Bulletin of the Iranian Mathematical Society Vol. 34 No. 2 (2008), pp 27-37.

# PROBABILITY OF MUTUALLY COMMUTING N-TUPLES IN SOME CLASSES OF COMPACT GROUPS

## A. ERFANIAN\* AND F. RUSSO

## Communicated by Jamshid Moori

ABSTRACT. In finite groups the probability that two randomly chosen elements commute or randomly ordered n-tuples of elements mutually commute have recently attracted interest by many authors. There are some classical results estimating the bounds for this kind of probability so that the knowledge of the whole structure of the group can be more accurate.

The same problematic has been recently extended to certain classes of infinite compact groups in [2], obtaining restrictions on the group of the inner automorphisms. Here such restrictions are improved for a wider class of infinite compact groups.

## 1. Introduction

Following [1] and [5], if G is a finite group, the probability that two randomly chosen elements of G commute 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. For infinite groups this ratio is no longer meaningful, but for the class of compact groups it is possible to proceed in analogy with the finite case. In order to give an adapted formulation of the probability that two randomly chosen elements of an infinite compact group commute, a

MSC(2000): Primary: 20D15, 20P05; Secondary: 20E32

Keywords: Mutually commuting n-tuples, commutativity degree, compact groups, topological groups

Received: 17 May 2007, Accepted: 19 January 2008

<sup>\*</sup>Corresponding author (c) 2008 Iranian Mathematical Society.

<sup>27</sup> 

brief introduction on the strategy being used in the finite case seems to be appropriate.

If n is a positive integer and G is a compact group, the n-tuples  $(x_1, x_2, \ldots, x_n)$  of elements of G with the property that  $x_i x_j = x_j x_i$ , for all  $1 \leq i, j \leq n$ , are called *mutually commuting n-tuples*. Each finite group being trivially a compact group, it is clear that the notion of mutually commuting n-tuples generalizes the previous notion, given for finite groups, of two randomly chosen commuting elements. The probability that randomly chosen ordered n-tuples of the group elements are mutually commuting n-tuples is denoted by  $\Pr_n Com(G)$ . Clearly, if n = 2 and a group G is finite, then  $\Pr_2 Com(G) = \#com(G)/|G|^2$ .

More directly, if G is a finite group, then for every integer  $n \ge 2$ ,

$$\Pr_{n} \operatorname{Com}(G) = \frac{|\{(x_{1}, x_{2}, \dots, x_{n}) \in G^{n} ; x_{i}x_{j} = x_{j}x_{i} \text{ for all } 1 \le i, j \le n\}|}{|G|^{n}},$$

and if G is non-abelian, then  $\Pr_n \operatorname{Com}(G) \leq 5/8$ . Furthermore, this bound is achieved if and only if G/Z(G) is isomorphic to the non-cyclic group of order 4, where Z(G) denotes the center of the group G. This result has been known for some time [5].

Here, we adopt the standard formulation for the notion of measure space in probability, for the notion of locally compact topological group and for the notion of Haar measure. They can be found for instance in [3] and [6].

It is useful to recall that every locally compact topological group G admits a left Haar measure  $\mu$ , which is a positive Radon measure on a  $\sigma$ -algebra containing Borel sets with the property that  $\mu(xE) = \mu(E)$  for each element x of the measure space X (see [6, Sections 18.1 and 18.2]). The support of  $\mu$  is G and it is usually unbounded, but if G is compact, then  $\mu$  is bounded. For this reason we may assume without ambiguity that a compact group G has a unique probability measure space  $(G, \mathcal{M}, \mu)$  with normalized Haar measure  $\mu$  (see [6, Proposition 18.2.1]).

Now, we state the following definition, adapted to the compact case.

