Arch. Math. 115 (2020), 599–609

0003-889X/20/060599-11
published online July 17, 2020
https://doi.org/10.1007/s00013-020-01504-w

Archiv der Mathematik

Check for updates

Word problems for finite nilpotent groups

Rachel D. Camina, Ainhoa Iñiguez, and Anitha Thillaisundaram

Abstract. Let w be a word in k variables. For a finite nilpotent group G, a conjecture of Amit states that $N_w(1) \geq |G|^{k-1}$, where for $g \in G$, the quantity $N_w(g)$ is the number of k-tuples $(g_1, \ldots, g_k) \in G^{(k)}$ such that $w(g_1, \ldots, g_k) = g$. Currently, this conjecture is known to be true for groups of nilpotency class 2. Here we consider a generalized version of Amit's conjecture, which states that $N_w(g) \geq |G|^{k-1}$ for g a w-value in G, and prove that $N_w(g) \geq |G|^{k-2}$ for finite groups G of odd order and nilpotency class 2. If w is a word in two variables, we further show that the generalized Amit conjecture holds for finite groups G of nilpotency class 2. In addition, we use character theory techniques to confirm the generalized Amit conjecture for finite p-groups (p a prime) with two distinct irreducible character degrees and a particular family of words. Finally, we discuss the related group properties of being rational and chiral, and show that every finite group of nilpotency class 2 is rational.

Mathematics Subject Classification. Primary 20F10, Secondary 20D15.

Keywords. Words, Amit's conjecture, Rational words.

1. Introduction. A word w in k variables $x_1, \ldots, x_k$ is an element in the free group F_k on $x_1, \ldots, x_k$. For any k elements $g_1, \ldots, g_k$ in a group G, we can define the element $w(g_1, \ldots, g_k) \in G$ by applying to w the group homomorphism from F_k to G sending x_i to g_i for $1 \leq i \leq k$.

We denote by G_w the set of word values of w in G, i.e., the set of elements $g \in G$ such that the equation $w = g$ has a solution in $G^{(k)}$, the direct product of k copies of G.

For a word w in k variables and a group G, for any $g \in G$, the *fibre* of g in $G^{(k)}$ is

$$\{(g_1, \ldots, g_k) \in G^{(k)} \mid w(g_1, \ldots, g_k) = g\}.$$

If G is a finite group and $g \in G$, we define $N_{w,G}(g)$ to be

$$N_{w,G}(g) = |\{(g_1, \ldots, g_k) \in G^{(k)} \mid w(g_1, \ldots, g_k) = g\}|;$$

i.e., the size of the fibre of g in $G^{(k)}$. When the group G is clear, we will simply write $N_w(g)$. The function $N_{w,G}$ is a (non-negative) integer-valued class function since it is constant on the conjugacy classes. The set $\mathrm{Irr}(G)$ of irreducible complex characters of G is an orthonormal basis for the vector space of the complex class functions and $N_{w,G}$ can be written as a linear combination of the irreducible characters of G:

$$N_{w,G} = N_w = \sum_{\chi \in \mathrm{Irr}(G)} N_w^{\chi} \chi$$

where

$$N_w^{\chi} = (N_w, \chi) = \frac{1}{|G|} \sum_{g \in G} N_w(g)\overline{\chi(g)} = \frac{1}{|G|} \sum_{(g_1,\ldots,g_k) \in G^{(k)}} \overline{\chi\big(w(g_1, \ldots, g_k)\big)}$$

is unique for any $\chi \in \mathrm{Irr}(G)$.

Much about the functions $N_{w,G}$, or rather $P_{w,G} = N_{w,G}/|G|^k$, has been done, particularly for the commutator word $w = [x, y]$ and for the case G is a p-group for some prime p; see [1,4,9,12,13,22] and also [2,3,7,8,10,18]. In addition, Nikolov and Segal [20] gave a characterization of finite nilpotent groups and of finite solvable groups based on the function $P_{w,G}$: a finite group is nilpotent if and only if the values of $P_{w,G}(g)$ are bounded away from zero as g ranges over G_w and w ranges over all group words; and a finite group is solvable if and only if the probabilities $P_{w,G}(1)$ are bounded away from zero as w ranges over all group words. Iñiguez and Sangroniz [13] proved that for any finite group G of nilpotency class 2 and any word w, the function N_w is a generalized character of G, that is, a $\mathbb{Z}$-linear combination of irreducible characters. What is more, if G is a finite p-group of nilpotency class 2 with p odd and w any word, then N_w is a character of G. In general, for $p = 2$, the function N_w is not a character; one can easily check for N_{x^2,Q_8}. In [13], the authors also characterize when the function N_{x^n} is a character for 2-groups of nilpotency class 2.

