Version of 1.12.05

Squares in locally compact groups

D.H.Fremlin

University of Essex, Colchester, England

I investigate the measures of sets of squares in topological groups with Haar measures.

1 Sets of squares For a group X and a set $A \subseteq X$, write $A^{(2)}$ for $\{a^2 : a \in A\}$. Let X be a locally compact Hausdorff group and μ a left Haar measure on X. What can we say about the measure $\mu X^{(2)}$?

In general, $X^{(2)}$ need not even be measurable (see Example 2 below). But if X is σ-compact then $X^{(2)}$ is σ-compact and therefore measurable. If $X = \{-1,1\}^{\mathbb{N}}$, then $X^{(2)} = \{e\}$ is negligible; if $X = S^1$ then $X^{(2)} = X$ is conegligible; if $X = \{-1,1\} \times S^1$ then $\mu X^{(2)} = \frac{1}{2}\mu X$.

2 Example Let Y be the group $\{-1,1\}^{\mathbb{N}}$, so that Y is a compact Hausdorff group and $u^2 = e_Y$ for every $u \in Y$. Take any set $A \subseteq Y$ and let X be the set $[A]^{<\omega} \times Y$ with the multiplication defined by

$$(I,u)\cdot(J,v) = (I\triangle J, w_{I\cap J}uv),$$

where $w_K = \prod_{u\in K} u$ for $K \in [Y]^{<\omega}$. Then X is an abelian group. **P** (i)

$$\begin{aligned}((I,u)\cdot(J,v))\cdot(K,y) &= (I\triangle J, w_{I\cap J}uv)\cdot(K,y) = (I\triangle J\triangle K), w_{I\cap J}w_{(I\triangle J)\cap K}uvy)\\ &= (I\triangle J\triangle K), w_L uvy) = (I,u)\cdot((J,v))\cdot(K,y))\end{aligned}$$

where $L = (I\cap J)\cup(I\cap L)\cup(J\cap L)$. So X is a semigroup. (ii) Of course $\cdot$ is commutative. (iii) $(I,u)\cdot(\emptyset,e_Y) = (I,u)$ for all I and u, so X has identity $e_X = (\emptyset,e_Y)$. (iii) $(I,u)\cdot(I,w_I u^{-1}) = (\emptyset,e_Y)$ for all I and u, so X has inverses. **Q**

Give X the product topology when $[A]^{<\omega}$ is given the discrete topology; then X is a locally compact metrizable abelian topological group with a compact open subgroup $K = \{(\emptyset,u) : u \in Y\}$ homeomorphic to Y.

The set $\{x^2 : x \in X\} = \{(\emptyset,w_I) : I \in [A]^{<\omega}\} \subseteq K$ can be identified with the subgroup of Y generated by A. So this can be either non-measurable or measurable with non-zero measure. Note that $K^{(2)} = \{e_X\}$ is negligible.

3 Proposition For any $n \ge 1$ there is a finite group X such that $\dfrac{\#(X^{(2)})}{\#(X)} = 1 - \dfrac{1}{2^n}$.

proof Let F be a field with 2^n elements and X the set of non-singular upper triangular 2×2 matrices over F. If $\begin{pmatrix} a & b \\ 0 & d\end{pmatrix} \in X$, then it is a square (in X) iff either $b = 0$ or $a \ne d$. **P** The square of $\begin{pmatrix} x & y \\ 0 & z\end{pmatrix}$ is $\begin{pmatrix} x^2 & y(x+z) \\ 0 & z^2\end{pmatrix}$. Since every element of F is a square (the map $t \mapsto t^2$ is injective; also the multiplicative group $F\setminus\{0\}$ has odd order), every element of F has a unique square root, and we can solve the equations

$$x^2 = a,\quad y(x+z) = b,\quad z^2 = d$$

iff we can solve the equation $y(\sqrt{a}+\sqrt{d}) = b$, that is, iff either $a \ne d$ or $b = 0$. **Q**

So the number of non-squares in X is just $(2^n-1)^2$, while $\#(X) = 2^n(2^n-1)^2$, and we have the ratio sought.

4 Corollary For any $\alpha \in [0,1]$ there is a compact Hausdorff group X such that $\mu X^{(2)} = \alpha$, where μ is the Haar probability measure on X.

proof If $\alpha = 1$ take $X = \{e\}$. Otherwise, by Proposition 3, we can choose a sequence $\langle X_n\rangle_{n\in\mathbb{N}}$ of finite groups such that, setting $\alpha_n = \#(X_n^{(2)})/\#(X_n)$, we have $\prod_{n=0}^{\infty}\alpha_n = \alpha$; now take $X = \prod_{n\in\mathbb{N}} X_n$.