Let G be a compact group with the normalized Haar measure  $\mu$ . On the product measure space  $G \times G$ , it is possible to consider the product probability measure  $\mu \times \mu$ . If we have

$$C_2 = \{ (x, y) \in G \times G \mid xy = yx \},\$$

then  $C_2 = f^{-1}(1_G)$ , where  $f : G \times G \to G$  is defined via  $f(x, y) = x^{-1}y^{-1}xy$  and  $1_G$  denotes the neutral element of G. It is clear that f

is continuous then  $C_2$  is a compact and measurable subset of  $G \times G$ . Therefore, it is possible to define

$$\Pr_2 Com(G) = (\mu \times \mu)(C_2)$$

Similarly, with the above notations, we may define  $Pr_n Com(G)$  for all positive integers  $n \ge 2$ , as follows. Suppose that  $G^n$  is the product of *n*-copies of *G* and  $\mu^n = \mu \times \mu \times \ldots \times \mu$  for *n*-times. Then,

$$\Pr_n Com(G) = \mu^n(C_n),$$

where

$$C_n = \{(x_1, \dots, x_n) \in G^n \mid x_i x_j = x_j x_i \text{ for all } 1 \le i, j \le n\}.$$

Obviously, if G is finite, then G is a compact group with the discrete topology, and so the Haar measure of G is the counting measure. Therefore,

$$\Pr_n \operatorname{Com}(G) = \mu^n(C_n) = \frac{|C_n|}{|G|^n}$$

which is the same as definition of  $Pr_nCom(G)$  in the finite case.

Now, we are ready to give our main results.

**Theorem A.** Let G be a non-abelian compact group such that G/Z(G) is a p-elementary abelian group of rank 2, where p is a prime. Then,

$$\Pr_n Com(G) = \frac{p^n + p^{n-1} - 1}{p^{2n-1}} \,.$$

**Theorem B.** Let G be a non-abelian compact group and G/Z(G) be a pgroup, where p is prime. If  $\Pr_n Com(G) = \frac{p^n + p^{n-1} - 1}{p^{2n-1}}$  then G/Z(G) is p-elementary abelian of rank 2.

**Theorem C.** For every non-abelian compact group G and any prime p, if we have  $[G : Z(G)] = p^k$ , then

$$\Pr_n Com(G) \le \frac{(p-1)\sum_{i=0}^{n-2} p^{i(k-1)} + p^{(n-1)k-n+2}}{p^{(n-1)k+1}}$$

Erfanian and Russo

for all integers 
$$n \ge 2$$
 and  $k \ge 2$ .

Furthermore, this bound is achieved if G/Z(G) is a p-elementary abelian group of rank k and  $[G: C_G(x)] = p$  for all  $x \notin Z(G)$ .

Most of our notation is standard and can be found in [1,2,5,7].

## 2. Proving Theorem A

Here, G is assumed to be a non-abelian compact group (not necessarily finite, even uncountable) with normalized Haar measure  $\mu$ . First, we state the following simple lemmas.

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

$$Pr_2Com(G) = \int_G \mu(C_G(x))d\mu(x),$$

where  $\mu(C_G(x)) = \int_G \chi_{C_2}(x, y) d\mu(y)$  and  $\chi_{C_2}$  denotes the characteristic map of the set  $C_2$ .

**Proof.** Since  $\mu(C_G(x)) = \int_G \chi_{C_2}(x, y) d\mu(y)$ , we have by the Fubini-Tonelli's Theorem,

$$Pr_{2}Com(G) = (\mu \times \mu)(C_{2}) = \int_{G \times G} \chi_{C_{2}} d(\mu \times \mu)$$
$$= \int_{G} \int_{G} \chi_{C_{2}}(x, y) d\mu(x) d\mu(y)$$
$$= \int_{G} \mu(C_{G}(x)) d\mu(x).$$

**Lemma 2.2.** Let H be a closed subgroup of G and n be a positive integer. Then, we have:

 $\begin{array}{ll} \text{(i)} \ \ I\!\!f\,[G:H] \geq n, \ t\!hen \ \!\mu(H) \leq \frac{1}{n}. \\ \text{(ii)} \ \ I\!\!f\,[G:H] \leq n, \ t\!hen \ \!\mu(H) \geq \frac{1}{n} \ . \end{array}$ 

**Proof.** Assume that [G : H] = k, where k is a positive integer. Then, the proof follows from the equality,

$$1 = \mu(G) = \mu(\bigcup_{i=1}^{k} x_i H) = \sum_{i=1}^{k} \mu(x_i H) = k\mu(H).$$

**Lemma 2.3.** Let G/Z(G) be a p-group of order  $p^r$ , where p is prime and r is a positive integer. An element x does not belong to Z(G) if and only if  $\mu(C_G(x)) \leq \frac{1}{p}$ .