The following is well known; see [1]:

Conjecture (Amit). *For any finite nilpotent group G and any word w in k variables,*

$$N_w(1) \geq |G|^{k-1}.$$

Up till now, Amit's conjecture has only been proved for groups of nilpotency class 2. This was done by Levy [15] and independently by Iñiguez and Sangroniz [13].

Amit's conjecture is seen to hold for certain words w. If w is a two-variable word, then $N_w(1) \geq |G|$ for all finite nilpotent groups G by Solomon [23]. Whenever $N_{w,G}$ is a character, Amit's conjecture also holds; see [13]. It then follows that Amit's conjecture holds for all left-normed commutators $w_n = [x_1, \ldots, x_n]$ and for all generalized commutators $v_n = x_1x_2\cdots x_nx_1^{-1}x_2^{-1}\cdots x_n^{-1}$; see [19,24] respectively.

We consider a version of Amit's conjecture as applied to general fibres:

Conjecture (Generalized Amit conjecture). *For any finite nilpotent group G, any word w in k variables, and any $g \in G_w$,*

$$N_w(g) \geq |G|^{k-1}.$$

This appears as a conjecture in Ashurst's thesis [4, Conjecture 6.2.1]. Note that the bound $N_w(g) = |G|^{k-1}$ is achieved by a surjective word map with uniform distribution for example $w = x[y, z]$. Moreover, Cocke and Ho have shown that a finite group is nilpotent if and only if every surjective word map has uniform distribution [6, Theorem B], so the Amit bound is met by all surjective word maps. By Solomon's result in [23], we also know that if w is a two variable word, then $N_w(g) \geq |G|$ for all $g \in Z(G)$ and all finite nilpotent groups G. Here we improve this result to all groups G of nilpotency class 2 and all $g \in G_w$.

However first note that since a finite nilpotent group is a direct product of its Sylow subgroups, it suffices to consider finite p-groups. This is because if $G = H \times K$, and $g = hk \in G_w$ for an n-variable word w with $h \in H$ and $k \in K$, then $N_{w,G}(g) = N_{w,H}(h)N_{w,K}(k)$. This relies on the fact that if $g_i = h_ik_i$ for $1 \leq i \leq n$ with $h_i \in H$ and $k_i \in K$, then $w(g_1, \ldots, g_k) = w(h_1k_1, \ldots, h_nk_n) = w(h_1, \ldots, h_n)w(k_1, \ldots, k_n)$. Hence if the conjecture holds for each group H and K, it then holds for their direct product G.

Theorem A. *Suppose G is a finite p-group of nilpotency class 2 and w is a word in two variables. Then $N_w(g) \geq |G|$ for all $g \in G_w$.*

Iñiguez and Sangroniz [13] proved that the generalized Amit conjecture holds for free p-groups of nilpotency class 2 and exponent p. Our next result does not meet Amit's bound, but can be proved for all words w and for all groups G of odd order and nilpotency class 2.

Theorem B. *Suppose G is a finite p-group of nilpotency class 2 for p an odd prime, and w is a word in k variables. Then $N_w(g) \geq |G|^{k-2}$ for all $g \in G_w$.*

Next, we extend a result of Pournaki and Sobhani to words w_ℓ of the form $w_\ell = [x_1, y_1]\cdots[x_\ell, y_\ell]$. Pournaki and Sobhani originally considered the single commutator w_1 [21, Theorem 2.2]. Before stating our result, we recall that $\mathrm{cd}(G)$ denotes the set of degrees of irreducible complex characters of G, and $\mathrm{cs}(G)$ denotes the set of conjugacy class sizes in G.