5 Remark Note that if X is a compact abelian Hausdorff group with Haar probability measure μ, $\mu X^{(2)}>0$ and $X^{(2)}\ne X$, then $\mu X^{(2)}=2^{-n}$ for some $n\ge 1$. **P** $X^{(2)}$ is a non-negligible compact subgroup of X so is open. Because X is compact, it can be covered by finitely many cosets of $X^{(2)}$ and the quotient group $Z=X/X^{(2)}$ is finite. Moreover, $z^2=e_Z$ for every $z\in Z$, so $\#(Z)=2^n$ for some n; we are supposing that $X^{(2)}\ne X$ so $n\ge 1$. Now $X^{(2)}$ has just 2^n cosets in X so $\mu X^{(2)}=2^{-n}$. **Q**

6 Proposition (M.R.Burke) Let X be an abelian locally compact σ-compact Hausdorff topological group and μ a Haar measure on X. Suppose that $\mu X^{(2)}>0$. Then $A^{(2)}$ is non-negligible whenever $A\subseteq X$ is non-negligible.

proof (a) To begin with, suppose that X is metrizable, therefore Polish. Because X is abelian, $X^{(2)}$ is a subgroup, and $x\mapsto x^2:X\to X^{(2)}$ is a continuous homomorphism; let $Y=\{x:x^2=e\}$ be its kernel, so that Y is a closed subgroup. Let $Z=X/Y$ be the quotient group. If x, $y\in X$, then $x^2=y^2$ iff $x^{-1}y\in Y$ iff $xY=yY$; so we have a group isomorphism $\phi:X^{(2)}\to Z$ defined by saying that $\phi(x^2)=xY$ for every $x\in X$. Now $\phi^{-1}:Z\to X^{(2)}$ is continuous. **P** If U is any neighbourhood of the identity in $X^{(2)}$, there is a neighbourhood V of the identity such that $V^2\subseteq U$; now $V'=\{xY:x\in V\}$ is a neighbourhood of the identity in Z and $\phi^{-1}(z)\in U$ for every $z\in V'$. **Q**

$X^{(2)}$ is σ-compact, therefore Haar measurable, and we are supposing that it is not Haar negligible; it must therefore be an open set in X, and both Z and $X^{(2)}$ are Polish. So ϕ is a Borel measurable homomorphism between Polish groups and must be continuous. Thus ϕ is a topological group isomorphism.

If $K\subseteq X$ is compact and not Haar negligible, then $K'=\{xY:x\in K\}$ is non-negligible in Z (Fremlin 03, 443Pe). Now $K^{(2)}=\phi^{-1}[K']$ must be non-negligible for Haar measure on $X^{(2)}$ and therefore for Haar measure on X.

? If $A^{(2)}$ is Haar negligible in X, then there is a negligible Borel set $E\subseteq X$ including $A^{(2)}$, and $F=\{x:x^2\in E\}$ is a Borel set including A. F includes a non-negligible compact set K such that $K^{(2)}\subseteq E$ is negligible, which is impossible. **X**

(b) For the general case, **?** suppose, if possible, that $A^{(2)}$ is negligible. Because μ is inner regular with respect to the zero sets (Fremlin 03, 443M), there is a sequence $\langle K_n\rangle_{n\in\mathbb{N}}$ of zero sets such that $\bigcup_{n\in\mathbb{N}}K_n$ is a conegligible subset of $X\setminus A^{(2)}$. For each $n\in\mathbb{N}$ there is a sequence $\langle V_{ni}\rangle_{i\in\mathbb{N}}$ of neighbourhoods of the identity such that $K_n=\bigcap_{i\in\mathbb{N}}V_{ni}$. Let Y be a compact normal subgroup of X included in $\bigcap_{n,i\in\mathbb{N}}V_{ni}$ such that $Z=X/Y$ is metrizable (Fremlin 03, 4A5S). There is a Haar measure ν on Z such that the canonical map $\pi:X\to Z$ is inverse-measure-preserving (Fremlin 03, 443Pd); consequently $\nu^*(\pi[A])>0$. On the other hand, $C=X\setminus\bigcup_{n\in\mathbb{N}}K_n$ is μ-negligible and $CY=Y$, so $\pi[C]$ is ν-negligible and $z^2\in\pi[C]$ for every $z\in\pi[A]$, contradicting (a) above. **X**

7 Examples (a) Let K_4 be a non-cyclic group of order 4, so that $K_4=\{e,a,b,c\}$ where $a^2=b^2=c^2=e$. Let $\mathrm{Aut}(K_4)$ be its automorphism group, so that $\mathrm{Aut}(K_4)$ is isomorphic to the group of all permutations on $\{a,b,c\}$. If $\psi\in\mathrm{Aut}(K_4)$ is such that $\psi(a)=b$, $\psi(b)=c$ and $\psi(c)=a$, then $K_4=\{t\psi(t):t\in K_4\}$. **P** $e=e\psi(e)$, $a=bc=b\psi(b)$ etc. **Q**

