ELEMENTS WITH SQUARE ROOTS IN COMPACT GROUPS

F. G. RUSSO

Abstract. The probability that a randomly chosen element has a square root is studied in [1, 2, 8] in the finite case. Here we deal with the infinite case.

1. The compact case

It is well–known that a compact group G has a unique probability measure space $(G, \mathcal{M}, \mu)$, where μ is the normalized Haar measure on G. In particular, μ is a left–invariant positive Radon measure on the σ–algebra $\mathcal{M}$ containing the Borel sets. Furthermore μ is finitely additive. This terminology is standard and details can be found in [7]. We will refer always to G as a compact group and to μ as the measure just described. Note that groups admitting such a measure are called amenable: abelian groups are amenable, but already the free group on two generators is not amenable, as it is known. Then the nonabelian case is significant.

The map $f : x \in G \mapsto x^2 \in G$ is continuous and closed, then

$$f(G) = \{x^2 \mid x \in G\} = G^2 \tag{1.1}$$

is a measurable closed subset of G and it is meaningful to define

$$p(G) = \mu(G^2) \tag{1.2}$$

as the *probability that a randomly chosen element in G has a square root*. If G is finite, then μ becomes the counting measure on G, and we get

$$p(G) = \frac{|G^2|}{|G|}, \tag{1.3}$$

which was investigated in [1, 2, 8].

The aim of the present paper is to extend to the infinite case the results of [1, 2, 8]. We follow the ideas in [4, 5, 9], because they use some general arguments of P. Erdös, W. H. Gustafson and P. Turan in [3, 6].

2. General properties

The next lemma expresses (1.2) in terms of finite index subgroups.

Lemma 2.1. *Let H be a closed subgroup of G and $n \geq 1$. If $|G : H| = n < \infty$, then $\mu(H) = \frac{1}{n}$. If $|G : H| = \infty$, then $\mu(H) = 0$.*

Date: received: 06 August 2009; revised: 23 February 2010.
Key words and phrases. elements with square roots; probability; compact groups.
AMS Subject Classification 2010: 20D60; 20P05.

Proof. Assume that $|G:H|=n$ is finite. Then $G=\bigcup_{i=1}^{n} g_iH$. So we have

$$1=\mu(G)=\mu(\bigcup_{i=1}^{n} g_iH)=\sum_{i=1}^{n}\mu(g_iH)=\sum_{i=1}^{n}\mu(H)=n\mu(H) \tag{2.1}$$

and therefore $\mu(H)=\frac{1}{n}$. Now assume that $|G:H|=\infty$ and $\alpha=\mu(H)$. If $\alpha>0$, then $t\alpha>1$ for some positive integer t. By assumption, $G=\bigcup_{i\in I} g_iH$, where I is an infinite set. Choose a subset J of I of cardinality t. It follows that

$$1=\mu(G)\geq\mu(\bigcup_{j\in J} g_jH)\geq\sum_{j\in J}\mu(g_jH)=t\alpha>1. \tag{2.2}$$

This contradicts $\mu(H)>0$ and the proof of the lemma follows. □

In general G^2 is not a subgroup of G but this is true in the abelian case.

Remark 2.2. By Lemma 2.1, if G is abelian, then $p(G)=\mu(G^2)=\frac{1}{|G:G^2|}$.

Remark 2.3. When G is abelian, we know that G/G^2 is an elementary 2–group. Remark 2.2 allows us to conclude that the set

$$X=\{p(G)\mid G \text{ is a finite abelian group}\} \tag{2.3}$$

coincides with the subset $Y=\{2^{-n}:n\geq 0\}$ of $[0,1]$. Note that this observation ends completely the abelian case for finite groups. For infinite groups we have analogously

$$Z=\{p(G)\mid G \text{ is an abelian group}\}=Y\cup\{0\}. \tag{2.4}$$

Then we know all the values of (1.2) for abelian groups.

Remark 2.3 agrees with [8, Proposition 2.1]. The two pathological cases $p(G)=0$ and $p(G)=1$ are described below and for finite groups they can be found in [8].

Remark 2.4. If G is finite, then $p(G)\geq\frac{1}{|G|}>0$. This can never happen and we deduce that $p(G)>0$. Now assume G is infinite. If G^2 is trivial, that is, no nontrivial element of G has a square root, then $p(G)=0$. Conversely, $p(G)=\mu(G^2)=0$ if and only if G^2 has zero μ–measure almost everywhere in G. This case may happen if and only if G^2 is a discrete subset of G (and in particular when G^2 is finite). We conclude that $p(G)>0$ if and only if G^2 is a nontrivial nondiscrete subset of G.

Remark 2.5. $p(G)=1$ if and only if each element of G has a square root. In case G is an abelian group this is the well-known notion of 2-divisible group (see [7, Appendix 1]). In fact this means that an arbitrary element $g\in G$ can be always written as $g=x^2$ for a suitable $x\in G$. Equivalently $G=G^2$.