Theorem C. *Let G be a finite p-group such that $\mathrm{cd}(G) = \{1, m\}$ for $m > 1$ and $w_\ell = [x_1, y_1]\cdots[x_\ell, y_\ell]$ a product of ℓ disjoint commutators for $\ell \in \mathbb{N}$. Then $G' = G_{w_\ell}$ and $|\{N_{w_\ell}(g) : g \in G'\}| = 2$. Furthermore $N_{w_\ell}(g) \geq |G|^{2\ell-1}$ for all $g \in G'$.*

It is interesting to note that if instead of requiring $|\mathrm{cd}(G)| = 2$ we require $|\mathrm{cs}(G)| = 2$, then there exist groups with $|\{N_{w_\ell}(g) : g \in G_{w_\ell}\}| = n$ for all positive integers n. This is a recent result due to Naik [17].

Theorem C yields the following corollary.

Corollary D. *Let G be a finite group of nilpotency class 2 and $|G'| = p$ with p a prime. Then $N_{w_\ell}(g) \geq |G|^{2\ell-1}$ whenever $g \in G'$.*

We remark that the same result for N_{w_ℓ} was obtained in [13, Propositions 6.1 and 6.2] for finite p-groups with different restrictions.

Finally we consider the different notions of rationality and chirality; see Section 4 for definitions. In particular, we point out that if G is a finite group of nilpotency class 2 and w is a word, then $N_w(g) = N_w(g^e)$ for all e coprime to the order of G. This is an improvement on [5, Theorem 5.2] for the case of finite groups.

All groups in this paper are finite.

2. Fibres of non-identity elements. Given a group G of nilpotency class 2 and a word w, we consider the sizes of fibres of non-identity elements under the word map.

First we observe that if the word map $w : G^{(k)} \to G$ which sends $(x_1, \dots, x_k)$ to $w(x_1, \dots, x_k)$ is a homomorphism, then the fibre of any element in G_w is a coset of the kernel of the map. Hence the fibre of each element in G_w is of the same size, namely $|G|^k/|G_w|$ (which is at least $|G|^{k-1}$). When G is abelian, all word maps are homomorphisms. We use this idea to analyse the nilpotency class 2 case.

Another key observation, that will be used throughout, is that $[xy, z] = [x, z][y, z]$ and $[x, yz] = [x, y][x, z]$ in a group of nilpotency class 2.

Two words $w, w' \in F_k$ are said to be *equivalent* if they belong to the same orbit under the action of the automorphism group of F_k. In [13, Proposition 2.1], the authors prove that if w and w' are equivalent, then $N_{w,G} = N_{w',G}$ for any finite p-group G of nilpotency class 2. They then go on to prove that the following words are a system of representatives of the action of $\mathrm{Aut}(F_k)$ on F_k [13, Proposition 2.3]:

$$[x_1, x_2]^{p^{s_1}} \cdots [x_{2r-1}, x_{2r}]^{p^{s_r}}, \quad \text{for } 0 \leq s_1 \leq \cdots \leq s_r, \tag{1}$$

$$x_1^{p^{s_1}} [x_1, x_2]^{p^{s_2}} [x_2, x_3]^{p^{s_3}} \cdots [x_{r-1}, x_r]^{p^{s_r}}, \quad \text{for } s_1 \geq 0,\ 0 \leq s_2 \leq \cdots \leq s_r. \tag{2}$$

Thus, it is enough for us to consider words of these types. We can now prove Theorem A.

Proof of Theorem A. Let Z denote the centre of G. We first consider words of type (1), so $w = [x_1, x_2]^{p^{s_1}}$. In this case, $G_w \subseteq Z$ and the result follows from Solomon's result [23].

Now consider words of type (2), so $w = x_1^{p^{s_1}} [x_1, x_2]^{p^{s_2}}$. If $G^{p^{s_1}} \leq Z$, then again the result follows from [23]. So, suppose $G^{p^{s_1}}$ is not central, then $Z^{p^{s_1}} \neq 1$. We now proceed by induction on the order of G, noting that the result holds for abelian groups.

