A SURVEY ON SOME RECENT INVESTIGATIONS
OF PROBABILITY IN GROUP THEORY

AHMAD M. A. ALGHAMDI, DANIELE ETTORE OTERA, AND FRANCESCO G. RUSSO

Abstract. We describe some recent contributions on the probability of commuting pairs, introduced by P. Erdős, W. Gustafson and P. Turán around 1968 and 1973. Both combinatorial methods and character theory have significant application in this context and we illustrate some standard techniques and strategies, once generalizations of the probability of commuting pairs want to be studied. The importance of the subject is emphasized in some remarks and open questions, which reformulate some classical conjectures in group theory via a probabilistic approach.

1. Generalizations of the commutativity degree

If the commutator \([x, y] = x^{-1}y^{-1}xy\) of two elements \(x\) and \(y\) of a finite group \(G\) is trivial, then \(x\) and \(y\) are permutable and, roughly speaking, we can proceed to a detailed description of \(G\). In fact, it is well-known that there are satisfying results of classification for finite abelian groups. The question can be seen from a wider point of view: we can ask how an algebraic structure, not necessarily a group, is close to have all elements which are permutable, involving algebras, graphs and so on.

Originally, the idea goes back to the works [17, 24, 26, 41], where it is investigated in various ways, and with different techniques, the influence of the number of the commuting pairs of elements on the structure of a finite group. The case of an infinite group was initiated in [26], involving compact groups and suitable measures of probability, and already in this work W. Gustafson noted the role of the differential geometry and of the abstract harmonic analysis in order to do a significant parallel with the finite case. In a certain sense [17, 24, 26, 41] are milestones for an entire line of research, largely exploited in [6, 11, 12, 13, 14, 16, 18, 20, 23, 25, 30, 32, 43] in the finite case and [19, 21, 22, 27, 35, 36] in the infinite case. The papers [31, 44] are just mentioned in order to show that it is possible to variate the condition on \([x, y]\) involving arbitrary words, which could not be the commutator word \([x, y]\):

Still we can draw conclusions on the structure of the group from restrictions of probabilistic nature.

The commutativity degree of a finite group \(G\) is defined as the ratio

\[
d(G) = \frac{|\{(x, y) \in G^2 \mid [x, y] = 1\}|}{|G|^2}
\]

and in [18] the \(n\)-th nilpotency degree

\[
d^{(n)}(G) = \frac{|\{(x_1, \ldots, x_{n+1}) \in G^{n+1} \mid [x_1, \ldots, x_n, x_{n+1}] = 1\}|}{|G|^{n+1}}
\]

is clearly a generalization of \(d(G)\), when \(n = 1\). Similarly, the relative \(n\)-th nilpotency degree

\[
d^{(n)}(H, G) = \frac{|\{(x_1, \ldots, x_n, x_{n+1}) \in H^n \times G \mid [x_1, \ldots, x_n, x_{n+1}] = 1\}|}{|H^n||G|}
\]

where \(H\) is a subgroup of \(G\), is a generalization of \(d(G)\), when \(n = 1\) and \(H = G\).

More recently, the following concepts were introduced, unifying most of the previous notions. Given two subgroups \(H\) and \(K\) of \(G\) and two integers \(n, m \geq 1\), in [2] it was defined

\[
p^{(n, m)}(H, K) = \frac{|\{(x_1, \ldots, x_n, y_1, \ldots, y_m) \in H^n \times K^m \mid [x_1, \ldots, x_n, y_1, \ldots, y_m] = g\}|}{|H^n||K|^m}
\]

as the probability that a randomly chosen commutator of weight \(n + m\) of \(H \times K\) is equal to a given element of \(G\). The case \(n = m = 1\) can be found in [11] and is called generalized commutativity degree of \(G\). For \(n = m = 1\) and
Corollary 1.2 (See [2], Corollary 3).

In particular, we have $p_g^{(1,1)}(H, G) = d^{(n)}(H, G)$ and

$$p_g^{(1,1)}(H, G) = \frac{|\{(x, y) \in H \times G \mid [x, y] = g\}|}{|H||G|} = \frac{1}{|H||G|} \sum_{\chi \in \text{Irr}(G)} \frac{|H|\langle \chi_H, \chi_H \rangle}{\chi(1)} \chi(g),$$

where $\chi_H$ denotes the restriction of $\chi$ to $H$ and $\langle \ , \ \rangle$ the usual inner product of characters.

In order to show some classical results, related to the above concepts, we can see that the idea is to begin from bounds on the probability and then to get to restrictions on the group. The following theorem shows this fact, when we deal with (1.4).

