Subnormalizers and the degree of nilpotence in finite groups

SUBNORMALIZERS AND THE DEGREE OF NILPOTENCE IN FINITE GROUPS

PIETRO GHERI

ABSTRACT. We present a CFSG-free proof of the fact that the degree of nilpotence of a finite nonnilpotent group is less than $1/2$.

1. INTRODUCTION AND TOOLS

Let G be a finite group. The *degree of commutativity of* G is the probability that two randomly chosen elements of G commute. As a natural generalization, the *degree of nilpotence of* G is defined to be the probability that two randomly chosen elements of G generate a nilpotent subgroup, that is

$$\mathrm{dn}(G) = \frac{|\{(x,y) \in G \mid \langle x,y\rangle \text{ is nilpotent }\}|}{|G|^2} = \frac{1}{|G|}\sum_{x\in G}\frac{|Nil_G(x)|}{|G|}. \tag{1}$$

where for any $x \in G$, $Nil_G(x)$ is the set of elements $y \in G$ such that $\langle x, y\rangle$ is nilpotent.

In 1978 Gustafson proved that the degree of commutativity of a finite nonabelian group is less or equal than $5/8$ ([4]). In [3] Guralnick and Wilson proved an analogous theorem for the degree of nilpotence.

Theorem 1.1. *Let G be a finite group. If $\mathrm{dn}(G) > 1/2$ then G is nilpotent. The value $1/2$ is tight.*

This was obtained as a corollary of a similar result concerning the probability that two elements generate a solvable subgroup. However, while Gustafson's proof was very short and only involved basic tools, Guralnick and Wilson's proof used the Classification of finite simple groups. In that work the authors ask if there is a Classification-free proof of their result on the degree of nilpotence. In this paper we present such a proof.

We immediately clarify that the tightness of the value $1/2$ is trivial, since one can verify directly that $\mathrm{dn}(S_3) = 1/2$.

The first step in our proof consists of replacing the set $Nil_G(x)$ in (1) with another set, namely $S_G(\langle x\rangle)$, the *Wielandt subnormalizer of* $\langle x\rangle$ *in* G. The reasons of this substitution will be clarified in the last section.

Definition 1.2 ([5], page 238)**.** Let H be a subgroup of G. The *subnormalizer of* H *in* G is the set

$$S_G(H) = \{g \in G \mid H \trianglelefteq\trianglelefteq \langle H, g\rangle\}.$$

Wielandt's subnormality criterion can be restated using this definition: a subgroup H of a finite group G is subnormal if and only if $S_G(H) = G$.

A crucial result for our proof is a theorem proved by Casolo in 1990 which gives a formula to count the elements of the subnormalizer of a p-subgroup. Given a prime p

2010 *Mathematics Subject Classification.* 20D15, 20P05.

dividing the order of G and a p-subgroup H of G, we write $\lambda_G(H)$ for the number of Sylow p-subgroups of G containing H. When $H = \langle x \rangle$ is a cyclic subgroup we write $S_G(x)$ and $\lambda_G(x)$, in place of $S_G(\langle x \rangle)$ and $\lambda(\langle x \rangle)$.

Theorem 1.3 ([2]). *Let H be a p-subgroup of G and $P \in Syl_p(G)$. Then*

$$|S_G(H)| = \lambda_G(H)|N_G(P)|. \tag{2}$$

The proof of this result does not rely on CFSG.

With the degree of nilpotence in mind, we can then define a new probability where, as we said before, $Nil_G(x)$ is replaced by $S_G(x)$. If we set $\mathrm{sp}_G(x) = |S_G(x)|/|G|$ we have that $\mathrm{sp}_G(x) \geq |Nil_G(x)|/|G|$ since every subgroup of a finite nilpotent group is subnormal. Then we set

$$\mathrm{sp}(G) = \frac{1}{|G|}\sum_{x \in G} \frac{|S_G(x)|}{|G|}.$$

Moreover if x is a p-element, using Theorem 1.3 the ratio $\mathrm{sp}_G(x)$ can be written as

$$\mathrm{sp}_G(x) = \frac{|S_G(x)|}{|G|} = \frac{\lambda_G(x)|N_G(P)|}{|G|} = \frac{\lambda_G(x)}{n_p(G)} \tag{3}$$

where $n_p(G)$ is the number of Sylow p-subgroups of G. The value $\mathrm{sp}_G(x)$ is then the proportion of Sylow p-subgroups of G containing x.

2. Proof

The main step for our proof of Theorem 1.1 is the following probabilistic version for cyclic subgroups of Wielandt's subnormality criterion.