Suppose $g \in G_w$ and $\mathbf{\Omega} = w^{-1}(g)$, the preimage of g in $G^{(2)}$. Let $N = Z^{p^{s_1}}$ and consider $\bar{G} = G/N$. Set $\bar{\mathbf{\Omega}} = w^{-1}(\bar{g}) \subseteq \bar{G}^{(2)}$. Inductively $|\bar{\mathbf{\Omega}}| \geq |\bar{G}|$. For each $\mathbf{v} \in \bar{\mathbf{\Omega}}$, choose a representative $(a_1, a_2) \in G^{(2)}$ with $(\bar{a}_1, \bar{a}_2) = \mathbf{v}$. Then $w(a_1, a_2) = gu^{p^{s_1}}$ for some $u \in Z$ and then $w(a_1u^{-1}, a_2s_2) = g$ for all $s_2 \in N$. So

$$\mathbf{\Omega} \supseteq \bigcup_{\mathbf{v}\in\bar{\mathbf{\Omega}}} \{a_1u^{-1}\} \times a_2N,$$

a disjoint union. Hence $|\mathbf{\Omega}| \geq |N||\bar{\mathbf{\Omega}}| \geq |G|$. □

Before proving Theorem B, we introduce one more concept, that of the 'defined word map'. We are used to a word $w \in F_k$ defining a word map from $G^{(k)}$ to G. In a defined word map, some of the entries are fixed elements of G and are not allowed to vary. For a fixed tuple $(a_1, \ldots, a_k) \in G^{(k)}$, we will write $w^{(i_1,\ldots,i_k)}_{(a_1,\ldots,a_k)}$ for the defined word map where the i_j-th term is replaced with a_j. This is particularly useful when G is of nilpotency class 2 as then this defined word map is often a homomorphism.

Proof of Theorem B. We first consider words of type (1), in this case, the argument also works for $p = 2$. Given w of type (1), we consider the corresponding defined word map given by fixing the even entries as $(a_2, a_4, \ldots, a_{2r}) \in G^{(r)}$ say. That is

$$w^{(2,4,\ldots,2r)}_{(a_2,a_4,\ldots,a_{2r})} : G \times \overset{r}{\cdots} \times G \to G,$$
$$(x_1, x_3, \ldots, x_{2r-1}) \mapsto [x_1, a_2]^{p^{s_1}} \cdots [x_{2r-1}, a_{2r}]^{p^{s_r}}.$$

As G is of nilpotency class 2, this map is a homomorphism. Furthermore, the image is a subgroup of the centre Z of G and thus the kernel has size at least $|G|^r/|Z|$.

Suppose $g \in G_w$ and in particular $g = w(a_1, a_2, a_3 \ldots, a_{2r})$ for some $a_i \in G$. Now, by the previous paragraph, if we fix the a_i for i even, we see there are at least $|G|^r/|Z|$ tuples $(b_1, b_3, \ldots, b_{2r-1})$ satisfying $g = w(b_1, a_2, b_3, \ldots, b_{2r-1}, a_{2r})$. Fix such a $(b_1, b_3, \ldots, b_{2r-1})$, and construct the new defined word map $w^{(1,3,\ldots,2r-1)}_{(b_1,b_3,\ldots,b_{2r-1})}$ which sends $G^{(r)}$ to G by mapping $(x_2, x_4, \ldots, x_{2r})$ to $w(b_1, x_2, \ldots, b_{2r-1}, x_{2r})$. Again this is a homomorphism to Z. Note that g lies in the image of each of these maps, and the preimage of g for each of these homomorphisms has size at least $|G|^r/|Z|$. Thus summing over the r-tuples $(b_1, b_3, \ldots, b_{2r-1})$ yields that $N_w(g) \geq (|G|^r/|Z|)(|G|^r/|Z|) = |G|^{2r}/|Z|^2 \geq |G|^{2r-2}$.

We now consider words of type (2). We consider different cases depending on whether $Z^{p^{s_1}}$ is trivial or not. When $Z^{p^{s_1}} \neq 1$, we use induction on the order of the group: we assume that for all groups of smaller order of nilpotency class 2 or less, our result holds. Note the result holds for abelian groups so we have the base step.

Case (i): Suppose $Z^{p^{s_1}} = 1$.