**Theorem 1.1** (See [2], Theorem 3.3). Let $G$ be a finite group, $H, K$ subgroups of $G$ and $p$ be the smallest prime divisor of $|G|$. Then

(i) $p_g^{(n,m)}(H, K) \leq \frac{2^p + p - 2}{p^{m+n}}$;

(ii) $p_g^{(n,m)}(H, K) \geq \frac{(1-p)Y_{n+m} + pH^n}{|H|^n|K|^m} - \frac{(|K|+p)|C_H(K)^n|}{|H|^n|K|^m}$;

where $Y_{H^n} = \{|x_1, \ldots, x_n\} \in H^n \mid C_K([x_1, \ldots, x_n]) = 1\}$.

As consequence we have the following restriction on the index of the centralizers.

**Corollary 1.2** (See [2], Corollary 3.4). In Theorem 1.1, if $p_g^{(n,m)}(H, K) = \frac{2^p + p - 2}{p^{m+n}}$ and $p \neq 2$, then

$$\frac{p \cdot p^n}{(p - 2)^n} \geq |H : C_H(K)|.$$

Another interesting application can be found in [32], where it is defined the exterior degree

$$d^\wedge(G) = \frac{|\{(x, y) \in G^2 \mid x \wedge y = 1\}|}{|G|^2}$$

of a finite group $G$, where $\wedge$ denotes the exterior product, related to the nonabelian tensor square of a finite group, introduced in [4, 5, 15] and largely studied in topology and K-theory. Still we have a modification of the notion of $d(G)$ and the knowledge of upper and lower bounds allows us to give restrictions of structural nature on $G$.

2. A REFORMULATION FOR SUBGROUPS LATTICES

In the present section we want to illustrate some variation on the theme of the commutativity degree, recently investigated in [33, 46]. Given two subgroups $H$ and $K$ of a finite group $G$, the product $HK = \{hk \mid h \in H, k \in K\}$ is not always a subgroup of $G$. $H$ and $K$ permute if $HK = KH$, or equivalently, if $HK$ is a subgroup of $G$. $H$ is said to be permutable (or quasinormal) in $G$, if it permutes with every subgroup of $G$. It is possible to strengthen this notion in the sense of Kegel (see [33]), saying that $H$ is $S$-permutable (or $S$-quasinormal) with $K$, if $H$ permutes with all Sylow subgroups of $K$ (for all primes in the set of the prime divisors of the order of $K$). If $H$ permutes with all Sylow subgroups of $G$, we say that $H$ is $S$-permutable in $G$.

We recall that the set of all subgroups of $G$ is called the subgroup lattice of $G$ and is denoted by $L(G)$. It is a complete bounded lattice with respect to the set inclusion, having initial element the trivial subgroup $\{1\}$ and final element $G$ itself (see [45]). Its binary operations $\lor, \land$ are defined in the usual way as $X \lor Y = X \cap Y$, $X \land Y = \langle X \cup Y \rangle$, for all $X, Y \in L(G)$. Furthermore, $L(G)$ is modular, if all the subgroups of $G$ satisfy the well known modular law.
G is said to be modular, if $\mathcal{L}(G)$ is modular (see [45, Section 2.1]). This notion is related to the following concept. A group G is said to be quasihamiltonian, if all of its subgroups are permutable. By a result of Iwasawa [45, Theorem 2.4.14], quasihamiltonian groups are characterized in terms of generators and relations, but, at the same time, these groups are characterized to be nilpotent and modular (see [45, Exercise 3, p.87]). Immediately we note that restrictions on $\mathcal{L}(G)$ influence the structure of G.

If $\mathcal{S}(G)$ is a nonempty sublattice of $\mathcal{L}(G)$, the symbol $\mathcal{S}^+(G)$ denotes the set of all subgroups $H$ of G which are permutable with all $S \in \mathcal{S}(G)$. It is easy to check that $\mathcal{S}^+(G)$ is a sublattice of $\mathcal{L}(G)$. If $\mathcal{S}(G) = \text{Syl}(G)$ is the set of all Sylow subgroups of G (for all primes), then Syl$^+(G)$ is the set of all S–permutable subgroups of G. If $\mathcal{S}(G) = \mathcal{L}(G)$, then $\mathcal{L}^+(G)$ is the set of all permutable subgroups of G. It turns out that a group G is quasihamiltonian if and only if $\mathcal{L}(G) = \mathcal{L}^+(G)$. By analogy, a group G in which all subgroups are S–permutable is characterized by the condition $\mathcal{L}(G) = \text{Syl}^+(G)$ and this happens exactly when G is a nilpotent group. More generally, it is possible to deduce structural information on G by looking at the condition $\mathcal{S}^+(G) = \mathcal{L}(G)$ for a given choice of $\mathcal{S}(G)$ and not necessarily for $\mathcal{S}(G) = \text{Syl}(G)$.