Set $K=K_4^{\mathbb{N}}$, so that K is a compact metrizable group and $\{z^2:z\in K\}$ has one point, so is Haar negligible. For $\phi\in\mathrm{Aut}(K_4)$, define $\tilde\phi:K\to K$ by setting $\tilde\phi(z)(n)=\phi(z(n))$ for $z\in K$ and $n\in\mathbb{N}$. Then $\phi\mapsto\tilde\phi$ is a homomorphism from $\mathrm{Aut}(K_4)$ to $\mathrm{Aut}_c(K)$, the group of topological-group-automorphisms of K. We can therefore form a semidirect product $X=\mathrm{Aut}(K_4)\times K$ with multiplication given by

$$(\phi_1,z_1)\cdot(\phi_2,z_2)=(\phi_1\phi_2,z_1\tilde\phi_1(z_2)),$$

and X will be a compact metrizable topological group if it is given the product topology ($\mathrm{Aut}(K_4)$ being given its discrete topology, of course).

For any $z\in K$, we have a $w\in K$ such that $w(n)\phi(w(n))=z(n)$ for every n. So $\{x^2:x\in X\}$ contains

$$(\phi,w)^2=(\phi^2,w\tilde\phi(w))=(\phi^2,z).$$

But this means that $X^{(2)}$ includes the coset $\{(\phi^2,z):z\in K\}$ and has measure at least $\frac{1}{6}$ if X is given its Haar probability measure.

On the other hand, the open subgroup $Y=\{(\iota,z):z\in K\}$ is isomorphic to K so $Y^{(2)}$ is negligible, while Y is not.

(b) Let G be 'the' non-abelian group of order 21, so that G has Sylow subgroups G_3, G_7 of orders 3 and 7 respectively, G_7 is normal and for suitable generators a, b of G_3, G_7 we have $aba^{-1} = b^2$. It is easy to check that $G_7 = \{hghg^{-1} : h \in G_7\}$ for every $g \in G_3$. Set $K = G_7^{\mathbb{N}}$ and consider the action $\bullet$ of G_3 on K defined by setting $g\bullet\langle h_n\rangle_{n\in\mathbb{N}} = \langle gh_ng^{-1}\rangle_{n\in\mathbb{N}}$ for $g \in G_3$, $\langle h_n\rangle_{n\in\mathbb{N}} \in K$. Then for every $g \in G_3$ the map $z \mapsto z(g\bullet z) : K \to K$ is a measure-preserving bijection. So if we take X to be the corresponding semidirect product $G_3 \times K$, with the multiplication

$$(g_1, z_1) \cdot (g_2, z_2) = (g_1g_2, z_1(g_1\bullet z_2))$$

and the product topology, we shall have $X^{(2)} = X$ and the map $x \mapsto x^2 : X \to X$ is a Haar-measure-preserving homeomorphism.

8 Definition Let X be a compact Hausdorff group, and μ its Haar probability measure. I will say that X has **property (†)** if

$$\mu\{x : x^2 \in K\} \geq \mu K$$

for every compact $K \subseteq X^{(2)}$.

9 Proposition (a) Any finite group has property (†).

(b) Any abelian compact Hausdorff group has property (†).

(c) Any product of compact Hausdorff groups with property (†) has property (†).

(d) If X is a compact Hausdorff group and every finite-dimensional representation of X has property (†), then X has property (†).

(e) The two groups of Example 7 have property (†).

proof (a) This is trivial, as $\#(\{x : x^2 \in K\}) \geq \#(K)$ for every $K \subseteq X^{(2)}$.

(b) Let X be a compact Hausdorff group with Haar probability measure μ, and $K \subseteq X^{(2)}$ a compact set; set $A = \{x : x^2 \in K\}$. If $\mu X^{(2)} = 0$ then of course $\mu A \geq 0 = \mu K$. Otherwise, $X^{(2)}$ is an open subgroup of X. Let Y be the closed subgroup $\{x : x^2 = e\}$. As in Proposition 6, we have an isomorphism $\phi : X^{(2)} \to X/Y$ defined by setting $\phi(x^2) = xY$ for every $x \in X$. Because ϕ has a closed graph it is a homeomorphism and is a measure space isomorphism for the Haar probability measures of $X^{(2)}$ and X/Y. Now the Haar probability measure on $X^{(2)}$ is just a scalar multiple of the subspace measure $\mu_{X^{(2)}}$. So

$$\mu A = \mu(AY) = \lambda\{xY : x \in A\}$$

(where λ is the Haar probability measure of X/Y)

$$= \frac{1}{\mu X^{(2)}}\mu(\phi^{-1}[\{xY : x \in A\}]) = \frac{1}{\mu X^{(2)}}\mu A^{(2)} \geq \mu A^{(2)} = \mu K.$$

