International Journal of Mathematics, Game Theory and Algebra ISSN 1060-9881
Volume 19, Number 1/2, pp. 7–14

DETECTING THE COMMUTING PROBABILITY OF THE DERIVED SUBGROUP

A. Erfanian[1,*] ***and F. Russo***[2,†]
[1]Department of Mathematics, Centre of Excellence
in Analysis on Algebraic Structures,
Ferdowsi University of Mashhad, Mashhad, Iran
[2]Department of Mathematics, University of Naples Federico II,
Naples, Italy

Abstract

There is a long standing line of research, which is devoted to investigate bounds for $|G'|$ when G is an infinite group. This line goes back to a classic result of I. Schur. The present paper deals with the structure of G' when G is a compact group, showing that $|G'|$ can be controlled by the notion of commuting probability.

2000 Mathematics Subject Classification. Primary: 20D60, 20P05; Secondary: 20D08.

Keywords. Commuting probability, compact group, p-elementary abelian groups of rank 2, derived subgroup.

1. Introduction

If G is a finite group, the probability that a randomly chosen pair of elements of G commutes is defined to be $\#com(G)/|G|^2$, where $\#com(G)$ is the number of pairs $(x,y) \in G \times G$ with $xy = yx$, G^2 is the product of two copies of G and $|G|^2$ is the order of G^2. Note that this ratio is denoted by $cp(G) = k(G)/|G|$ in [1, 3, 5, 10] where $k(G)$ is the number of the conjugacy classes of G. See also [2, 4, 7]. More precisely, if G is a finite group,

$$cp(G) = \frac{|\{(x_1,x_2) \in G^2 \; ; \; x_i x_j = x_j x_i \text{ for all } 1 \le i, j \le 2\}|}{|G|^2}.$$

If G is a non-abelian group, then $cp(G) \le 5/8$; furthermore this bound is achieved if and only if $G/Z(G)$ has order 4, where $Z(G)$ is the center of G. Such a result can be found in [5].

The ratio $cp(G)$ has been extended to a compact group G already in [5, Section 2], defining $cp(G) = (\mu \times \mu)(C)$, where $C = \{(x,y) \in G^2 \mid xy = yx\}$, $f : (x,y) \in G^2 \to [x,y] \in G$, $C = f^{-1}(1)$ and μ is the normalized Haar measure on G. Note that C is measurable, since it

*E-mail address: erfanian@math.um.ac.ir
†E-mail address: francesco.russo@dma.unina.it

is the anti-image of the closed set $\{1\}$ under the map f which is continuous (see [5, Section 2]). These information and the properties of the Haar measure on G guarantee that $cp(G)$ is well–defined (see also [6, Chapter 2]). Obviously, if G is finite, then it is a compact group with the discrete topology and so the Haar measure on G is the counting measure. Most of the results in [1, 3, 4, 5, 7, 10] can be seen in such a way. We list now our main results. Section 2 will allow us to prove them in Section 3.

Theorem A. *Let G be a non-abelian connected compact group, $Z_0(G)$ be the identity component of $Z(G)$ and $G/Z_0(G)$ be a p-group, where p is a prime. Then the following statements are equivalent:*

(i) *$G/Z_0(G)$ is a p-elementary abelian group of rank 2;*

(ii) *G' is a p-elementary abelian group of rank 2;*

(iii) $cp(G) = \frac{p^2+p-1}{p^3}$.

Theorem B. *Let G be a non-abelian compact group, $sol(G/Z(G))$ be the soluble radical of $G/Z(G)$, $F(G/Z(G))$ be the Fitting subgroup of $G/Z(G)$, d be the maximum number of elements in a conjugacy class of G, l be the derived length of $G/Z(G)$, p be a prime and n,m be positive integers.*

(i) *If $|G/Z(G)| = n$, then $d^{-\frac{1}{2}(1+log_2 d)} \leq |G'|^{-1} < cp(F(G/Z(G)))^{\frac{1}{2}}|G/Z(G) : F(G/Z(G))|^{-\frac{1}{2}} \leq |G/Z(G) : F(G/Z(G))|^{-\frac{1}{2}}$.*

(ii) *If $G/Z(G)$ is soluble of order n, then $d^{-\frac{1}{2}(1+log_2 d)} \leq |G'|^{-1} < log_2(|G/Z(G) : sol(G/Z(G))|)^{-\frac{1}{3}}$.*

(iii) *If $|G/Z(G)| = n$, then $d^{-\frac{1}{2}(1+log_2 d)} \leq |G'|^{-1} < |G/Z(G) : sol(G/Z(G))|^{-\frac{1}{2}}$.*

(iv) *If $G/Z(G)$ is finite soluble with $l \geq 4$, then $d^{-\frac{1}{2}(1+log_2 d)} \leq |G'|^{-1} < \frac{4l-7}{2^{l+1}}$.*

(v) *If $|G/Z(G)| = p^m$, then $p^{-\frac{1}{2}m(m-1)} \leq |G'|^{-1} < \frac{p^l+p^{l-1}-1}{p^{2l-1}}$.*

2. Preliminaries

In this section, G is assumed to be a non-abelian compact group (not necessarily finite even uncountable) with normalized Haar measure μ.