Suppose $g \in G_w$ and in particular $g = w(a_1, \ldots, a_r)$ for some $a_i \in G$. Define

$$\bar{w} = [x_1, x_2]^{p^{s_2}} [x_2, x_3]^{p^{s_3}} \cdots [x_{r-1}, x_r]^{p^{s_r}}.$$

Then $a_1^{-p^{s_1}} g = \bar{w}(a_1, \ldots, a_r)$. Fixing the odd elements and constructing the corresponding defined word map $\bar{w}^{(1,3,\ldots,t)}_{(a_1,a_3,\ldots,a_t)}$, where $t = 2\lceil r/2\rceil - 1$, gives a homomorphism into Z. Thus the number of tuples $(b_2, \ldots, b_s)$, with $s = 2\lfloor r/2\rfloor$, such that $\bar{w}(a_1, b_2, \ldots) = a_1^{-p^{s_1}} g$ and thus $w(a_1, b_2, \ldots) = g$ is at least $|G|^{\lfloor r/2\rfloor}/|Z|$.

Fixing the even elements of w does define a homomorphism as we have insisted $Z^{p^{s_1}} = 1$ and p odd and thus $(y_1y_2)^{p^{s_1}} = y_1^{p^{s_1}} y_2^{p^{s_1}}$ as required. Furthermore $G^{p^{s_1}}$ is central, as $Z^{p^{s_1}} = 1$, and thus the corresponding defined word map is a homomorphism into Z. So, fixing the even elements yields a homomorphism with kernel of order at least $|G|^{\lceil r/2\rceil}/|Z|$. Thus, combining as before gives that g has a fibre of size at least

$$(|G|^{\lfloor r/2\rfloor}/|Z|)(|G|^{\lceil r/2\rceil}/|Z|) = |G|^r/|Z|^2 \geq |G|^{r-2}.$$

When $Z^{p^{s_1}} \neq 1$, we proceed by induction and use the usual word map, as seen below.

Case (ii): Suppose $Z^{p^{s_1}} \neq 1$.

Here we proceed analogously to the last paragraph in the proof of Theorem A. In the notation of that proof, we obtain

$$\mathbf{\Omega} \supseteq \bigcup_{\mathbf{v}\in\bar{\mathbf{\Omega}}} \{a_1u^{-1}\} \times a_2N \times \cdots \times a_rN,$$

a disjoint union. Thus $|\mathbf{\Omega}| \geq |N|^{r-1}|\bar{\mathbf{\Omega}}| \geq |G|^{r-2}$. □

Remark 2.1. (i) For a word w of type (1) and all primes p, if $|Z|^2 \leq |G|$, then the generalized Amit conjecture holds.

(ii) For a word w of type (2) with $s_1 = 0$, the word map defined by w is surjective and hence its distribution is uniform; cf. [4, Lemma 3.2.1] or [6, Theorem B]. This implies that the generalized Amit conjecture holds.

3. Characters. Here we show, using character theory techniques, that the generalized Amit conjecture holds for certain words and certain groups.

Recall $w_\ell(x_1, y_1, \ldots, x_\ell, y_\ell) = [x_1, y_1]\cdots[x_\ell, y_\ell]$ is the product of ℓ disjoint commutators for $\ell \in \mathbb{N}$, and $\mathrm{cd}(G)$ is the set of degrees of irreducible complex characters of G. The following results first appeared in the second author's thesis.

Theorem 3.1. *Let G be a finite p-group such that $\mathrm{cd}(G) = \{1, m\}$ for $m > 1$. If $1 \neq g \in G'$, then*

$$N_{w_\ell}(g) = \frac{|G|^{2\ell}}{|G'|}\Big(1 - \frac{1}{m^{2\ell}}\Big).$$

Furthermore $G' = G_{w_\ell}$ and $N_{w_\ell}(g) \geq |G|^{2\ell-1}$ for $1 \neq g \in G'$.

