuth, D. (1981). The Art of Computer Programming, Vol. II, 2nd ed. Addison Wesley: Reading, Massachusetts.

Letac, G. (1981). Problèms Classiques de Probabilitiè sur un Couple de Gelfand. In Lecture Notes in Mathematics, No. 860. Springer-Verlag: Berlin.

Levy, P. (1953). Premiers Elements de l'Arithmetique des Substitutions Aleatoires. C.R. Acad. Sci. 237, 1488-1489.

Lewis, T. (1967). The factorization of the rectangular distribution. J. Appl. Prob. 4, 529-542.

Lukacs, E. (1970). Characteristic Functions, 2nd Ed. Griffin: London.

Marshall, A. W., and Olkin, I. (1979). Inequalities: Theory of Majorization and its Applications. Academic Press: New York.

Pascaud, J. (1973). Anneaux de groups réduits: C.R. Acad. Sci. Paris, Sér. A 277, 719-722.

Rubin, H. (1967). Supports of convolutions of identical distributions. Proc. Fifth Berkeley Symp. on Mathematics, Statistics, and Probability. Vol. 2, 415-422.

Pontryagin (1966). Topological Groups, 2nd ed. Gordon and Breach: New York.

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

Serre, J. P. (1977). Linear Representations of Finite Groups. Springer-Verlag: New York

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER
312

2. GOVT ACCESSION NO.
AD-A109663

3. RECIPIENT'S CATALOG NUMBER

4. TITLE (and Subtitle)
FACTORING PROBABILITIES ON COMPACT GROUPS

5. TYPE OF REPORT & PERIOD COVERED
TECHNICAL REPORT

6. PERFORMING ORG. REPORT NUMBER

7. AUTHOR(s)
Persi Diaconis and Mehrdad Shashahani

8. CONTRACT OR GRANT NUMBER(s)
N00014-76-C-0475 & NSF GRANT MCS80-24649

9. PERFORMING ORGANIZATION NAME AND ADDRESS
Department of Statistics
Stanford University
Stanford, CA 94305

10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
NR-042-267

11. CONTROLLING OFFICE NAME AND ADDRESS
Office Of Naval Research
Statistics & Probability Program Code 436
Arlington, VA 22217

12. REPORT DATE
DECEMBER 2, 1981

13. NUMBER OF PAGES
16

14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)

15. SECURITY CLASS. (of this report)
UNCLASSIFIED

15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

APPROVED FOR PUBLIC RELEASE: DISTRIBUTION UNLIMITED.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

Also prepared under NSF GRANT MCS80-24649 and issued as Technical Report No. 178, Dept. of Statistics - Stanford University.

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Pseudo-random number generation; compact groups; non-parametric measures of correlation.

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

PLEASE SEE REVERSE SIDE.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

S/N 0102-LF-014-6601

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

#312

FACTORING PROBABILITIES ON COMPACT GROUPS

When can a probability P be factored as $P_1 * P_2$? This problem arises in efficient generation of pseudo random integers and permutations. It is thus natural to think of P defined on a group. We show that any strictly positive measure can be factored. The uniform distribution can be factored in a non-trivial way for any compact group having more than three elements. If it is required that $U = P * P$, then factorization is possible if and only if the group is not Abelian or the product of the quarternions and a finite number of two element groups.

ATE

LME