Word fibres in finite p-groups and pro-p groups

Ainhoa Iñiguez Goizueta

Mansfield College

University of Oxford

A thesis submitted for the degree of

Doctor of Philosophy

Hilary 2016

Acknowledgements

First of all I would like to thank my supervisor Dan Segal for this opportunity and for supporting me after the different decisions I made during these years. He has introduced me to a number of fascinating topics such as words and profinite groups that I will also continue working on in the future. I would also like to thank Rachel Camina on the role as my co-supervisor for her support and help after I returned back to continue with my thesis in 2013. Thanks to the University of Cambridge and to family Haines for providing the possibility to work at Cambridge for several periods between 2013-2015. I can't forget to thank the members of GRECA with whom I had very interesting discussions on my thesis either. Gustavo Fernandez for all his support from the very beginning and to Josu Sangroniz for his collaboration in part of this thesis. Neither to say to Andrei Jaikin who I thank for the stay in Madrid and other mathematica discussions.

This project would not have been possible without the financial support provided by Eusko Jaurlaritza, GRECA, Oxford Mathematical Institute and Mrs. Haines.

Finally, I wish to thank my family and friends for their constant support in the easy and difficult times during these years. Particularly my mum, who has always been there for me supporting me through all my decisions. This is for you.

Word fibres in finite p-groups and pro-p groups

Ainhoa Iñiguez Goizueta

Mansfield College

University of Oxford

A thesis submitted for the degree of

Doctor of Philosophy

Hilary 2016

Given a group word w in k variables, a group G and $g \in G$, we consider the set $S_w(g)$ of k-tuples $(g_1, \dots, g_k) \in G^{(k)}$ such that $w(g_1, \dots, g_k) = g$ and when G is finite, the size of $S_w(g)$, $N_w(g)$. N. Amit conjectured that for any finite nilpotent group G and any word in k variables, $N_w(1) \geq |G|^{k-1}$. In this thesis we first prove Amit's conjecture for finite groups of nilpotency class 2. This was independently proved by Levy in [1]. More generally, we study the class functions N_w for this class of groups and show that the inequality can be improved to $N_w(1) \geq |G|^k/|G_w|$ (G_w is the set of w-values in G) if G has odd order. This last result is explained by the fact that the functions N_w are characters of G in this case. For groups of even order, all that can be said is that N_w is a generalized character, something that is false in general for groups of nilpotency class greater than 2. We characterize group theoretically when N_{x^n} is a character if G is a 2-group of nilpotency class 2. We also address the (much harder) problem of studying if $N_w(g) \geq |G|^{k-1}$ for $g \in G_w$, proving that this is the case for the free p-groups of nilpotency class 2 and exponent p.

Finally, we look at the analogous problem for finitely generated pro-p groups. Let G be a finitely generated pro-p group and $\{G_n\}$ some filtration. We define the dimension of a closed subset $H \subseteq G$ as

$$\mathrm{Dim}_{\{G_n\}}(H) = \liminf_{n\to\infty} \frac{\log_p |HG_n^{(k)}/G_n^{(k)}|}{\log_p |(G/G_n)^{(k)}|}.$$

In this setting, a rather natural way to define the metric is by using the filtration $G_n = G^{p^n} = \langle x^{p^n} : x \in G \rangle$. For this filtration, we ask whether for any word w in k variables, $\mathrm{Dim}_{\{G_n\}} S_w(1) \geq k - 1/k$. We show that for free pro-p groups, using the filtration given by its dimension subgroups, this is not true in general.