Proof. For $1 \neq g \in G'$, using the second orthogonality relation [14, Theorem 2.18], we have

$$\begin{aligned} 0 &= \sum_{\chi\in\mathrm{Irr}(G)} \chi(g)\chi(1) = \sum_{\substack{\chi\in\mathrm{Irr}(G)\\ \chi(1)=1}} \chi(g) + \sum_{\substack{\chi\in\mathrm{Irr}(G)\\ \chi(1)=m}} \chi(g)\chi(1) \\ &= \sum_{\substack{\chi\in\mathrm{Irr}(G)\\ \chi(1)=1}} \chi(g) + m \sum_{\substack{\chi\in\mathrm{Irr}(G)\\ \chi(1)=m}} \chi(g). \end{aligned}$$

Now, noting from [14, Corollary 2.23] that the number of irreducible linear characters is $|G : G'|$, and from [14, Lemma 2.19] that if χ is linear, then $\chi(g) = \chi(1)$ since $G' \leq \ker\chi$, we obtain

$$0 = |G : G'| + m \sum_{\substack{\chi\in\mathrm{Irr}(G)\\ \chi(1)=m}} \chi(g).$$

Therefore,

$$\sum_{\substack{\chi\in\mathrm{Irr}(G)\\ \chi(1)=m}} \chi(g) = -\frac{|G : G'|}{m}.$$

Next, as $N^{\chi}_{w_\ell} = (N_{w_\ell}, \chi) = \big(\frac{|G|}{\chi(1)}\big)^{2\ell-1}$ for any $\chi \in \mathrm{Irr}(G)$ by [24, Theorem 1], we have

$$\begin{aligned}
N_{w_\ell}(g) &= \sum_{\chi\in\mathrm{Irr}(G)} \Big(\frac{|G|}{\chi(1)}\Big)^{2\ell-1} \cdot \chi(g)\\
&= \sum_{\substack{\chi\in\mathrm{Irr}(G)\\ \chi(1)=1}} |G|^{2\ell-1} + \sum_{\substack{\chi\in\mathrm{Irr}(G)\\ \chi(1)=m}} \Big(\frac{|G|}{m}\Big)^{2\ell-1} \cdot \chi(g)\\
&= |G|^{2\ell-1}\cdot |G : G'| + \Big(\frac{|G|}{m}\Big)^{2\ell-1} \cdot \Big(\frac{-|G : G'|}{m}\Big)\\
&= \frac{|G|^{2\ell}}{|G'|}\cdot \Big(1 - \frac{1}{m^{2\ell}}\Big),
\end{aligned}$$

hence the first result. For the final statement, we note that since $m \geq 2$, we have

$$\Big(1 - \frac{1}{m^{2\ell}}\Big) \geq \frac{3}{4}\ .$$

Consequently, all elements in G' appear as images of w_ℓ; so $G' = G_{w_\ell}$. What is more, since G is non-abelian, we have $|G : G'| \geq 2$ and hence the lower bound is proved for the fibres. □

Proof of Theorem C. By Theorem 3.1, it remains to prove that $N_{w_\ell}(1) \geq |G|^{2\ell-1}$ and that $N_{w_\ell}(1) \neq N_{w_\ell}(g)$ for $1 \neq g \in G'$. For the first part, note that

$$N_{w_\ell}(1) + \sum_{1\neq g\in G'} N_{w_\ell}(g) = \sum_{g\in G'} N_{w_\ell}(g) = |G|^{2\ell}. \tag{3}$$

Since we showed in Theorem 3.1 that $G' = G_{w_\ell}$, it follows from the previous result that for $1 \neq g \in G'$,

$$N_{w_\ell}(g) = \frac{|G|^{2\ell}}{|G'|}\Big(1 - \frac{1}{m^{2\ell}}\Big) < \frac{|G|^{2\ell}}{|G'|}$$

and hence $N_{w_\ell}(1) > \frac{|G|^{2\ell}}{|G'|} > |G|^{2\ell-1}$ using (3).

In particular, we note that $N_{w_\ell}(1) > \frac{|G|^{2\ell}}{|G'|} > N_{w_\ell}(g)$ for $1 \neq g \in G'$, proving there exist exactly two fibre sizes. □