A significant situation is the following. The structure of a compact abelian Lie group $G=\mathbb{T}^t\times E$ can be found in [7], where $\mathbb{T}$ denotes the solenoidal group, E is a finite group and $t\geq 0$. We know that $\mathbb{T}$ is a divisible abelian group (see [7, Corollary A1.43]). Then

$$\begin{aligned} p(G)&=\mu((\mathbb{T}^t\times E)^2)=\mu((\mathbb{T}^t)^2\times E^2)=\mu((\mathbb{T}^2)^t)\cdot\mu(E^2)\\ &=\mu(\mathbb{T}^2)^t\cdot\mu(E^2)=1^t\cdot\frac{|E^2|}{|E|}=\frac{|E^2|}{|E|}. \end{aligned}$$

If G is nonabelian, then the absence (resp. presence) of squares cannot be easily characterized, but we may always consider the largest closed abelian subgroup of G, whose existence is ensured by classical results in [7], and characterize here the absence (resp. presence) of squares as above.

The abelian case is summarized by the following result.

Theorem 2.6. *Let G be a nontrivial abelian group. Then:*

(i) $p(G) = 1$ *if and only if G is 2–divisible;*
(ii) $p(G) = 0$ *if and only if* $|G : G^2| = \infty$ *;*
(iii) $Z = Y \cup \{0\}$*, following the notation of Remark 2.3.*

Proof. (i). This follows from Remark 2.5.
(ii). This follows from Remarks 2.2 and 2.4.
(iii). This follows from Remark 2.3.

□

Theorem 2.6 extends [8, Theorem 2.4] to the infinite case and allows us to classify the abelian groups by means of (1.2).

Remark 2.7. A classical Wilcox's Theorem in [7] implies that a connected compact group is 2-divisible. Then $p(G) = 1$ for each connected compact group.

Since μ is finitely additive, (1.2) is multiplicative as a usual probability function. Therefore the following observation is straightforward.

Remark 2.8. Let A and B be two compact groups. Then $p(A \times B) = p(A)p(B)$.

Now we are going to do some considerations on the limit cases 0 and 1 with respect to (1.2). We distinguish an abelian case and a nonabelian case.

Corollary 2.9. *For any $\epsilon \in \mathbb{R}$ with $\epsilon > 0$, there exists an abelian group G such that $0 < p(G) < \epsilon$.*

Proof. Consider $n > 1$ such that $1/2^n < \epsilon$ and the compact abelian group $G = A \times B$, where A is a finite elementary abelian 2–group such that $p(A) = 1/2^n$ and B is a 2–divisible abelian group. By Theorem 2.6 (i), Remark 2.8 and [8, Corollary 2.5], $p(G) = p(A) \cdot p(B) = 1/2^n \cdot 1 < \epsilon$. □

Corollary 2.10. *For any $\epsilon \in \mathbb{R}$ with $\epsilon > 0$, there exists a nonabelian group G such that $1 - \epsilon < p(G) < 1$.*

Proof. Consider $n > 1$ such that $1/2^n < \epsilon$ and the nonabelian compact group $G = A \times B$, where $A = PSL(2, 2^n)$ and B is a 2–divisible abelian group. By Theorem 2.6 (i), Remark 2.8 and [8, Corollary 3.2], $p(G) = p(A) \cdot p(B) = \frac{(2^n-1)}{2^n} \cdot 1$. On the other hand, $1 - \epsilon < \frac{(2^n-1)}{2^n} < 1$, therefore $1 - \epsilon < p(G) < 1$. □

Corollaries 2.9 and 2.10 extend [8, Corollaries 2.5, 3.2]. In particular, we have just proved that 0 and 1 are accumulation points for the subset

$$T = \{p(G) \mid G \text{ is a compact group}\} \tag{2.5}$$

in the interval $[0, 1]$.

3. A result of density

This section is devoted to extend both Corollaries 2.9, 2.10 and [2, Theorem 1.1] to the context of the compact groups. Most of the following proof is just like the proof of [2, Theorem 1.1] and is adapted to convenience of the reader.

Theorem 3.1. *The set T in (2.5) is dense in* $[0,1]$.

Proof. By Corollaries 2.9, 2.10, there is no loss of generality in showing that, if $0 < x < 1$, then x is a limit point of T. There exists an integer m such that $1/2 < 2^m x < 1$. Note that $(0,1) = \bigcup_{m\geq 0} [1/2^{m+1}, 1/2^m)$. Let $y = 2^m x$. We can choose an integer $n_1 \geq 1$ such that

$$(2^{n_1}-1)/2^{n_1} \leq y \leq (2^{n_1+1}-1)/2^{n_1+1}, \tag{3.1}$$

noting that $[1/2,1) = \bigcup_{n\geq 1} [(2^n-1)/2^n, (2^{n+1}-1)/2^{n+1})$. Let $s_1 = (2^{n_1}-1)/2^{n_1}$ and $r_1 = (2^{n_1+1}-1)/2^{n_1+1}$. Again we can choose an integer $n_2 \geq 1$ such that