**Proof.** It is clear that if  $x \notin Z(G)$ , then  $[C_G(x) : Z(G)] \leq p^{r-1}$  and therefore,

$$p^r = [G: Z(G)] = [G: C_G(x)][C_G(x): Z(G)] \le p^{r-1}[G: C_G(x)],$$

which implies that  $\mu(C_G(x)) \leq \frac{1}{p}$ . Conversely, if  $\mu(C_G(x)) \leq \frac{1}{p}$  and  $x \in Z(G)$ , then  $\mu(C_G(x)) = \mu(Z(G)) = 1$ , which is a contradiction. Hence,  $x \notin Z(G)$  and the proof is complete.

**Theorem 2.4.** If G/Z(G) is a p-elementary abelian group of rank 2, then  $\Pr_2 Com(G) = \frac{p^2 + p - 1}{p^3}$ , for every prime p.

**Proof.** Assume that G/Z(G) is *p*-elementary abelian of rank 2. . Then, we may write G as the union of  $p^2$  distinct cosets,

$$G = Z(G) \cup x_1 Z(G) \cup x_2 Z(G) \cup \ldots \cup x_{p^2 - 1} Z(G),$$

and so  $1 = \mu(G) = p^2 \mu(Z(G))$ , since  $\mu$  is a left Haar-measure.

If  $a, b \in x_i Z(G)$ , for  $1 \leq i \leq p^2 - 1$ , then  $a = x_i z_1$  and  $b = x_i z_2$ , for some  $z_1, z_2 \in Z(G)$  so that

$$ab = x_i z_1 x_i z_2 = x_i x_i z_1 z_2 = x_i x_i z_2 z_1 = x_i z_2 x_i z_1 = ba.$$

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

$$\mu(C_G(a)) = \mu(Z(G)) + \mu(aZ(G)) + \mu(a^2Z(G)) + \dots + \mu(a^{p-1}Z(G))$$
$$= p\mu(Z(G)) = p(\frac{1}{p^2}) = \frac{1}{p}.$$

Thus, we have,

$$\begin{aligned} \Pr_{2} \operatorname{Com}(G) &= \int_{G} \mu(C_{G}(x)) d\mu(x) \\ &= \int_{Z(G)} \mu(C_{G}(x)) d\mu(x) + \sum_{i=1}^{p^{2}-1} \int_{x_{i}Z(G)} \mu(C_{G}(x)) d\mu(x) \\ &= \mu(Z(G)) + \sum_{i=1}^{p^{2}-1} \frac{1}{p} \mu(x_{i}Z(G)) \\ &= \mu(Z(G)) + \frac{1}{p} \sum_{i=1}^{p^{2}-1} \mu(Z(G)) \\ &= (\frac{1}{p}(p^{2}-1)+1) \mu(Z(G)) \\ &= \frac{p^{2}+p-1}{p} \mu(Z(G)) \\ &= \frac{p^{2}+p-1}{p^{3}}. \end{aligned}$$

Now, we give a proof for Theorem A.

**Proof of Theorem A.** We may proceed by induction on n. If n = 2, then the proof is clear by Theorem 2.4. Now, assume that the result holds for n - 1. Then, by the same strategy as in Theorem 2.4 and the induction hypothesis we have,