Proof of Corollary D. For $g = 1$, the result is true by [13,15]. We claim that a non-linear irreducible character χ vanishes outside of the centre Z of G. Consider $g \in G\backslash Z$. So there exists some $x \in G$ such that $t = [g, x] \neq 1$. Since $|G'| = p$, the element t is a generator of G'. If we now consider a complex representation ρ affording χ, we have that $\rho(t) = \epsilon I$ where $\epsilon \in \mathbb{C}$ by [14, Lemma 2.25]. In the case $\epsilon = 1$, we have $t \in \ker\rho$ and therefore $G' \leq \ker\rho$ which is a contradiction to χ being non-linear; compare [14, Lemma 2.22]. Therefore $\epsilon \neq 1$ and since

$$\chi(g) = \chi(g^x) = \chi(gt) = \mathrm{tr}_\rho(gt) = \mathrm{tr}(\rho(g)\rho(t)) = \mathrm{tr}(\epsilon\rho(g)I) = \epsilon\,\chi(g),$$

we conclude that $\chi(g) = 0$, and the claim holds. From [14, Corollary 2.28 and Lemma 2.29], we deduce that $\chi(1)^2 = |G : Z|$. Therefore G is a group of central type with just two irreducible complex character degrees, i.e., $\mathrm{cd}(G) = \{1, |G : Z|^{1/2}\}$. Now the assertion holds using the previous theorem. □

4. Rationality and chirality. In this section, we draw together some definitions and ideas that have appeared in the literature and conclude with a corollary which, although is a direct consequence of the results of [13], has not previously been explicitly stated and we believe is of interest.

According to [5], a pair (G, w), where G is a group and w is a word, is called *chiral* if $G_w \neq G_w^{-1}$. The group G is called *chiral* if (G, w) is chiral for some w. Otherwise G is *achiral*. In [5], the authors comment that the existence of chiral groups follows from a result of Lubotzky [16]. They then began the process of classifying all finite chiral groups. In particular, they found all chiral groups of order less than 108; there are two of them. These results negatively answer a question posed by Ashurst in her thesis [4, Question 5]: If G is a finite group, $g \in G$, and $w \in F_\infty$, is it necessarily true that $P(G, w = g) = P(G, w = g^{-1})$?

Related to the definition of achiral is the definition of weakly rational. According to [11], a word w is *rational* if for every finite group G and any $g \in G$, we have $N_w(g) = N_w(g^e)$ for every e relatively prime to $|G|$. Additionally, a word w is *weakly rational* if and only if for every finite group G and for every integer e relatively prime to $|G|$, the set G_w is closed under e-th powers. Clearly rational implies weakly rational; see [11] for more discussion.

We change the emphasis of the definition and say a pair (G, w) for G a group and w a word is *rational* if for all $g \in G$ and for every e relatively prime to $|G|$, we have $N_w(g) = N_w(g^e)$. A group G is *rational* if (G, w) is rational for all words w. Similarly we define a pair (G, w) to be *weakly rational* if for every e relatively prime to $|G|$, the set G_w is closed under e-th powers. A group G is *weakly rational* if (G, w) is weakly rational for all pairs (G, w) running over all words w. Clearly if G is rational, it is weakly rational and if it is weakly rational, it is achiral.

In [2] and [13], the authors show that the pair (G, w) is rational if and only if N_w is a generalized character of G.

Lemma 4.1 ([2, Corollary 3.3] and [13, Lemma 3.1]). *Let G be a group and w a word. Then $N_w = N_{w,G}$ is a generalized character of G if and only if $N_w(g) = N_w(g^e)$ for any $g \in G$ and e relatively prime to the order of G.*

In particular, in [13], they showed this is exactly what happens for any word w and any finite group of nilpotency class 2.

Theorem 4.2 ([13, Theorem 3.2]). *Let G be a p-group of nilpotency class 2 and w a word. Then $N_w = N_{w,G}$ is a generalized character of G.*

We include these results here to highlight the following corollary which is a partial improvement on [5, Theorem 5.2] which says that all class 2, rank 3, nilpotent groups are achiral.

Corollary 4.3. *Every finite group G of nilpotency class 2 is rational.*

Proof. First note that an abelian group is rational, and by Lemma 4.1 and Theorem 4.2, a p-group of nilpotency class 2 is rational. It follows for finite nilpotent groups of class 2 using the comment before Theorem A. □

Acknowledgements. We thank Dan Segal for many useful conversations, and we thank Benjamin Klopsch and the referee for suggesting several improvements to the exposition of the paper. The first author would like to thank the Isaac Newton Trust for supporting her sabbatical during which some of this research took place. The second and third authors thank the Department of Pure Mathematics and Mathematical Statistics of the University of Cambridge, and the third author also thanks Fitzwilliam and Homerton Colleges for supporting several research visits to Cambridge.