$$(2^{n_2}-1)/2^{n_2} \leq y/r_1 \leq (2^{n_2+1}-1)/2^{n_2+1}, \tag{3.2}$$

noting that $1/2 \leq y/r_1 < 1$. As before, let $s_2 = (2^{n_2}-1)/2^{n_2}$ and $r_2 = (2^{n_2+1}-1)/2^{n_2+1}$. Iterating this process, there exist positive integers $n_1, n_2, n_3, \ldots$ and two sequences $\{s_i\}$ and $\{r_i\}$ such that $s_i = (2^{n_i}-1)/2^{n_i}, r_i = (2^{n_i+1}-1)/2^{n_i+1}$ and $s_i \leq \frac{y}{r_1 r_2 \ldots r_{i-1}} < r_i$ for all $i \geq 1$. Of course, $0 < s_i < r_i < 1$ for all $i \geq 1$. We have $n_i \leq n_{i+1}$ for all $i \geq 1$, since

$$s_i \leq \frac{y}{r_1 r_2 \ldots r_{i-1}} < \frac{y}{r_1 r_2 \ldots r_{i-1} r_i} < r_{i+1}. \tag{3.3}$$

Thus $\{s_i\}$ is a monotonically increasing sequence, bounded by 1, and so convergent. Moreover, $\{s_i\}$ has infinitely many distinct terms; otherwise $\{s_i\}$, and hence $\{r_i\}$, would be eventually constant, and so, for some $j \geq 1$, we would have

$$\frac{y}{r_1 r_2 \ldots r_{j-1} r_j^{k-1}} < r_j \tag{3.4}$$

or $r_1 r_2 \ldots r_{j-1} r_j^k$ for $k \geq 1$. This is impossible, since $y > 0$ and $\lim_{k\to\infty} r_j^k = 0$. Therefore, $\{s_i\}$ converges to 1 (after omitting repeated terms), because it is a subsequence of $\{(2^n-1)/2^n\}$. This allows us to note that the sequence $\{a_i\}$ converges to 1, where $a_i = y/r_1 r_2 \ldots r_{i-1}$. Consequently, the sequence $\{b_i\}$ converges to y, where $b_i = r_1 r_2 \ldots r_{i-1}$. Thus we have

$$\lim_{k\to\infty} \frac{r_1 r_2 \ldots r_{i-1}}{2^m} = \frac{y}{2^m} = x. \tag{3.5}$$

For each $i \geq 1$ we consider the compact group $G^{(i)} = G_0 \times G_1 \times \ldots \times G_{i-1}$, where B is a 2–divisible abelian group, $\mathbb{Z}(2)$ denotes the cyclic group of order 2 (this terminology is more usual in compact groups, see [7]) and

$$G_0 = \underbrace{\mathbb{Z}(2) \times \ldots \times \mathbb{Z}(2)}_{m-times} \times B = \mathbb{Z}(2)^m \times B \tag{3.6}$$

and $G_k = PSL(2, 2^{n_k+1}) \times B$. Remark 2.8 and the calculations in Corollaries 2.9 and 2.10 imply

$$p(G^{(i)}) = p(G_0)p(G_1)\ldots p(G_{i-1}) = \frac{1}{2^m} r_1 r_2 \ldots r_{i-1}. \tag{3.7}$$

We have $\lim_{i\to\infty} p(G^{(i)}) = x$ and so the result follows. □

References

[1] J. Blum, Enumeration of the square permutations in S_n, *J. Comb. Theory Ser. A* **17** (1974), 156-161.
[2] A. K. Das, On group elements having square roots, *Bull. Iranian Math. Soc.* **31** (2005), 33–36.
[3] P. Erdös and P. Turan, On some problems of statistical group theory, *Acta Math. Acad. Sci. Hung.* **19** (1968), 413–435.
[4] A. Erfanian and F. Russo, Probability of mutually commuting n-tuples in some classes of compact groups, *Bull. Iran. Math. Soc.* **34** (2008), 27–37.
[5] A. Erfanian and F. Russo, Isoclinism in probability of commuting n-tuples, *Italian J. Pure Appl. Math.* **25** (2009), 27–36.
[6] W. H. Gustafson, What is the probability that two groups elements commute?, *Amer. Math. Monthly* **80** (1973), 1031–1304.
[7] K. H. Hofmann and S. A. Morris, *The structure of compact groups,* (de Gruyter, Berlin, 1998).
[8] M. S. Lucido and M. R. Pournaki, Elements with square roots in finite groups, *Algebra Colloq.* **12** (2005), 677–690.
[9] M. R. R. Moghaddam, A. R. Salemkar and K. Chiti, n–isoclinism classes and n–nilpotency degree of finite groups, *Algebra Colloq.* **12** (2005), 225–261.

Laboratorio di Dinamica Strutturale e Geotecnica (StreGa), Universitá degli Studi del Molise, via Duca degli Abruzzi, 86039, Termoli (CB), Italy
E-mail address: francescog.russo@yahoo.com