Contents

Chapter 0

Preliminaries

0.1 Words and fibres

A *word* w is an expression of the form

$$w(x_1, \ldots, x_k) = \prod_{j=1}^{s} x_{i_j}^{\epsilon_j}$$

for some $s < \infty$ with $i_j \in \{1, \ldots, k\}$ and $\epsilon_j = \pm 1$ for each j. The corresponding *verbal mapping* on a group G is $f_w : G^{(k)} \mapsto G$ defined by evaluating w, so

$$f_w(g_1, \ldots, g_k) = w(g_1, \ldots, g_k) = \prod_{j=1}^{s} g_{i_j}^{\epsilon_j}.$$

Equivalently, there exists a unique homomorphism $\pi_{(g_1,\ldots,g_k)} : F_k \mapsto G$, where F_k is the free group on $\{x_1, \ldots, x_k\}$, sending x_i to g_i $(i = 1, \ldots, k)$ such that $f_w(g_1, \ldots, g_k) = \pi_{(g_1,\ldots,g_k)} w$.

It is sometimes convenient to identify a word with an element of F_k. Different words may represent the same element of F_k, but of course they all induce the same verbal mapping (see [2]).

For a subset $S \subseteq G$ and $m \in \mathbb{N}$ we write $S^{*m} = \{s_1 s_2 \cdots s_m \,|\, s_i \in S\}$. We write $G_w = \{w(g_1, \ldots, g_k) \,|\, (g_1, \ldots, g_k) \in G^{(k)}\}$ the set of w-values in G. Note that gener-

ally G_w is a proper subset of G. We define the *verbal subgroup* corresponding to G to be $w(G) = \langle G_w \rangle$, the group generated by G_w. We say that the word w has *width* m in G if $w(G) = G_w^{*m}$ and m is the smallest value with this property. If there is no such $m < \infty$, then we say that w has infinite width in G.

For a word w in k variables and a group G, for any $g \in G$ we denote by S_w the function defined by

$$S_w(g) = \{(g_1, \ldots, g_k) \in G^{(k)} \mid w(g_1, \ldots, g_k) = g\}, \tag{0.1}$$

the *fibre* of g in $G^{(k)}$. If G is a finite group, we define N_w to be the function defined by

$$N_w(g) = |S_w(g)| = \sharp\{(g_1, \ldots, g_k) \in G^{(k)} \mid w(g_1, \ldots, g_k) = g\}; \tag{0.2}$$

i.e. the size of the fibre of g in $G^{(k)}$. We also define the function P_w to be defined by

$$P_w(g) = \frac{N_w(g)}{|G|^k}.$$

Note P_w only depends on the word w and not on the number of variables of w, so we can assume $w \in F_\infty$. We will write $P_{w,G}(g)$ when it is important to emphasize the group G (equivalently $N_{w,G}(g)$ when necessary).

0.2 Regular p-groups

Definition 1. We say a p-group is regular if for every $x, y \in G$, $x^p y^p = (xy)^p c^p$ for some $c \in \langle x, y \rangle'$.

The condition in the definition of a regular p-group is local, since it only involves the subgroup generated by x and y. Hence all subgroups and quotient groups of regular p-groups are again regular. All abelian p-groups and all groups of exponent p are regular. The theory of regular p-groups is almost fully developed in P. Hall's fundamental paper on p-groups [3]. For any finite p-group G, if the nilpotency class of G is less than p then G is regular. In particular, any p-group of order at most p^p is regular.

For any finite p-group G and any $r \geq 0$, we define the characteristic subgroups of G, $\Omega_r(G) = \langle x \in G \mid x^{p^r} = 1 \rangle$ and $\mho_r(G) = \langle x^{p^r} \mid x \in G \rangle$. If G is regular a p-group,

then $\Omega_r(G) = \{x \in G \,|\, x^{p^r} = 1\}$, $\mho_r(G) = \{x^{p^r} \,|\, x \in G\}$ and $|G : \Omega_r(G)| = |\mho_r(G)|$ for any $r \geq 0$. See Section 3.2 in [4] for more details on regular p-groups.

0.3 Amalgamated central product of groups

Free products of groups are generalized by a notion of amalgamated central products of groups joined together along specified subgroups. We introduce Definition 1.3.16 of [5] for the specific case that we will use in Chapter 3.