$$\begin{aligned} \Pr_{n} \operatorname{Com}(\mathbf{G}) &= \\ &= \int_{G^{n}} \chi_{C_{n}}(x_{1}, \dots, x_{n}) d\mu^{n}(x_{1}, \dots, x_{n}) \\ &= \int_{G^{n}} \chi_{C_{n-1}}(x_{2}, \dots, x_{n}) \chi_{C_{2}}(x_{1}, x_{2}) \dots \chi_{C_{2}}(x_{1}, x_{n}) d\mu^{n}(x_{1}, \dots, x_{n}) \\ &= \int_{G} \left[ \int_{G^{n-1}} \chi_{C_{n-1}}(x_{2}, \dots, x_{n}) \chi_{C_{2}}(x_{1}, x_{2}) \\ & \dots \chi_{C_{2}}(x_{1}, x_{n}) d\mu^{n-1}(x_{2}, \dots, x_{n}) \right] d\mu(x_{1}) \\ &= \int_{Z(G)} \left[ \int_{G^{n-1}} \chi_{C_{n-1}}(x_{2}, \dots, x_{n}) \chi_{C_{2}}(x_{1}, x_{2}) \\ & \dots \chi_{C_{2}}(x_{1}, x_{n}) d\mu^{n-1}(x_{2}, \dots, x_{n}) d\mu(x_{1}) \right] \end{aligned}$$

32

$$\begin{split} &+ \int_{G-Z(G)} \left[ \int_{G^{n-1}} \chi_{C_{n-1}}(x_2, \dots, x_n) \chi_{C_2}(x_1, x_2) \\ &\dots \chi_{C_2}(x_1, x_n) d\mu^{n-1}(x_2, \dots, x_n) d\mu(x_1) \\ &= \int_{Z(G)} \Pr_{n-1} \operatorname{Com}(G) d\mu(x_1) \\ &+ \int_{G-Z(G)} \left[ \int_{C_G(x_1)^{n-1}} \chi_{C_{n-1}}(x_2, \dots, x_n) d\mu^{n-1}(x_2, \dots, x_n) \right] d\mu(x_1) \\ &= \mu(Z(G)) \Pr_{n-1} \operatorname{Com}(G) \\ &+ \int_{G-Z(G)} \left[ \int_{C_G(x_1)^{n-1}} \chi_{C_{n-1}}(x_2, \dots, x_n) d\mu^{n-1}(x_2, \dots, x_n) \right] d\mu(x_1) \\ &= \mu(Z(G)) \Pr_{n-1} \operatorname{Com}(G) + \mu(G - Z(G)) \mu(C_G(x_1))^{n-1} \\ &= \frac{1}{p^2} \left( \frac{p^{n-1} + p^{n-2} - 1}{p^{2n-3}} \right) + (1 - \frac{1}{p^2}) (\frac{1}{p})^{n-1} \\ &= (\frac{p^{n-1} + p^{n-2} - 1}{p^{2n-1}}) + (\frac{p^2 - 1}{p^{n+1}}) \\ &= \frac{p^n + p^{n-1} - 1}{p^{2n-1}}, \end{split}$$

and the proof is complete.

## 3. Proving Theorem B

**Proof of Theorem B.** Let  $\Pr_n \operatorname{Com}(G) = \frac{p^n + p^{n-1} - 1}{p^{2n-1}}$  and G/Z(G) be not *p*-elementary abelian of rank 2. If  $[G : Z(G)] \in \{1, p\}$ , then G/Z(G) is cyclic and so *G* is abelian, which is a contradiction. Thus,  $[G : Z(G)] > p^2$  and therefore,  $\mu(Z(G)) < \frac{1}{p^2}$ . Moreover, if  $x \notin Z(G)$ 

then  $\mu(C_G(x)) < \frac{1}{p}$ , by Lemma 2.3. A similar argument as given in the proof of Theorem A implies that

$$\begin{aligned} \Pr_{n} \operatorname{Com}(G) &= \mu(Z(G)) \operatorname{Pr}_{n-1} \operatorname{Com}(G) + (1 - \mu(Z(G))[\mu(C(x_{1}))]^{n-1} \\ &\leq \mu(Z(G)) \left(\frac{p^{n-1} + p^{n-2} - 1}{p^{2n-3}}\right) + (1 - \mu(Z(G)))(\frac{1}{p})^{n-1} \\ &< \frac{1}{p^{2}} \left(\frac{p^{n-1} + p^{n-2} - 1}{p^{2n-3}}\right) + (1 - \frac{1}{p^{2}})(\frac{1}{p})^{n-1} \\ &= (\frac{p^{n-1} + p^{n-2} - 1}{p^{2n-1}}) + (\frac{p^{2} - 1}{p^{n+1}}) \\ &= \frac{p^{n} + p^{n-1} - 1}{p^{2n-1}}, \end{aligned}$$

which is a contradiction and this completes the proof.