(c) Let $\langle X_i\rangle_{i\in I}$ be a family of compact Hausdorff groups with property (†), and X their product. For each $i \in I$, let μ_i be the Haar probability measure on X_i, $f_i : X_i \to X_i^{(2)}$ the squaring map, ν_i the image measure $\mu_i f_i^{-1}$ on $X_i^{(2)}$, and λ_i the subspace measure on $X_i^{(2)}$. Then property (†) asserts that $\lambda_i K \leq \nu_i K$ for every compact $K \subseteq X_i^{(2)}$; as both λ_i and ν_i are Radon measures, $\lambda_i E \leq \nu_i E$ whenever $E \subseteq X_i^{(2)}$ is measured by ν_i (Fremlin 03, 416E).

Now $X^{(2)} = \prod_{i\in I} X_i^{(2)}$ and the Haar probability measure of X is just the Radon product of the measures μ_i (Fremlin 03, 441Xi). Writing $f(x) = x^2$ for $x \in X$, $f : X \to X^{(2)}$ is inverse-measure-preserving for μ and the product ν of $\langle \nu_i\rangle_{i\in I}$. Let λ be the subspace measure on $X^{(2)}$. For any measurable cylinder set C in $X^{(2)} = \prod_{i\in I} X_i^{(2)}$, we have

$$\lambda C = \mu C = \prod_{i\in I} \mu_i C_i$$

(where $C = \prod_{i\in I} C_i$)

$$= \prod_{i \in I} \lambda_i C_i \le \prod_{i \in I} \nu_i C_i = \nu C;$$

so $\lambda W \le \nu W$ whenever W is a finite disjoint union of measurable cylinder sets, therefore for any finite union of measurable cylinder sets. Now the set of such finite unions includes a base for the topology of $X^{(2)}$, and both λ and ν are Radon measures, so $\lambda W \le \nu W$ whenever ν measures W (FREMLIN 03, 415G(iv)). But this means that $\lambda K \le \nu K = \mu f^{-1}[K]$ for every compact $K \subseteq X^{(2)}$, and X has property (†).

(d) Suppose that $K \subseteq X^{(2)}$ is compact and let $\epsilon > 0$. Set $A = \{x : x^2 \in K\}$. Then there is a neighbourhood U of the identity in X such that $\mu(AU) \le \mu A + \epsilon$, where μ is the Haar probability measure on X. Let $\phi : X \to GL(r, \mathbb{R})$ be a representation of X with kernel $Y \subseteq U$ (FREMLIN 03, 446C). Let ν be the image measure $\mu\phi^{-1}$ on $Z = \phi[X]$, so that ν is Haar probability measure on Z. Then $\phi[K] \subseteq Z^{(2)}$ and $z^2 \in \phi[K]$ for every $z \in \phi[A]$, so

$$\begin{aligned}\epsilon + \mu A \ge \mu(AU) \ge \mu(AY) &= \mu\phi^{-1}[\phi[A]] \\ &= \nu\phi[A] \ge \nu\phi[K] = \mu(KY) \ge \mu K.\end{aligned}$$

As ϵ is arbitrary, $\mu A \ge \mu K$; as K is arbitrary, X has property (†).

(e)(i) Consider first the group X of 7a. The point is that the maps $t \mapsto t\psi(t)$ and $t \mapsto t\psi^2(t) : K_4 \to K_4$ are bijections, so $w \mapsto w\tilde{\psi}(w)$ and $w \mapsto \tilde{\psi}^2(w) : K \to K$ are measure space isomorphisms. On the other hand, if $\sigma \in \mathrm{Aut}(K_4) \setminus \{\psi, \psi^2\}$ then $\{t\sigma(t) : t \in K_4\}$ has at most two members and $\{w\tilde{\sigma}(w) : w \in K\}$ is negligible. So if $L \subseteq X^{(2)}$ is compact, then

$$\mu L = \frac{1}{6}(\nu\{z : (\psi, z) \in L\} + \nu\{z : (\psi^2, z) \in L\})$$

(where μ is the Haar probability measure of X and ν is the Haar probability measure of K)

$$\begin{aligned}&= \frac{1}{6}(\nu\{w : (\psi, w\tilde{\psi}^2(w)) \in L\} + \nu\{w : (\psi^2, w\tilde{\psi}(w)) \in L\}) \\ &= \frac{1}{6}(\nu\{w : (\psi^2, w)^2 \in L\} + \nu\{w : (\psi, w)^2 \in L\}) \le \mu\{x : x^2 \in L\}.\end{aligned}$$

(ii) Of course the group of 7b also has property (†) because $x \mapsto x^2$ is inverse-measure-preserving for Haar measure.