Definition 2. Let T and H be 2-groups with cyclic center and $|Z(T)| \leq |Z(H)|$. For any injective homomorphism $\theta : Z(T) \mapsto Z(H)$,

$$Z = \{(z^{-1}, \theta(z)) \,|\, z \in Z(T)\}$$

is a subgroup of $Z(T \times H)$ in $T \times H$. The factor group $T * H = (T \times H)/Z$ is a central product of T and H with $Z(T)$ amalgamated with the corresponding subgroup of $Z(H)$.

Lemma 3. *If all the generators of $Z(T)$ are in the same orbit under the action of the automorphism group of T (or if a similar situation holds in H), the group $T * H$ is unique up to isomorphism.*

Proof. From Definition 2, $(T \times H)/Z$ is a central product of T and H with $Z(T)$ amalgamated with the corresponding subgroup of $Z(H)$ such that Z is defined by some injective homomorphism $\theta : Z(T) \mapsto Z(H)$.

Suppose that z_1 and z_2 are two genetarors of $Z(T)$. By hypothesis, there exists some $\tau \in \mathrm{Aut}(T)$ such that $z_1 = \tau(z_2)$. Consequently, $\tau \times id_H \in \mathrm{Aut}(T \times H)$ and for $(z_2^{-1}, \theta(z_2)) \in Z$, one gets

$$(\tau \times id_H)(z_2^{-1}, \theta(z_2)) = (\tau(z_2^{-1}), \theta(z_2)) = (z_1^{-1}, \theta(z_2)) = (z_1^{-1}, (\theta \circ \tau^{-1})(z_1)).$$

If we write $\tilde{\theta} = \theta \circ \tau^{-1}_{|Z(T)}$, $\tau \times id_H$ maps Z to $\tilde{Z}$ which is defined exactly as Z only by replacing θ with $\tilde{\theta}$. As a consequence, this induces an isomorphism between the amalgamated central products $(T \times H)/Z$ and $(T \times H)/\tilde{Z}$.

□

The hypothesis in Lemma 3, is satisfied if $T = \mathcal{D}_{2^{3r}}$ or $T\mathcal{Q}_{2^{3r}}$, and hence we will say that $T * H$ is the central product of T and H with amalgamated $Z(T)$.

0.4 Pro-p groups

A pro-p group is obtained when you look at a (suitably coherent) collection of finite p-groups all at once. 'Coherent' means that the groups in question form an inverse system; that is, a family of finite groups $\{G_\lambda\}$ indexed by a directed set Λ, and for each pair $\alpha, \beta \in \Lambda$ with $\alpha \leq \beta$ a homomorphism $\theta_{\beta\alpha} : G_\beta \to G_\alpha$. Whenever $\alpha \leq \beta \leq \gamma$ it is required that $\theta_{\beta\alpha} \circ \theta_{\gamma\beta} = \theta_{\gamma\alpha}$, and each $\theta_{\alpha\alpha}$ is the identity automorphism. To say that Λ is a directed set means that Λ is partially ordered and that for every $\alpha, \beta \in \Lambda$ there exists $\gamma \in \Lambda$ with $\gamma \geq \alpha$ and $\gamma \geq \beta$. The *inverse limit* of this system, denoted by

$$G = \varprojlim_{\lambda \in \Lambda} G_\lambda,$$

may be defined by a suitable universal property, or more concretely as a subgroup G of the Cartesian product of all the G_λ, as follows:

$$G = \{(g_\lambda) \,|\, \theta_{\beta\alpha}(g_\beta) = g_\alpha \text{ whenever } \beta \geq \alpha\} \leq \prod_{\lambda \in \Lambda} G_\lambda.$$

Thus G maps naturally into each of the finite groups G_λ (by projecting to a factor), and G is completely determined by the system $\{G_\lambda\}_{\lambda \in \Lambda}$ such that the homomorphisms $\theta_{\beta\alpha}$ are supposed to be included as part of the definition of the system. In a natural way, G is a topological group. Giving each of the finite groups G_λ the discrete topology, we endow $\prod_{\lambda \in \Lambda} G_\lambda$ with the product topology; instead of being discrete, this is a compact Hausdorff space, by Tychonoff's Theorem. It is easy to see that the inverse limit G is a closed subgroup, so in this way G becomes a compact Hausdorff topological group. For each $\lambda \in \Lambda$ the kernel K_λ of the projection $\pi_\lambda : G \to G_\lambda$ is an open normal subgroup of G, and the family $\{K_\lambda\}$ forms a base for the neighbourhoods of 1 in G. In most naturally-arising situations, the maps $\theta_{\beta\alpha}$ are all surjective, in which case one speaks of a surjective inverse system.