Lemma 2.1. *Let $C_G(x)$ be the centralizer of an element x in G. Then*

$$cp(G) = \int_G \mu(C_G(x))d\mu(x),$$

where $\mu(C_G(x)) = \int_G \chi_C(x,y)d\mu(y)$ and χ_C denotes the characteristic map of the set C.

Proof. See [2, Lemma 3.1]. $\diamondsuit$

Lemma 2.2. *Let H be a closed subgroup of G, n,r be positive integers and p be a prime.*

(i) *If $|G:H| \geq n$, then $\mu(H) \leq \frac{1}{n}$.*

(ii) *If $|G:H| \leq n$, then $\mu(H) \geq \frac{1}{n}$.*

(iii) *Assume that $G/Z(G)$ is a p-group of order p^r. An element x belongs to $Z(G)$ if and only if $\mu(C_G(x)) > \frac{1}{p}$.*

Proof. See [2, Lemmas 3.2, 3.4]. $\diamondsuit$

Lemma 2.3. *Let r be a positive integer. If $G/Z(G)$ is a p-elementary abelian group of rank r, then $cp(G) \leq \frac{p^r+p-1}{p^{r+1}}$, for every prime p. The equality holds when $r=2$.*

Proof. Assume that $G/Z(G)$ is a p-elementary abelian group of rank r . By Lemma 2.1 and Lemma 2.2, we have

$$\begin{aligned} cp(G) &= \int_G \mu(C_G(x))d\mu(x) = \int_{G-Z(G)} \mu(C_G(x))d\mu(x) + \mu(Z(G)) \\ &\leq \tfrac{1}{p}(\mu(G) - \mu(Z(G))) + \mu(Z(G)) = \tfrac{1}{p}(1 - \tfrac{1}{p^r}) + \tfrac{1}{p^r} = \tfrac{p^r+p-1}{p^{r+1}} \end{aligned}$$

If $r=2$, then G is the union of p^2 distinct cosets

$$G = Z(G) \cup x_1Z(G) \cup x_2Z(G) \cup \ldots \cup x_{p^2-1}Z(G)$$

and so $1 = \mu(G) = p^2\mu(Z(G))$. Moreover, if $a,b \in x_iZ(G)$, for $1 \leq i \leq p^2-1$, then $a = x_iz_1$ and $b = x_iz_2$ for some $z_1,z_2 \in Z(G)$ so that

$$ab = x_iz_1x_iz_2 = x_ix_iz_1z_2 = x_ix_iz_2z_1 = x_iz_2x_iz_1 = ba.$$

Thus, if $a \in x_iZ(G)$, then $C_G(a) = Z(G) \cup aZ(G) \cup a^2Z(G) \cup \ldots \cup a^{p-1}Z(G)$ and so

$$\begin{aligned} \mu(C_G(a)) &= \mu(Z(G)) + \mu(aZ(G)) + \mu(a^2Z(G)) + \ldots + \mu(a^{p-1}Z(G)) \\ &= p\mu(Z(G)) = p(\tfrac{1}{p^2}) = \tfrac{1}{p} \end{aligned}$$

Thus, we have

$$\begin{aligned} cp(G) &= \int_G \mu(C_G(x))d\mu(x) \\ &= \int_{Z(G)} \mu(C_G(x))d\mu(x) + \sum_{i=1}^{p^2-1} \int_{x_iZ(G)} \mu(C_G(x))d\mu(x) \\ &= \mu(Z(G)) + \tfrac{1}{p}\sum_{i=1}^{p^2-1} \mu(Z(G)) = (\tfrac{1}{p}(p^2-1)+1)\mu(Z(G)) \\ &= \tfrac{p^2+p-1}{p^3}. \ \diamondsuit \end{aligned}$$

Proposition 2.4. *Let N be a closed normal subgroup of G. Then*

$$cp(G) \leq cp(G/N).$$

In particular, if $N \cap G' = 1$, then the equality holds.