10 Proposition Let X be a compact Hausdorff group with property (†), and μ its Haar probability measure. If $A \subseteq X$ then

$$\mu^* A + \mu X^{(2)} \le 1 + \mu^* A^{(2)}, \quad \mu_* A + \mu X^{(2)} \le 1 + \mu_* A^{(2)}.$$

proof (a) To begin with, suppose that A is compact, so that $A^{(2)}$ is measurable. Take any $\epsilon > 0$. Then there is a compact set $L \subseteq X^{(2)} \setminus A^{(2)}$ such that $\mu K \ge \mu X^{(2)} - \mu A^{(2)} - \epsilon$. Set $F = \{x : x^2 \in L\}$; then $F \cap A = \emptyset$ and $\mu F \ge \mu L$, so

$$\mu A + \mu X^{(2)} \le 1 - \mu F + \mu X^{(2)} \le 1 - \mu L + \mu X^{(2)} \le 1 + \mu A^{(2)} + \epsilon.$$

As ϵ is arbitrary, $\mu A + \mu X^{(2)} \le 1 + \mu A^{(2)}$.

(b) For the general case, **?** suppose, if possible, that $1 + \mu^* A^{(2)} < \mu^* A + \mu X_2$. Let $E \supseteq A^{(2)}$ be a Borel set such that $\mu E = \mu^* A^{(2)}$, and set $F = \{x : x^2 \in E\}$; then F is a Borel set including A, so $1 + \mu E < \mu F + \mu X_2$. Let $K \subseteq F$ be a compact set such that $1 + \mu E < \mu K + \mu X_2$; then $K^{(2)} \subseteq E$ so $1 + \mu K^{(2)} \le 1 + \mu E < \mu K + \mu X_2$, contradicting (a). **X**

As for lower measures, there is a K_σ set $G \subseteq A$ such that $\mu G = \mu_* A$. Now $G^{(2)}$ is still K_σ, so

$$\mu_* A + \mu X_2 = \mu^* G + \mu X_2 \le 1 + \mu^* G^{(2)} \le 1 + \mu_* A^{(2)}.$$

11 Proposition Let X be a finite group. If $A \subseteq B \subseteq X$, then $\#(A) + \#(B^{(2)}) \le \#(B) + \#(A^{(2)})$.

proof We have only to note that $\#(A) - \#(f[A]) \le \#(B) - \#(f[B])$ for any function f defined on X, and in particular when $f(x) = x^2$.

Remark Note that if $X = (S^1)^{\mathbb{N}}$, $K = \{e\}$ and $L = \{x : \mathcal{R}\mathrm{e}\, x(n) \ge 0 \text{ for every } n \in \mathbb{N}\}$, then $\mu K + \mu L^{(2)} = 1$ but $\mu L + \mu K^{(2)} = 0$. So we do not have a direct translation of the result here which is valid for infinite groups, even if they are compact, metrizable and abelian.

12 Example The group SO(3) of orthogonal 3×3 matrices with determinant 1 does not have property (†).

proof (a) Every element of SO(3) except the identity e is a rotation. Its square (if not the identity) is a rotation about the same axis; so every element of SO(3) except e has exactly two square roots; in particular, $\mathrm{SO}(3)^{(2)} = \mathrm{SO}(3)$.

For a 3×3-matrix $a = \langle \alpha_{ij} \rangle_{i,j<3}$ write $\|a\|_{HS} = \sqrt{\sum_{i,j<3} \alpha_{ij}^2}$. Note that (i) for any 3×3-matrices a and b, $\|ab\|_{HS} \le \|a\|_{HS}\|b\|_{HS}$ (ii) if $x \in \mathrm{SO}(3)$ then $\|xa\|_{HS} = \|a\|_{HS} = \|ax\|_{HS}$ for every a. So we have a two-sided-invariant metric on SO(3) defined by setting $\rho(x, y) = \|x - y\|_{HS}$ for all x, $y \in \mathrm{SO}(3)$. SO(3) is a compact topological group under this metric.

SO(3) is a three-dimensional manifold, so three-dimensional Hausdorff measure μ_{H3} on SO(3) is finite and not zero, and is a Haar measure on SO(3); call this measure μ.