A pro-p group is said to be *countably based* if G is the inverse limit of an inverse system of finite groups indexed by $\mathbb{N}$. It is easy to see that every finitely generated

pro-p group is countably based, and that a countably based group is topologically generated by a countable set.

A pro-p group G has *rank* $r = \mathrm{rk}(G)$ if every closed subgroup of G can be generated (topologically) by r elements, and r is minimal with this property. The word 'rank' is also used in a different sense in the context of free profinite (or pro-p) groups; tradition insists that a 'free group of rank r' means a group having a free generating set of cardinality r. Since a non-abelian free profinite (or pro-p) group necessarily has infinite rank in the first sense, it will be clear from the context which usage is in force.

0.5 Hausdorff dimension

Suppose we have a subgroup H of a finite group G, and that we want to measure the relative size of H with respect to G. We can use the quotient $|H|/|G|$, or if G is a p-group even better $\log_p |H| / \log_p |G|$. If $|G| = p^a$ and $|H| = p^b$, then the number $|H|/|G| = p^{b-a}$ may hide the size relation between H and G for high values of p. That is why we are more interested in knowing the relation between a and b and why we consider $\log_p |H| / \log_p |G| = b/a$ instead.

If G is infinite, the first problem is that both $|H|/|G|$ and $\log_p |H| / \log_p |G|$ are meaningless. We can rewrite $|H|/|G|$ as $1/|G : H|$ and interpret $1/\infty$ as 0, and make this choice for the dimension of H in G. However, it will not distinguish subgroups of infinite index, and, intuitively, a subgroup of finite index of an infinite group should have dimension 1. On the other hand, the alternative of $\log_p |H| / \log_p |G|$ does not even allow a direct reinterpretation in the infinite setting.

Abercrombie proposed a way to overcome this situation in the case of profinite groups, using the concept of *Hausdorff dimension* over a metric space. Suppose that G is a countably based pro-p group such that $\{U_n\}_{n\in\mathbb{N}}$ is a descending chain of open normal subgroups which form a base of neighbourhoods of the identity. Since $|G| = \infty$, there is a natural metric in G, induced by $\{U_n\}$:

$$d(x, y) = \inf\{|G : U_n|^{-1} \mid xy^{-1} \in U_n\}.$$

This gives G the structure of a metric space and therefore we can compute the Hausdorff dimension of a subset of G with respect to this metric. Note that the topology defined by this metric coincides with the original topology of G.

There is a nice formula due to Abercrombie [6] and Barnea-Shalev [7] that provides the Hausdorff dimension of an arbitrary closed subgroup H of G. Note that it is given in purely algebraic (and analytic) terms.

Theorem 4 ([7]). *Let G be a finitely generated pro-p group with a filtration $\{G_n\}_{n\in\mathbb{N}}$ and let $H \leq_c G$ be a closed subgroup. Then*

$$\mathrm{hdim}_{\{G_n\}}(H) = \liminf_{n\to\infty} \frac{\log_p |HG_n/G_n|}{\log_p |G/G_n|} = \liminf_{n\to\infty} \frac{\log_p |H : H\cap G_n|}{\log_p |G/G_n|}.$$

Observe the similarity with the finite case. The finite quotients G/G_n give approximations of the group G, which are better as n increases. In the formula above, we project H in these finite quotients and compute its relative size inside them, which is the quotient $\log_p |HG_n/G_n|$. Finally, we take the $\log_p |G/G_n|$ limit when $n \to \infty$ to see the asymptotic behaviour of these numbers (the lim inf is necessary since the limit need not exist).