If p = 2,  $n \ge 2$  or p = 2, n = 2, then Theorems A and B imply the following two corollaries which are given in [2] and [5], respectively.

**Corollary 3.1.** Let G be a non-abelian compact (not necessarily finite, even uncountable) group. Then, G/Z(G) is 2-elementary abelian of rank 2 if and only if  $Pr_nCom(G) = \frac{3(2^{n-1})-1}{2^{2n-1}}$  for all  $n \ge 2$ .

**Corollary 3.2.** Let G be a non-abelian compact group. Then, G/Z(G) is 2-elementary abelian of rank 2 if and only if  $Pr_2Com(G) = \frac{5}{8}$ .

## 4. Proving Theorem C

To prove Theorem C, we have to state the following lemma. We should note that as the previous sections, G is again assumed to be a non-abelian compact group with normalized Haar measure  $\mu$ .

**Lemma 4.1.** If  $[G: Z(G)] = p^k$ , where p is prime, then,

$$\Pr_2 Com(G) \le \frac{p^k + p - 1}{p^{k+1}} \text{ for all integers } k \ge 2.$$

**Proof.** Since  $[G : Z(G)] = p^k$ , one can easily see that  $\mu(Z(G)) = \frac{1}{p^k}$ and  $\mu(C_G(a)) \leq \frac{1}{p}$ , for all  $a \notin Z(G)$  using Lemma 2.3. Now, by Lemma 2.1, we have,

$$Pr_{2}Com(G) = \int_{Z(G)} \mu(C_{G}(x))d\mu(x) + \sum_{i=1}^{p^{k}-1} \int_{x_{i}Z(G)} \mu(C_{G}(x))d\mu(x)$$
  

$$\leq \mu(Z(G)) + \sum_{i=1}^{p^{k}-1} \frac{1}{p}\mu(x_{i}Z(G))$$
  

$$= \frac{1}{p^{k}} + (p^{k}-1)\frac{1}{p^{k+1}}$$
  

$$= \frac{p^{k}+p-1}{p^{k+1}}.$$

Using Lemma 4.1, we can now prove Theorem C.

**Proof of Theorem C.** Suppose that  $k \ge 2$ . We proceed by induction on n. If n = 2, then the proof is clear by Lemma 4.1. Now, assume that the result holds for n - 1. Then, by the induction hypothesis and similar arguments as given in the proof of Theorem A, we have,

$$\begin{aligned} &\Pr_{n} \operatorname{Com}(G) = \mu(Z(G)) \operatorname{Pr}_{n-1} \operatorname{Com}(G) + (1 - \mu(Z(G))\mu(C(x_{1}))^{n-1} \\ &\leq \frac{1}{p^{k}} \left( \frac{(p-1)\sum_{i=0}^{n-3} p^{i(k-1)} + p^{(n-2)k-n+3}}{p^{(n-2)k+1}} \right) + \frac{p^{k}-1}{p^{n+k-1}} \\ &= \frac{(p-1)\sum_{i=0}^{n-3} p^{i(k-1)} + p^{(n-2)k-n+3} + p^{(n-1)k-n+2} - p^{(n-2)k-n+2}}{p^{(n-1)k+1}} \\ &= \frac{(p-1)\sum_{i=0}^{n-3} p^{i(k-1)} + p^{(n-2)k-n+2}(p-1) + p^{(n-1)k-n+2}}{p^{(n-1)k+1}} \\ &= \frac{(p-1)\sum_{i=0}^{n-2} p^{i(k-1)} + p^{(n-1)k-n+2}}{p^{(n-1)k+1}}. \end{aligned}$$

The second part of Theorem C follows from the fact that  $\mu(C_G(a)) = \frac{1}{p}$ , for all  $a \notin Z(G)$ . Hence, we should have equality in all of the above relations and the proof is complete.