In [33] it was introduced the following notion, generalizing the subgroup commutativity degree in [46] and similar investigations in [42].

**Definition 2.1** (See [33], Definition 2.1). For a group G, 
\[
spd(G) = \frac{|\{(X,Y) \in \mathcal{L}(G)^2 \mid X \text{ is S–permutable with } Y\}|}{|\mathcal{L}(G)|^2},
\]
is the subgroup S–commutativity degree of G.

Immediately we are able to characterize a large class of groups having $spd(G) = 1$.

**Proposition 2.2** (See [33], Proposition 2.5). For a group G we have $spd(G) = 1$ if and only if G is nilpotent.

There are open questions on the possibility to characterize other classes of groups as in Proposition 2.2 for values of $spd(G) \neq 1$. To sake of completeness, we list some bounds on $spd(G)$, which may be useful in this prospective.

**Corollary 2.3** (See [33], Corollary 2.14). Let G be a group and N be a normal subgroup of G such that $G/N$ and N are nilpotent. Then
\[
spd(G) \geq \left(\frac{|\mathcal{L}(N)| + |\mathcal{L}(G/N)| - 1}{|\mathcal{L}(G)|}\right)^2.
\]

**Corollary 2.4** (See [33], Corollary 2.15). Let G be a group and N be a normal subgroup of G of prime index. Then
\[
spd(G) \geq \frac{1}{|\mathcal{L}(G)|^2} (spd(N)|\mathcal{L}(N)|^2 + 2|\mathcal{L}(N)| + 1).
\]

We end this section, pointing out that for an infinite group it is open the problem to study a corresponding version of the subgroup commutativity degree and a corresponding version of the subgroup S–commutativity degree. The main problem is to find suitable measures on $\mathcal{L}(G)$, where G needs to be a compact group inducing a topology on $\mathcal{L}(G)$. The easy consideration of products of countably many finite groups gives us some evidences for which a general treatment should be possible.

3. A REFORMULATION OF DADE’S CONJECTURE

In the present section we end with a connection among the probability in group theory and variation of the well known Dade’s Conjecture (see [1]). We recall from [3, 28, 37, 38, 40, 39] the following notions.

**Definition 3.1.** Let G be a finite group and p be a prime number. The set of all p-subgroups of G is denoted by $\mathcal{P}(G)$. A totally ordered subset of $\mathcal{P}(G)$ is called a chain in $\mathcal{P}(G)$. We write a chain $\sigma$ in $\mathcal{P}(G)$ in the form
\[
\sigma : Q_0 < Q_1 < Q_2 < \ldots < Q_k,
\]
where $Q_i$ is a p–subgroup of G, for $0 \leq i \leq k$ and $Q_0 = \{1\}$. The length, or dimension $\dim(\sigma)$, of $\sigma$ is the integer k. Let $\mathcal{S}_p(G)$ denotes the set of all chains in $\mathcal{P}(G)$. If $g \in G$ and $\sigma \in \mathcal{S}_p(G)$ then G acts by conjugation on $\mathcal{S}_p(G)$ as follows:
\[
\sigma^g := g^{-1}\sigma g : Q_0^g < Q_1^g < Q_2^g < \ldots < Q_k^g.
\]

The subgroup
\[
G_{\sigma} := N_G(\sigma) := \bigcap_{i=1}^{k} N_G(Q_i) \leq N_G(Q_i)
\]
is the normalizer of $\sigma$ in $G$. With the symbol $\mathcal{A}_p(G)$ we denote the subset of $\mathcal{S}_p(G)$ consisting of all chains consisting of elementary abelian $p$-subgroups of $G$.