Proposition 2.1. *Let p be a prime dividing the order of G, $x \in G$ be a p-element of order p^r and $1 \leq k \leq r$. If $\mathrm{sp}_G(x) > 1/(p^k + 1)$ then $x^{p^{k-1}} \in O_p(G)$.*

Proof. By (2), we have $\mathrm{sp}_G(x) = \lambda_G(x)/n_p(G)$. Let $y_1, \dots, y_{p^k+1}$ be $p^k + 1$ distinct conjugates of x. Then there exists $P \in Syl_p(G)$ such that two of these conjugates both belong to P. For if not,

$$U_i = \{P \in Syl_p(G) \mid y_i \in P\},\ i \in \{1, \dots, p^k + 1\},$$

would be disjoint sets, each of cardinality $\lambda_G(x)$ (since the function λ_G is constant on the conjugacy classes of p-elements) and we would have

$$n_p(G) \geq \left| \bigcup_{i=1}^{p^k+1} U_i \right| = (p^k + 1)\lambda_G(x)$$

against the hypothesis.

Let $g \in G$ and set $y_0 = x$, $y_i = x^{gx^{i-1}}$ for $1 \leq i \leq p^k$. We then have two cases: either there exist $0 \leq i < j \leq p^k$ such that $y_i = y_j$ or the set of the y_i's has cardinality $p^k + 1$. In any case we then have that the following statement holds.

(∗) There exist i, j such that $0 \leq i < j \leq p^k$ and $\langle y_i, y_j \rangle$ is a p-group

We want to prove that if (∗) holds for all $g \in G$ then $x^{p^{k-1}} \in O_p(G)$. Arguing by induction on $|G|$ we can suppose that $x^{p^{k-1}} \in O_p(H)$, that is $\langle x^{p^{k-1}} \rangle$ is subnormal in H, for all proper subgroups H of G containing $x^{p^{k-1}}$.

We now recall the statement of the so-called zipper lemma of Wielandt, [5, Lemma 7.3.1]. Let K be a subgroup of a finite group G such that K is not subnormal in G, but

$K \trianglelefteq \trianglelefteq H$ for all proper subgroups of G containing K. Then K is contained in a unique maximal subgroup M of G; moreover, if for some $g \in G$, K^g is contained in M then $g \in M$.

Suppose that $x^{p^{k-1}} \notin O_p(G)$. Then, by the aformentioned zipper lemma, $x^{p^{k-1}}$ is contained in a unique maximal subgroup M of G, which is not normal in G.

If $1 \leq s < p^k$ then $x^{p^{k-1}} \in \langle x^s \rangle$ and so M is the unique maximal subgroup containing x^s. Moreover if for some $a \in G$, $(x^s)^a \in M$ then $x^s \in M^{a^{-1}}$ and so $M = M^{a^{-1}}$. Since M is maximal and is not normal in G, we have $a \in M$.

Let then $g \in G$, y_i be defined as above and suppose that $(*)$ holds. We separately consider two cases: one in which $i = 0$ and the other in which $i \geq 1$. If $i = 0$ then $\langle x, y_j \rangle$ is a p-group, which implies that $y_j = x^{gx^{j-1}} \in M$. It follows that $gx^{j-1} \in M$ and so $g \in M$. If instead $i \geq 1$ then $\langle y_i, y_j \rangle$ is a p-group and so is the subgroup

$$\langle x^{(x^{j-i})^{g^{-1}}}, x \rangle = \langle y_i, y_j \rangle^{x^{-(i-1)}g^{-1}}.$$

It follows that $x^{(x^{j-i})^{g^{-1}}} \in M$, so $(x^{j-i})^{g^{-1}} \in M$ and finally $g^{-1} \in M$.

We proved that if $(*)$ holds then $g \in M$. It follows that $G \leq M$, a contradiction. $\square$

The bound in the previous proposition is the best possible, as we can see looking at $G = PSL(2,p)$. We have that each Sylow p-subgroup of G has cardinality p, $n_p(G) = p+1$ and $O_p(G) = 1$. Then if $x \in G$ is a p-element we have that $\mathrm{sp}(G) = 1/(p+1)$.

Corollary 2.2. *Let $x \in G$ be an element that does not lie in the Fitting subgroup $\mathbf{F}(G)$ of G. Then $\mathrm{sp}_G(x) \leq 1/3$.*

Proof. Let p be a prime dividing the order of x such that the p-part x_p of x does not lie in $O_p(G)$. Then by Proposition 2.1 we have $\mathrm{sp}_G(x) \leq \mathrm{sp}_G(x_p) \leq 1/(p+1)$. $\square$

We can now prove Theorem 1.1.