(b) If $e + a \in \mathrm{SO}(3)$ then

$$e = (e + a)(e + a^T) = e + (a + a^T) + aa^T$$

so $\|a + a^T\|_{HS} \le \|a\|_{HS}^2$. If we set $b = \frac{1}{2}(a - a^T)$ then

$$\|a - b\|_{HS} = \tfrac{1}{2}\|a + a^T\|_{HS} \le \tfrac{1}{2}\|a\|_{HS}^2.$$

If $x \in \mathrm{SO}(3)$ and $y = x(e + a)$ then

$$\begin{aligned}\|y^2 - x^2\|_{HS} &= \|xax + xaxa + x^2a\|_{HS} = \|ax + xa + axa\|_{HS} \\ &\ge \|bx + xb\|_{HS} - 2\|a - b\|_{HS} - \|a\|_{HS}^2 \ge \|bx + xb\|_{HS} - \frac{3}{2}\|a\|_{HS}^2.\end{aligned}$$

(c) Set $z = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{SO}(3)$, so that the two square roots of z are $z_1 = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ and $z_2 = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. If $b = \begin{pmatrix} 0 & s & t \\ -s & 0 & u \\ -t & -u & 0 \end{pmatrix}$ is antisymmetric, then

$$\begin{aligned} z_1b + bz_1 &= \begin{pmatrix} 0 & s & t \\ -s & 0 & u \\ -t & -u & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & s & t \\ -s & 0 & u \\ -t & -u & 0 \end{pmatrix} \\ &= \begin{pmatrix} -2s & 0 & t + u \\ 0 & -2s & u - t \\ u - t & -t - u & 0 \end{pmatrix}\end{aligned}$$

so

$$\begin{aligned}\|z_1b + bz_1\|_{HS} &= \sqrt{8s^2 + 2(t + u)^2 + 2(t - u)^2} = \sqrt{8s^2 + 4t^2 + 4u^2} \\ &\ge \sqrt{2}\sqrt{2s^2 + 2t^2 + 2u^2} = \sqrt{2}\|b\|_{HS}.\end{aligned}$$

Putting this together with the formulae in (b), we see that if a is such that $e + a \in \mathrm{SO}(3)$, $y = z_1(e + a)$ and $b = \frac{1}{2}(a - a^T)$ then

$$\begin{aligned}\|y^2 - z\|_{HS} &\ge \|bz_1 + z_1 b\|_{HS} - \frac{3}{2}\|a\|_{HS}^2 \ge \sqrt{2}\|b\|_{HS} - \frac{3}{2}\|a\|_{HS}^2 \\ &\ge \sqrt{2}\|a\|_{HS} - \frac{\sqrt{2}}{2}\|a\|_{HS}^2 - \frac{3}{2}\|a\|_{HS}^2 \\ &\ge \sqrt{2}\|a\|_{HS} - 3\|a\|_{HS}^2 = \sqrt{2}\|y - z_1\|_{HS} - 3\|y - z_1\|_{HS}^2.\end{aligned}$$

Similarly,

$$\|y^2 - z\|_{HS} \ge \sqrt{2}\|y - z_2\|_{HS} - 3\|y - z_2\|_{HS}^2$$

for every $y \in \mathrm{SO}(3)$.

(d) There is a $\delta > 0$ such that $2\delta < \|z_1 - z_2\|_{HS}$ and $\|y^2 - x^2\|_{HS} \ge \frac{7}{5}\|y - x\|_{HS}$ whenever x, $y \in \mathrm{SO}(3)$ and $\|x - z_j\|_{HS}$, $\|y - z_j\|_{HS}$ are both less than or equal to δ for some j. Let $\eta > 0$ be such that $\eta < \|z - e\|_{HS}$ and whenever $x \in \mathrm{SO}(3)$ and $\|x^2 - z\|_{HS} \le \eta$ then $\|x - z_j\|_{HS} \le \delta$ for some j. Set $K = \{w : w \in \mathrm{SO}(3), \|w - z\|_{HS} \le \eta\}$. Every element of K has two square roots and they cannot both belong to $B(z_j, \delta)$ for the same j. So we have two square-root functions f_1, f_2 defined on K by saying that $f_j(w)^2 = w$ and $\|f_j(w) - z_j\|_{HS} \le \delta$ for each j. By the choice of δ, $\|f_j(w) - f_j(w')\|_{HS} \le \frac{5}{7}\|w - w'\|_{HS}$ for all w, $w' \in K$. So $\mu f_j[K] \le (\frac{5}{7})^3 \mu K < \frac{1}{2}\mu K$ for both j. But this means that

$$L = \{x : x^2 \in K\} = f_1[K] \cup f_2[K]$$

has measure less than μK, and we have our example.

alternative proof If we go to a bit more trouble we have a more informative argument, as follows.