Proof. Let λ, μ and ν be the corresponding Haar measure of N, G and G/N respectively. Let $x \in G$, $y \in N$ and $xN \in G/N$. The integral properties of the Haar measure on G allow us to write

$$\int_G \mu(C_G(x))d\mu(x) = \int_{G/N}\left(\int_N \mu(C_G(xy))d\lambda(y)\right)d\nu(xN).$$

Since ν is a Haar measure on G/N, ν acts on G/N as μ on G modulo N so that $\mu(C_G(xy)N) = \nu(C_G(xy)N/N)$. But in general $C_G(xy)N/N \leq C_{G/N}(xN)$, so that $\nu(C_G(xy)N/N) \leq \nu(C_{G/N}(xN))$ being ν monotone.

Then, $\mu(C_G(xy)N) = \nu(C_G(xy)N/N) \leq \nu(C_{G/N}(xN))$ and, from Lemma 2.1, we have

$$\begin{aligned}
&cp(G) = (\mu \times \mu)(C)\\
&= \textstyle\int_G \mu(C_G(x))d\mu(x) = \int_{G/N}(\int_N \mu(C_G(xy))d\lambda(y))\,d\nu(xN)\\
&\leq \textstyle\int_{G/N}(\int_N \mu(C_G(xy)N)d\lambda(y))\,d\nu(xN)\\
&\leq \textstyle\int_{G/N}\left(\int_N \nu(C_{G/N}(xN))d\lambda(y)\right)d\nu(xN)\\
&= \textstyle\int_{G/N}\nu(C_{G/N}(xN))\,(\int_N d\lambda(y))\,d\nu(xN)\\
&= \textstyle\int_{G/N}\nu(C_{G/N}(xN))d\nu(xN) = cp(G/N).
\end{aligned}$$

In particular, if $N \cap G' = 1$, then $C_G(xy) = C_G(xy)N$ and so $\mu(C_G(xy)) = \mu(C_G(xy)N)$. Furthermore, $\mu(C_G(xy)N) = \nu((C_G(xy)N)/N) = \nu(C_{G/N}(xN))$. So, the equality holds. $\diamondsuit$

Recall from [6] that G_0 denotes the *identity component* of G. In particular, $Z_0(G)$ denotes the identity component of $Z(G)$.

Lemma 2.5. *If G is connected, then $\mu(G') = \mu(G/Z_0(G))$.*

Proof. From [6, Theorem 9.24 (ii)], $G = Z_0(G)G'$ and $Z_0(G) \cap G'$ is totally disconnected. We conclude that

$$\mu(G) = \mu(Z_0(G)G') = \mu(Z_0(G)) + \mu(G') - \mu(Z_0(G) \cap G')$$

Since $Z_0(G) \cap G'$ is totally disconnected, $\mu(Z_0(G) \cap G') = 0$, and so

$$\mu(G') = \mu(G) - \mu(Z_0(G)) = \mu(G/Z_0(G)).\ \diamondsuit$$

The proof of Lemma 2.5 uses [6, Theorem 9.24 (ii)] which is a fundamental result in the Theory of Compact Groups. Moreover it allows us to have a precise control of the measure of G' as the following remark shows.

Remark 2.6. From [6, Theorem 9.24 (ii)], if we have a non-abelian compact group G, then there exists a family $\{S_j : j \in J\}$ of simple connected compact Lie groups and a totally disconnected central subgroup D of $Z_0(G) \times \prod_{j \in J} S_j$ such that $G \cong \frac{Z_0(G) \times \prod_{j \in J} S_j}{D}$. Since D is totally disconnected, $\mu(D) = 0$, and so $\mu(G)$ is equal to

$$\mu\Big(\frac{Z_0(G) \times \prod_{j \in J} S_j}{D}\Big) = (\mu(Z_0(G)) + \mu(\prod_{j \in J} S_j)) - \mu(D) = \mu(Z_0(G)) + \mu(\prod_{j \in J} S_j).$$

By Lemma 2.5, $\mu(G') = \mu(G/Z_0(G)) = \mu(\prod_{j \in J} S_j)$. $\diamondsuit$

The following lemma adapts [4, Lemma 2 (vi)].