Proof. First of all we observe that $[G : \mathbf{F}(G)] \leq 3$. For if $[G : \mathbf{F}(G)] \geq 4$ then by Corollary 2.2

$$\begin{aligned}
\mathrm{dn}(G) \leq \mathrm{sp}(G) &= \frac{1}{|G|}\sum_{x \in G}\frac{|S_G(x)|}{|G|} \\
&= \frac{1}{|G|}\left(|\mathbf{F}(G)| + \sum_{x \notin \mathbf{F}(G)}\frac{|S_G(x)|}{|G|}\right) \\
&\leq \frac{1}{|G|}\left(|\mathbf{F}(G)| + \frac{1}{3}\frac{|G| - |\mathbf{F}(G)|}{|G|}\right) \\
&= \frac{|G| + 2|\mathbf{F}(G)|}{3|G|} \leq \frac{1}{3} + \frac{1}{6} = \frac{1}{2}.
\end{aligned} \tag{4}$$

Thus $[G : \mathbf{F}(G)] \in \{2, 3\}$. Let G be a counterexample of minimal order. It is an easy exercise to verify that setting $N := \mathbf{F}(G)$, we have $G = N\langle x \rangle$ with $|x| = q \in \{2, 3\}$ and N is an elementary abelian group of order say p^k, for some prime $p \neq q$. Moreover $C_N(x) = 1$ and G is a Frobenius group with kernel N. For every $1 \neq a \in N$ we have

$$Nil_G(a) = N,$$

while for every $y \notin N$ we have

$$Nil_G(y) = \langle y \rangle.$$

Therefore

$$\operatorname{dn}(G) = \frac{1}{|G|}\sum_{g\in G}\frac{|Nil_G(g)|}{|G|} = \frac{1}{|G|}\left(\sum_{g\in N}\frac{|Nil_G(g)|}{|G|} + \sum_{g\notin N}\frac{|Nil_G(g)|}{|G|}\right)$$
$$= \frac{1}{p^k q}\left(1 + (p^k-1)\frac{1}{q} + (q-1)p^k\frac{1}{p^k}\right) = \frac{1}{p^k q} + \frac{p^k-1}{p^k}\frac{1}{q^2} + \frac{q-1}{p^k q},$$

which is greater then $1/2$ if and only if $q = 2$ and $p^k = 3$, that is if and only if $G \simeq S_3$. By direct calculation one see that $\operatorname{dn}(S_3) = 1/2$ and so we have the assertion. □

The next theorem is another result with the flavour of Gustafson's theorem, concerning the probability $\operatorname{sp}(G)$.

Theorem 2.3. *If* $\operatorname{sp}(G) > 2/3$ *then* G *is nilpotent, and the bound is the best possible.*

Proof. This is just a calculation which follows easily from Corollary 2.2. Let G be a nonnilpotent group: then $|\mathbf{F}(G)| \leq |G|/2$. Thus

$$\operatorname{sp}(G) = \frac{1}{|G|}\sum_{g\in G}\operatorname{sp}_G(x) = \frac{1}{|G|}\sum_{g\in \mathbf{F}(G)}\operatorname{sp}_G(x) + \frac{1}{|G|}\sum_{g\notin \mathbf{F}(G)}\operatorname{sp}_G(x)$$
$$\leq \frac{|\mathbf{F}(G)|}{|G|} + \frac{1}{3}\frac{|G\setminus \mathbf{F}(G)|}{|G|} = \frac{1}{3} + \frac{2}{3}\frac{|\mathbf{F}(G)|}{|G|} \leq \frac{2}{3}.$$

The fact that the bound is tight follows from an easy calculation that gives $\operatorname{sp}(S_3) = 2/3$. □

3. Some examples and remarks

In this section we first of all explain why it is crucial for our proof of Theorem 1.1 to replace $Nil_G(x)$ with $S_G(x)$. Looking at Gustafson's proof about the degree of commutativity ([4]) we find that a fundamental fact is that if $x \in G$ satisfies $|C_G(x)| > |G|/2$ then $x \in Z(G)$, that is $C_G(x) = G$. Corollary 2.2 gives a similar result concerning $S_G(x)$: if $|S_G(x)| > |G|/3$ then $x \in \mathbf{F}(G)$, that is $S_G(x) = G$. It is not difficult to see that the elements x such that $Nil_G(x) = G$ are exactly the elements in $\zeta_\omega(G)$, the hypercenter of G. The question could then be asked if there is a constant $c > 0$ such that if $|Nil_G(x)|/|G| > c$ then $x \in \zeta_\omega(G)$. The following proposition shows that such a constant does not exist.

Proposition 3.1. *There exists a sequence of groups* $(G_k)_{k\in\mathbb{N}}$ *together with* $x_k \in G_k$ *such that* $Z(G_k) = 1$ *and*

$$\lim_{k\to\infty}\frac{|Nil_{G_k}(x_k)|}{|G_k|} = 1.$$

Proof. For $k \in \mathbb{N}$ and $k \geq 2$, let $n = 2^k$. Moreover let $\mathbb{K} = \mathbb{F}_{2^n}$ be the field with 2^n elements and V be the additive group of $\mathbb{K}$, so that V is an elementary abelian group of size 2^n.