### 5. Examples

Here, we give some examples of finite and infinite groups satisfying our theorems.

(i). Assume,

$$G = \langle a, b \mid a^9 = b^3 = 1, bab^{-1} = a^4 \rangle.$$

Then, one can check that |G| = 27 and G/Z(G) is 3-elementary abelian of rank 2. By direct computations using the group theory package GAP and the formula given in Theorem A, we found:

$$Pr_{2}Com(G) = \frac{11}{27}, Pr_{3}Com(G) = \frac{35}{243},$$
$$Pr_{4}Com(G) = \frac{107}{2187}, Pr_{5}Com(G) = \frac{323}{19683}$$

These would confirm Theorems A and B.

(ii). Suppose,

 $G = \langle a, b, c \mid a^9 = b^3 = c^3 = 1, b^{-1}ab = a^4, c^{-1}ac = ab, c^{-1}bc = b \rangle$ . Then, we have that |G| = 81, |Z(G)| = 3 and G/Z(G) is 3-elementary abelian of rank 3. Again, using GAP and the upper bound given in Theorem C, we can check that

$$\Pr_{2}\operatorname{Com}(G) = \frac{17}{81} \le \frac{29}{81}, \quad \Pr_{3}\operatorname{Com}(G) = \frac{107}{2187} \le \frac{263}{2187},$$
$$\Pr_{4}\operatorname{Com}(G) = \frac{809}{59049} \le \frac{2369}{59049}.$$

So, this confirms the upper bound in Theorem C.

For the second part of Theorem C, we may state the following example.

(iii). Assume that G is any extra special p-group of order at least  $p^5$ . Recall that a p-group G is called extra-special if  $G' = Z(G) = \Phi(G)$  is cyclic of order p, where G' denotes the derived subgroup and  $\Phi(G)$ 

denotes the Frattini subgroup of G. The order of G will be  $p^{2k+1}$  for an integer  $k \geq 2$ . Obviously, G/Z(G) is p-elementary abelian of rank 2k. If  $x \notin Z(G)$ , then we can define a homomorphism from G to G' = Z(G) via  $y \longrightarrow [x, y]$ . The kernel of this homomorphism is  $C_G(x)$ . Since the image of this homomorphism has order p, we will have  $[G : C_G(x)] = p$ . Thus, by Theorem C, we have

$$\Pr_n \operatorname{Com}(G) = \frac{(p-1)\sum_{i=0}^{n-2} p^{i(2k-1)} + p^{2(n-1)k-n+2}}{p^{2(n-1)k+1}},$$

for all integers  $n \ge 2$  and  $k \ge 2$ .

(iv). If H is the direct product of G as the above examples and the group of unit circle, then we have an infinite non-abelian compact group with H/Z(H) isomorphic to G/Z(G). Thus, we may give three more examples on infinite case to confirm the main theorems.

#### References

- P. Erdos 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. of Algebra 1 (6) (2007) 251-262.
- [3] M. D. Fried and M. Jarden, Field Arithmetic, Revised Edition, *Ergebnisse*, 11, Springer Verlag, New York, 2005.
- [4] P. X. Gallagher, The number of conjugacy classes in a finite group, Math. Z. 118 (1970) 175-179.
- [5] W. H. Gustafson, What is the probability that two groups elements commute?, Amer. Math. Monthly 80 (1973) 1031-1304.
- [6] E. Hewitt and K. A. Ross, Abstract Harmonic Analysis, Springer Verlag, New York, 1963.
- [7] G. J. Sherman, What is the probability an automorphism fixes a group element?, Amer. Math. Monthly 82 (1975) 261-264.

#### A. Erfanian,

Department of Mathematics and Center of Excellence in Analysis on Algebraic Structures, Ferdowsi University of Mashhad,

Mashhad, Iran.

Email: erfanian@math.um.ac.ir

**F. Russo,** Department of Mathematics, University of Naples Federico II, Naples, Italy.

Email: francesco.russo@dma.unina.it