Lemma 2.7. *Let G be a non-abelian compact group with $|G : Z(G)| = n$, where n is a positive integer. Then $|G'|^{-1} < cp(G)$.*

Proof. A famous bound of Wiegold (see [8, p.102 (2)]) shows that, if $|G : Z(G)|$ is finite, then $|G'|$ is finite as well. Now, we can easily observe that the length of every conjugacy class is bounded above by the order of derived subgroup G' for every element $x \in G$. This means $|G : C_G(x)| \leq |G'|$ for all $x \in G$. By Lemma 2.2, $\mu(C_G(x)) \geq |G'|^{-1}$ for each element $x \in G$. Moreover, if $|G : Z(G)| = n$, then we may write G as the union of n distinct cosets

$$G = Z(G) \cup x_1 Z(G) \cup x_2 Z(G) \cup \ldots \cup x_{n-1} Z(G)$$

and so $\mu(Z(G)) = 1/n$. Thus we will have

$$\begin{aligned} &cp(G) = \textstyle\int_G \mu(C_G(x)) d\mu(x) = \int_{Z(G)} \mu(C_G(x)) d\mu(x) + \int_{x_1 Z(G)} \mu(C_G(x)) d\mu(x) + \\ &\cdots + \textstyle\int_{x_{n-1} Z(G)} \mu(C_G(x)) d\mu(x) = \mu(Z(G)) + \sum_{i=1}^{n-1} \int_{x_i Z(G)} \mu(C_G(x)) d\mu(x) \\ &\geq \tfrac{1}{n} + \textstyle\sum_{i=1}^{n-1} \int_{x_i Z(G)} |G'|^{-1} d\mu(x) > \tfrac{1}{n}|G'|^{-1} + \tfrac{n-1}{n}|G'|^{-1} = |G'|^{-1}. \quad \diamondsuit \end{aligned}$$

3. Proofs of Theorems A and B

This Section contains our main results with some instructive examples.

Proof of Theorem A. (i)$\Rightarrow$(ii). From [6, Theorem 9.24], $G = Z_0(G)G'$ so that G' is isomorphic as compact group to $G/Z_0(G)$. Now the property to be a p-elementary abelian group of rank 2 is invariant under isomorphisms of compact groups. Then the result follows.

(ii)$\Rightarrow$(iii). Again from [6, Theorem 9.24] we have that G' is isomorphic to $G/Z_0(G)$ and so $G/Z_0(G)$ is a p-elementary abelian group of rank 2. Since $Z_0(G) \leq Z(G)$ and the class of p-elementary abelian groups is closed with respect to forming subgroups, images and extensions of its members (see [8]), we conclude that $G/Z(G)$ is a p-elementary abelian group of rank 2. Now Lemma 2.3 gives the required bound.

(iii)$\Rightarrow$(i). Assume that $cp(G) = \frac{p^2+p-1}{p^3}$ and $G/Z_0(G)$ is not a p-elementary abelian group of rank 2. By assumption $G/Z_0(G)$ is a p-group. So, if $G/Z_0(G)$ has order 1 or p, then it is cyclic. Since $Z_0(G) \leq Z(G)$, also $G/Z(G)$ is cyclic. It follows that G is abelian and there is a contradiction. Thus $|G:Z_0(G)|\geq p^2$. If $|G:Z_0(G)|=p^2$, then $G/Z_0(G)$ is an abelian of order p^2 and it is either cyclic of order p^2 or a p-elementary abelian group of rank 2. In the first case we obtain again a contradiction and in the second case we finish. Now suppose that $|G:Z_0(G)|>p^2$. Using [6, Theorem 9.24 (ii)] and Lemma 2.5, we have

$$cp(G)=\int_G \mu(C_G(x))d\mu(x)=\int_{Z_0(G)G'}\mu(C_G(x))d\mu(x)$$

$$=\int_{Z_0(G)}\mu(C_G(x))d\mu(x)+\int_{G'}\mu(C_G(x))d\mu(x)-\int_{G'\cap Z_0(G)}\mu(C_G(x))d\mu(x)$$

$$=\int_{Z_0(G)}\mu(C_G(x))d\mu(x)+\int_{G'}\mu(C_G(x))d\mu(x)$$

$$=\int_{Z_0(G)}\mu(C_G(x))d\mu(x)+\int_{G'\setminus Z_0(G)}\mu(C_G(x))d\mu(x)$$

$$\leq \mu(Z_0(G))+(\mu(G')-\mu(Z_0(G)))=\mu(G')=\mu(G/Z_0(G)).$$

But $Z_0(G)$ is a closed normal subgroup of G with $|G:Z_0(G)|>p^2$, then Lemma 2.2 implies $\mu(G/Z_0(G))<\frac{1}{p^2}$. Now the relation $\frac{p^2+p-1}{p^3}<\frac{1}{p^2}$ gives a contradiction and the result follows. $\diamondsuit$

Proof of Theorem B. The finiteness of $G/Z(G)$ implies the finiteness of G' by a famous Schur's Lemma (see [8, Theorem 4.12]), so there are no problems to consider the maximum number of elements in a conjugacy class of G [8, Theorem 4.35].