By Zsigmondy's theorem there exists a prime p which divides $2^n - 1$ and doesn't divide $2^l - 1$ for any $1 \leq l < n$. Let $P = \langle x\rangle$ be the subgroup of order p in the multiplicative group $\mathbb{K}^\times$. P acts fixed point freely on V by multiplication and the elements of the group $V \rtimes P$ have order either 2 or p.

Let $\mathcal{G} = Gal(\mathbb{K}|\mathbb{F}_2)$, a cyclic group of order $n = 2^k$. Then $\mathcal{G}$ acts both on V and on P. If $\sigma \in \mathcal{G}$ is such that $x^\sigma = x$ then $x \in \mathbb{E} = \operatorname{Fix}_{\mathbb{K}}(\langle\sigma\rangle)$ the field fixed by σ. Since $x \notin \mathbb{F}_2$

we have $\mathbb{E} > \mathbb{F}_2$. By the choice of p, and since $|x| = p$ has to divide $|\mathbb{E}| - 1$, we have that $\mathbb{E} = \mathbb{K}$ so that $\sigma = 1$, i.e., $\mathcal{G}$ acts fixed point freely on P.

We can consider the group $G = (V \rtimes P) \rtimes \mathcal{G}$, whose order is $2^{n+k}p$.

It is easy to see that there are not any elements of composite order in G. In particular $Z(G) = 1$. Moreover $N_G(S) = S$ for all $S \in Syl_2(G)$ and if $S_1, S_2 \in Syl_2(G)$, $S_1 \neq S_2$, then $S_1 \cap S_2 = V$. Then $V = O_2(G)$ and so for all $v \in V \setminus 1$

$$Nil_G(v) = \bigcup_{S \in Syl_2(G)} S = V \cup (G \setminus (VP)).$$

Finally

$$\frac{|Nil_G(v)|}{|G|} = \frac{2^n + 2^{n+k}p - 2^n p}{2^{n+k}p} = 1 - \frac{p-1}{2^k p},$$

which tends to 1 as k tends to infinity. □

In [5], page 238, some candidates for the role of *subnormalizer* are defined, other then the one we used (Definition 1.2). For example, inspired by the Baer-Suzuki theorem, we may define $S^1_G(H)$ as follows:

$$S^1_G(H) = \{g \in G \mid H \trianglelefteq\trianglelefteq \langle H, H^g \rangle\}.$$

As explained in [1] the cardinality of this set can be written as

$$|S^1_G(H)| = \delta_G(H)|N_G(H)|$$

where

$$\delta_G(H) = \{H^g \mid H \trianglelefteq\trianglelefteq \langle H, H^g \rangle\}.$$

The following example shows that there is not an equivalent of Corollary 2.2 for $S^1_G(x)$, that is, a probabilistic version of the Baer-Suzuki theorem.

Example 3.2. Let $n = 2k$ for $k \in \mathbb{N}, k \geq 2$ and let $G = S_n, x = (1, 2)$. We want to count the number of transpositions that generates a 2-group together with x. If y is such a transposition then y commutes with x, because otherwise xy would be a 3-cycle. Then

$$\delta_G(x) = |\{x\} \cup \{(i, j) \mid 2 < i < j \leq n\}| = 1 + \frac{(n-2)(n-3)}{2}$$

and so

$$\frac{|S^1_G(x)|}{|G|} = \frac{1 + \frac{(n-2)(n-3)}{2}}{\frac{n(n-1)}{2}}$$

which tends to 1 as n goes to infinity.

Acknowledgements. This note is drawn from the author's PhD thesis which was undertaken at Università degli Studi di Firenze, and written under the patient supervision of Carlo Casolo, to whom a great deal of thanks is owed. The author would also like to thank Francesco Fumagalli and Eugenio Giannelli for their valuable comments and suggestions.

REFERENCES

1. Carlo Casolo. Subnormalizers in finite groups. *Communications in Algebra*, (18, n.11), 1990.
2. Carlo Casolo. On the subnormalizer of a p-subgroup. *Journal of Pure and Applied Algebra*, (77, n.3), 1992.
3. Robert M. Guralnick and John S. Wilson. The probability of generating a finite soluble group. *Proceedings of the London Mathematical Society*, (81, n.2), 2000.
4. William H. Gustafson. What is the probability that two group elements commute? *American Mathematical Monthly*, (80), 1973.
5. John C. Lennox and Stewart E. Stonehewer. *Subnormal subgroups of groups*. Oxford University Press, 1987.

DIPARTIMENTO DI MATEMATICA E INFORMATICA "U. DINI",
UNIVERSITÀ DEGLI STUDI DI FIRENZE, VIALE MORGAGNI 67/A, 50134 FIRENZE, ITALY.
Email address: pietro.gheri@unifi.it