(a) SO(3) can be parametrized as the set of matrices

$$\phi\begin{pmatrix} z \\ \alpha \\ \theta \end{pmatrix} = \begin{pmatrix} z & -\cos\theta\sqrt{1-z^2} & \sin\theta\sqrt{1-z^2} \\ \cos\alpha\sqrt{1-z^2} & z\cos\alpha\cos\theta - \sin\alpha\sin\theta & -z\cos\alpha\sin\theta - \sin\alpha\cos\theta \\ \sin\alpha\sqrt{1-z^2} & z\sin\alpha\cos\theta + \cos\alpha\sin\theta & -z\sin\alpha\sin\theta + \cos\alpha\cos\theta \end{pmatrix}$$

with $z \in [-1, 1]$, $\alpha \in \,]-\pi, \pi]$ and $\theta \in \,]-\pi, \pi]$. **P** If $x \in \mathrm{SO}(3)$ its first column is of the form $\begin{pmatrix} z \\ \cos\alpha\sqrt{1-z^2} \\ \sin\alpha\sqrt{1-z^2} \end{pmatrix}$ for some $z \in [-1, 1]$ and $\alpha \in [-\pi, \pi]$. Now an orthonormal basis for the subspace orthogonal to this vector is given by the vectors $\begin{pmatrix} -\sqrt{1-z^2} \\ z\cos\alpha \\ z\sin\alpha \end{pmatrix}$ and $\begin{pmatrix} 0 \\ -\sin\alpha \\ \cos\alpha \end{pmatrix}$; rotating this 2-dimensional subspace through an angle θ we get the proposed matrix. **Q**

(b) Now we can calculate the 9×3 matrix which is the derivative of ϕ at $\begin{pmatrix} z \\ \alpha \\ \theta \end{pmatrix}$; it is

$$T = \begin{pmatrix} 1 & 0 & 0 \\ \frac{z\cos\theta}{\sqrt{1-z^2}} & 0 & \sin\theta\sqrt{1-z^2} \\ -\frac{z\sin\theta}{\sqrt{1-z^2}} & 0 & \cos\theta\sqrt{1-z^2} \\ -\frac{z\cos\alpha}{\sqrt{1-z^2}} & -\sin\alpha\sqrt{1-z^2} & 0 \\ \cos\alpha\cos\theta & -z\sin\alpha\cos\theta - \cos\alpha\sin\theta & -z\cos\alpha\sin\theta - \sin\alpha\cos\theta \\ -\cos\alpha\sin\theta & z\sin\alpha\sin\theta - \cos\alpha\cos\theta & -z\cos\alpha\cos\theta + \sin\alpha\sin\theta \\ -\frac{z\sin\alpha}{\sqrt{1-z^2}} & \cos\alpha\sqrt{1-z^2} & 0 \\ \sin\alpha\cos\theta & z\cos\alpha\cos\theta - \sin\alpha\sin\theta & -z\sin\alpha\sin\theta + \cos\alpha\cos\theta \\ -\sin\alpha\sin\theta & -z\cos\alpha\sin\theta - \sin\alpha\cos\theta & -z\sin\alpha\cos\theta - \cos\alpha\sin\theta \end{pmatrix}.$$

So $T'T = \begin{pmatrix} \frac{2}{\sqrt{1-z^2}} & 0 & 0 \\ 0 & 2 & 2z \\ 0 & 2z & 2 \end{pmatrix}$ has constant determinant. Let λ be Lebesgue measure on $[-1,1]\times\,]-\pi,\pi]\times\,]-\pi,\pi]$. By FREMLIN 01, 265E the image measure $\lambda\phi^{-1}$ is a multiple of normalized 3-dimensional Hausdorff measure on SO(3), and is invariant, so is a Haar measure.

(c) If $x \in \mathrm{SO}(3)$ is a rotation through an angle $\gamma(x) \in [0,\pi]$, then its trace $\mathrm{tr}(x)$ is $1+2\cos\gamma(x)$. **P** Because $\mathrm{tr}(ab) = \mathrm{tr}(ba)$ for all 3×3 matrices a, b, $\mathrm{tr}(axa^{-1}) = \mathrm{tr}(x)$ for every $a \in \mathrm{SO}(3)$. Now there is some $a \in \mathrm{SO}(3)$ such that axa^{-1} is of the form $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\gamma(x) & \sin\gamma(x) \\ 0 & -\sin\gamma(x) & \cos\gamma(x) \end{pmatrix}$ and has trace $1+2\cos\gamma(x)$. **Q**

(d) This means that for $t \in [0,\pi]$

$$\begin{aligned}\Pr(\gamma(x)\le t) &= \Pr(\cos\gamma(x)\ge\cos t) = \Pr(\mathrm{tr}(x)\ge 1+2\cos t)\\ &= \Pr(\mathrm{tr}(\phi\begin{pmatrix} z\\ \alpha\\ \theta\end{pmatrix})\ge 1+2\cos t)\end{aligned}$$