References

[1] Abért, M.: On the probability of satisfying a word in a group. J. Group Theory **9**, 685–694 (2006)

[2] Amit, A., Vishne, U.: Characters and solutions to equations in finite groups. J. Algebra Appl. **10**(4), 675–686 (2011)

[3] Antolín, Y., Martino, A., Ventura, E.: Degree of commutativity of infinite groups. Proc. Amer. Math. Soc. **145**, 479–485 (2017)

[4] Ashurst, C.: Fibres of words in finite groups, a probabilistic approach. Ph.D. Thesis, University of Bath (2012)

[5] Cocke, W., Ho, M.-C.: On the symmetry of images of word maps in groups. Comm. Algebra **46**(2), 756–763 (2018)

[6] Cocke, W., Ho, M.-C.: The probability distribution of word maps on finite groups. J. Algebra **518**, 440–452 (2019)

[7] Das, A.K., Nath, R.K.: On generalized commutativity degree of a finite group. Rocky Mountain J. Math. **41**(6), 1987–2000 (2011)

[8] Delizia, C., Jezernik, U., Moravec, P., Nicotera, C.: Gaps in probabilities of satisfying some commutator-like identities. Israel J. Math. **237**, 115–140 (2020)

[9] Erdös, P., Turán, P.: On some problems of a statistical group-theory IV. Acta Math. Acad. Sci. Hungar. **19**, 413–435 (1967)

[10] Garion, S., Shalev, A.: Commutator maps, measure preservation, and T-systems. Trans. Amer. Math. Soc. **361**(9), 4631–4651 (2009)

[11] Guralnick, R., Shumyatsky, P.: On rational and concise words. J. Algebra **429**, 213–217 (2015)

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

[13] Iñiguez, A., Sangroniz, J.: Words and characters in finite p-groups. J. Algebra **485**, 230–246 (2017)

[14] Isaacs, I.M.: Character Theory of Finite Groups. Dover, New York (1994)

[15] Levy, M.: On the probability of satisfying a word in nilpotent groups of class 2. arXiv:1101.4286 (2011)

[16] Lubotzky, A.: Images of word maps in finite simple groups. Glasg. Math. J. **56**(2), 465–469 (2014)

[17] Naik, T.K.: On the probability distribution associated to commutator word map in finite groups. Comm. Algebra **27**(9), 3808–3817 (2019)

[18] Nath, R.K., Yadav, M.K.: On the probability distribution associated to commutator word map in finite groups. Int. J. Algebra Comput. **25**, 1107–1124 (2015)

[19] Nath, R.K., Prajapati, S.K.: On the number of solutions of a generalized commutator equation in finite groups. Acta Math. Hungar. **156**(1), 18–37 (2018)

[20] Nikolov, N., Segal, D.: A characterization of finite soluble groups. Bull. Lond. Math. Soc. **39**, 209–213 (2007)

[21] Pournaki, M.R., Sobhani, R.: Probability that the commutator of two group elements is equal to a given element. J. Pure Appl. Algebra **212**(4), 727–734 (2008)

[22] Rusin, D.J.: What is the probability that two elements of a finite group commute? Pac. J. Math. **82**(1), 237–247 (1979)

[23] Solomon, L.: The solution of equations in groups. Arch. Math. (Basel) **20**, 241–247 (1969)

[24] Tambour, T.: The number of solutions of some equations in finite groups and a new proof of Itô's theorem. Comm. Algebra **28**, 5353–5361 (2000)

Rachel D. Camina
Fitzwilliam College
Cambridge CB3 0DG
UK
e-mail: rdc26@dpmms.cam.ac.uk

Ainhoa Iñiguez
Faculty of Gastronomic Sciences
University of Mondragon
Donostia-San Sebastián
Spain
e-mail: ainiguez@bculinary.com

Anitha Thillaisundaram
School of Mathematics and Physics
University of Lincoln
Brayford Pool
Lincoln LN6 7TS
UK
e-mail: anitha.t@cantab.net

Received: 14 May 2020