Now we should recall some rudiments of representation theory from [29]. A representation of degree $n$ over a field $F$ is a homomorphism of groups $\rho : G \rightarrow \text{GL}(n, F)$. It turns out that $\rho$ induces naturally an $n \times n$ matrix $M_\rho$ with coefficients in $F$. A representation is reducible, if $M_\rho$ can be reduced in blocks, where we can distinguish the corresponding matrices of the blocks as induced by representations of degree smaller than $n$. If $F = \mathbb{C}$, Frobenius proved in 1896 that $G$ has only finitely many equivalence classes of irreducible representations over $F$ and their number coincides with the number $k(G)$ of the conjugacy classes in $G$. If $\rho_i : G \rightarrow \text{GL}(d_i, \mathbb{C})$ denote the irreducible representations of $G$ of degree $d_i$, where $i = 1, 2, \ldots, k(G)$, then each $d_i$ divides $|G|$ and we have $|G| = d_1^2 + d_2^2 + \ldots + d_k^2(G)$. Now it is interesting to see which powers of $p$ divides $d_i$. If $p^{\delta_i}$ denotes the highest power of $p$ dividing $|G|/d_i$, we say that $\delta_i$ is the $p$-defect of $\rho_i$. If $P$ is a $p$-Sylow subgroup of $G$ of order $p^a$, then $\delta_i \in \{0, 1, \ldots, a\}$ for all $i = 1, 2, \ldots, k(G)$. Therefore we can omit the index $i$ and define, for $\delta \in \{0, 1, \ldots, a\}$, $k_\delta(G)$ as the number of irreducible representations of $p$-defect $\delta$ of $G$.

E. Dade came up in the last 20 years with series of conjectures [7, 8, 9, 10] related to the structure of $G$. The simplest of these conjectures is the following.

**Conjecture 3.2.**

$$k_\delta(G) = \sum_{\sigma} (-1)^{\dim(\sigma)} k_\delta(G_\sigma)$$

for $\delta > 0$, where $\sigma$ ranges over a set of representatives for the conjugacy classes of non-empty chains in $\mathcal{A}_p(G)$.

Then we can define the following probability:

$$\text{procomp}^{(p)}(G) = \frac{|\{(g, \sigma) \in G \times \mathcal{S}_p(G) \mid g^{-1} \sigma g = \sigma\}|}{|G||\mathcal{S}_p(G)|}.$$

In a more useful form, we have

$$\text{procomp}^{(p)}(G) = \frac{1}{|G||\mathcal{S}_p(G)|} \sum_{\sigma \in \mathcal{S}_p(G)/G} |G_\sigma|,$$

where $\mathcal{S}_p(G)/G$ denotes the set of representatives which we obtain from $\mathcal{S}_p(G)$ under the natural action of $G$. For instance, if $G = S_3$ is the symmetric group on 3 letters and $p = 2$, then $\text{procomp}^{(2)}(S_3) = \frac{3}{7}$. If $p = 3$, then $\text{procomp}^{(3)}(S_3) = 1$.

For $H$ a subgroup of $G$, we can view $\text{procomp}^{(p)}(H)$ as a function from the subgroups of $G$ to the interval $[0, 1]$. So, we follow G. R. Robinson approach [28, 38], to consider an alternating sum over the representatives of the action of $G$ on $\mathcal{S}_p(G)$. A treatment with probabilistic techniques of $\text{procomp}^{(p)}(G)$ is still open and its importance is related to the following remark.

**Remark 3.3.** The solution of Dade’s conjecture can be seen from the point of view of (3.1). In fact, a solution of

$$\sum_{\emptyset \neq \sigma \in \mathcal{S}_p(G)/G} (-1)^{\dim(\sigma)} \text{procomp}^{(p)}(G_\sigma) = \text{procomp}^{(p)}(G),$$

where $\sigma$ ranges over a set of representatives for the conjugacy classes of non-empty chains in $\mathcal{S}_p(G)$, would be a significant progress in order to attack Dade’s conjecture. Numerical evidences show that several groups satisfying Conjecture 3.2 satisfy also (3.3).

**References**


A SURVEY ON SOME RECENT INVESTIGATIONS OF PROBABILITY IN GROUP THEORY

[16] H. Doostie and M. Maghasedi, Certain classes of groups with commutativity degree $d(G) < 1/2$, Ars Combinatoria 89 (2008), 263–270.
[34] M.R. Pournaki and R. Sobhani, Probability that the commutator of two group elements is equal to a given element, J. Pure Appl. Algebra 212 (2008), 727–734.

DEPARTMENT OF MATHEMATICAL SCIENCES, FACULTY OF APPLIED SCIENCES, UMM ALQURA UNIVERSITY, P.O. BOX 14035, MAKKAH, 21955, SAUDI ARABIA
E-mail address: amghamdi@uqu.edu.sa

DÉPARTEMENT DE MATHEMATIQUE, BATIMENT 425, FACULTÉ DE SCIENCE D’ORSAY, UNIVERSITÉ PARIS-SUD 11, F-91405, ORSAY CEDEX, FRANCE
E-mail address: daniele.otera@math-psud.fr

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF PALERMO, VIA Archirafi 14, 90123, PALERMO, ITALY.
E-mail address: francescog.russo@yahoo.com