(when $z \in [-1,1]$, $\alpha \in\,]-\pi,\pi]$ and $\theta \in\,]-\pi,\pi]$ are independent and uniformly distributed)

$$\begin{aligned}&= \Pr(z + z\cos\alpha\cos\theta - \sin\alpha\sin\theta - z\sin\alpha\sin\theta + \cos\alpha\cos\theta \ge 1+2\cos t)\\ &= \Pr(z + z\cos(\alpha+\theta) + \cos(\alpha+\theta) \ge 1+2\cos t)\\ &= \Pr(z + z\cos\beta + \cos\beta \ge 1+2\cos t)\end{aligned}$$

(when $z \in [-1,1]$, $\beta \in [-\pi,\pi]$ are independent and uniformly distributed)

$$= \frac{1}{2\pi}\int_{-\pi}^{\pi}\Pr(z \ge \tfrac{1+2\cos t-\cos\beta}{1+\cos\beta})d\beta = \frac{1}{2\pi}\int_{-t}^{t}\frac{1}{2}(1-\tfrac{1+2\cos t-\cos\beta}{1+\cos\beta})d\beta$$

(because if $t < |\beta| \le \pi$ then $\frac{1+2\cos t-\cos\beta}{1+\cos\beta} > 1$)

$$\begin{aligned}&= \frac{1}{2\pi}\int_{-t}^{t}(1-\tfrac{1+\cos t}{1+\cos\beta})d\beta = \frac{t}{\pi} - \frac{1+\cos t}{\pi}\int_0^t \frac{1}{1+\cos\beta}d\beta\\ &= \frac{t}{\pi} - \frac{1+\cos t}{\pi}\tan\frac{t}{2} = \frac{t-\sin t}{\pi}.\end{aligned}$$

Accordingly the probability density function of the random variable $\gamma(x)$ is $\frac{1}{\pi}(1-\cos t)$ for $0 \le t \le \pi$, and in particular is strictly increasing.

(e) Now try

$$K = \{x : \gamma(x) \ge \tfrac{2\pi}{3}\}, \quad L = \{x : x^2 \in K\} = \{x : \tfrac{\pi}{3} \le \gamma(x) \le \tfrac{2\pi}{3}\}.$$

Because the probability density function of $\gamma(x)$ is strictly increasing, $\mu L < \mu K$ and SO(3) does not have property (†).

13 Corollary In $X = \mathrm{SO}(3)^{\mathbb{N}}$ there is a negligible set E such that $\{y : y^2 \in E\}$ is conegligible.

proof Take K and L such that $L = \{x : x^2 \in K\}$ and $\mu L < \mu K$, where μ is Haar probability measure on SO(3). Then $\mu(\mathrm{SO}(3)\setminus K) < \mu(\mathrm{SO}(3)\setminus L) \le 1$ so there is a sequence $\langle r_n\rangle_{n\in\mathbb{N}}$ in $\mathbb{N}$ such that

$$\textstyle\sum_{n=0}^{\infty}\mu(\mathrm{SO}(3)\setminus K)^{r_n} < \infty, \quad \sum_{n=0}^{\infty}\mu(\mathrm{SO}(3)\setminus L)^{r_n} = \infty.$$

Let $\langle I_n\rangle_{n\in\mathbb{N}}$ be a disjoint sequence of subsets of $\mathbb{N}$ such that $\#(I_n) = r_n$ for every n, and set

$$E = \{y : y \in X,\ \{n : y(i) \in \mathrm{SO}(3)\setminus K \text{ for every } i \in I_n\} \text{ is infinite}\}.$$

Then E is negligible. But

$$\{y : y^2 \in E\} = \{y : y \in X,\ \{n : y(i) \in \mathrm{SO}(3) \setminus L \text{ for every } i \in I_n\} \text{ is infinite}\}$$

is conegligible.

Remark Since $X^{(2)} = X$, this gives a stronger example to add to Example 7a.

14 Problems (a) For which rational $\alpha \in]0, 1]$, if not all, is there a finite group X such that $\frac{\#(X^{(2)})}{\#(X)} = \alpha$?

(b) Is there a compact Hausdorff group X such that $X^{(2)} = X$ but $U^{(2)}$ is nowhere dense for some non-empty open $U \subseteq X$?

Acknowledgements Conversations with M.R.Burke, S.Solecki, A.W.Miller, K.Kunen, J.Hart; hospitality of M.R.Burke, A.W.Miller, University of Wisconsin (Madison), University of Illinois (Urbana).

References

Fremlin D.H. [03] *Measure Theory, Vol. 4: Topological Measure Spaces.* Torres Fremlin, 2003.