Lemma 2.7, combined with [4, Theorem 4 (ii)] and Proposition 2.4, implies

$$|G'|^{-1}<cp(G)<cp(G/Z(G))\leq$$

$$cp(F(G/Z(G)))^{\frac{1}{2}}|G/Z(G):F(G/Z(G))|^{-\frac{1}{2}}\leq |G/Z(G):F(G/Z(G))|^{-\frac{1}{2}}.$$

On the other hand, the bound of Wiegold [8, Chapter 4, p.126-127] gives

$$(*) \qquad d^{-\frac{1}{2}(1+log_2 d)}\leq |G'|^{-1},$$

then (i) is proved.

Lemma 2.7, combined with [4, Theorem 8 (i)] and Proposition 2.4, gives

$$|G'|^{-1}<cp(G)<cp(G/Z(G))<log_2(|G/Z(G):sol(G/Z(G))|)^{-\frac{1}{3}}.$$

As before we use $(*)$ and (ii) follows.

Lemma 2.7, combined with [4, Theorem 9] and Proposition 2.4, gives

$$|G'|^{-1}<cp(G)<cp(G/Z(G))\leq |G/Z(G):sol(G/Z(G))|^{-\frac{1}{2}}.$$

As before we use $(*)$ and (iii) follows.

Lemma 2.7, combined with [4, Theorem 12 (i)] and Proposition 2.4, gives

$$|G'|^{-1}<cp(G)<cp(G/Z(G))\leq \frac{4l-7}{2^{l+1}}.$$

As before we use $(*)$ and (iv) follows.

Lemma 2.7, combined with [4, Theorem 12 (ii)] and Proposition 2.4, gives

$$|G'|^{-1} < cp(G) < cp(G/Z(G)) \leq \frac{p^l + p^{l-1} - 1}{p^{2l-1}}.$$

Now the bound [8, p.102] gives

$$(**) \qquad p^{-\frac{1}{2}m(m-1)} \leq |G'|^{-1},$$

then (v) follows. $\diamondsuit$

The conditions $(*)$ and $(**)$ in the proof of Theorem B are classical restrictions on $|G'|$ (see [9]) of an infinite group G. Recent developments can be found in literature: for instance, [9] improves $(*)$ using techniques of Combinatorial Group Theory (see [9, Theorems 1.1, 1.3, 1.4]). The same authors of [9] have continued to improve these bounds during the last twenty years.

Example 3.1. Let n be a positive integer and $G = E \times \mathbb{T}^n$, where $\mathbb{T}^n$ is the n-dimensional torus group and E is a finite non-abelian group. See [6, pp.11–17] and [6, Proposition 2.42] for details. Of course, G is a compact group and if we know $cp(E)$, then $cp(G) = cp(E)cp(\mathbb{T}^n) = cp(E)$ by an application of Lemma 2.1. This means that informations on $cp(G)$ can be deduced from those on $cp(E)$. Note that $cp(E)$ is well known by [1, 3, 4, 5, 7, 10], since E is a finite group. This construction gives a source of examples both for Theorem A and Theorem B. $\diamondsuit$

Acknowledgement

We thank the referee for some useful suggestions.

References

[1] P. Erdös and P. Turan, On some problems of statistical group theory, *Acta Math. Acad. Sci. Hung.* **19** (1968), 413–435.

[2] A. Erfanian and R. Kamyabi-Gol, On the mutually n-tuples in compact groups, *Int. J. Algebra* **(6)** Vol. 1 (2007), 251–262.

[3] P. X. Gallagher, The number of conjugacy classes in a finite group, *Math. Z.* **118** (1970), 175–179.

[4] R. M. Guralnick and G. R. Robinson, On the commuting probability in finite groups, *J. Algebra* **300** (2006), 509–528.

[5] W. H. Gustafson, What is the probability that two groups elements commute? , *Amer. Math. Monthly* **80** (1973), 1031–1034.

[6] K. H. Hofmann, and S. A. Morris, *The Structure of Compact Groups*, de Gruyter, Berlin, New York, 1998.

[7] M. S. Lucido and M. R. Pournaki, Elements with Square Roots in Finite Groups, *Algebra Colloq.* **12** (2005), 677–690.

[8] D. J. Robinson, *Finiteness conditions and generalized soluble groups*, vol. I and vol.II, Springer Verlag, Berlin, 1972.

[9] D. Segal and A. Shalev, On groups with bounded conjugacy classes, *Quart. J. Math. Oxford* **(2)**, 50 (1999), 505–516.

[10] G. J. Sherman, What is the probability an automorphism fixes a group element?, *Amer. Math. Monthly* **82** (1975), 261-264.