Note that the Hausdorff dimension of a closed subgroup of G depends on the filtration $\{G_n\}$ used to define the metric of G, and there are examples showing that this is so (see [7], Example 2.5). In any case, there is usually a natural choice for the system of neighbourhoods of the identity. For example, for a general finitely generated pro-p group, we can take $G_n = G^{p^n}$ whereas in the case of free pro-p groups we would generally consider the dimension subgroups D_n (see Chapter 11 in [8]).

For a finitely generated pro-p group G and any word w in k variables, we want to measure somehow the sizes of the closed sets $S_w(1)$ with respect to some filtration $\{G_n\}_{n\in\mathbb{N}}$ of G. Using what we learnt about the Hausdorff dimension, we define the dimension of a closed set H of a finitely generated pro-p group G with a filtration $\{G_n\}$, as follows:

$$\mathrm{Dim}_{\{G_n\}}(H) = \liminf_{n\to\infty} \frac{\log_p |H_{\pi_n}|}{\log_p |G_{\pi_n}|} = \liminf_{n\to\infty} \frac{\log_p |HG_n/G_n|}{\log_p |G/G_n|}$$

$$= \liminf_{n\to\infty} \frac{\log_p |H : H \cap G_n|}{\log_p |G/G_n|}, \tag{0.3}$$

where X_{π_n} is the image of X under the natural quotient map $\pi_n : G \to G/G_n$ for any $X \subseteq G$. Similarly, for any subset Y of $G^{(k)}$, $Y_{\pi_n^{(k)}}$ is the image of Y under $\pi_n^{(k)}$. A natural way to define a filtration in $G^{(k)}$ is by $\{G_n^{(k)}\}$. Hence, for any word w in k variables and G a finitely generated pro-p group with the filtration $\{G_n\}$, we define

$$\begin{aligned} \mathrm{Dim}_{\{G_n\}} S_w(1) &= \liminf_{n\to\infty} \frac{\log_p |S_w(1)_{\pi_n^{(k)}}|}{\log_p |G^{(k)}_{\pi_n^{(k)}}|} = \liminf_{n\to\infty} \frac{\log_p |S_w(1) G_n^{(k)}/G_n^{(k)}|}{\log_p |(G/G_n)^{(k)}|} \\ &= \liminf_{n\to\infty} \frac{\log_p |S_w(1) : S_w(1) \cap G_n^{(k)}|}{\log_p |(G/G_n)^{(k)}|}. \end{aligned} \tag{0.4}$$

Considering the natural filtration $G_n = G^{p^n} = \langle x^{p^n} : x \in G \rangle$ for a finitely generated pro-p group G, we will study whether

$$\mathrm{Dim}_{\{G_n\}} S_w(1) \geq k - 1/k$$

holds.

Chapter 1

Introduction

The number of solutions of equations over finite fields has been an important problem in number theory since Gauss. Since then it has been studied particularly intensively in the 20th century, the proof of the Weil conjectures being a highlight. This project intends to be a beginning of such a study in a non-commutative setting. The point of restricting to p-groups is that these are 'close to commutative', and so one may hope for analogues of more classical results.

In Chapter 1 we will introduce some background on word fibres in finite group theory. For a group we can ask what happens when we multiply elements together. If we want to make this sound more like mathematics, we can rephrase it as a series of questions about verbal mappings. Let F_k be the free group on $x_1, \ldots, x_k$. Then for a word $w \in F_k$ some will want to describe the fibres and the image of the corresponding verbal mapping $f = f_w$; others will want to know how big they are. Both kinds of question are easily answered when f happens to be a homomorphism (the group theorist's comfort zone). However, verbal mappings are not usually homomorphisms, unless G is an abelian group.

Given a group G, the focus here will be to study the fibres $S_w(g)$, for $g \in G_w$. If G is abelian, $f_w : G^{(k)} \to G$ is a homomorphism and hence each non-empty fibre $S_w(g)$ is a coset of the kernel $S_w(1)$. Using (0.2), for a finite abelian group G and any $g \in G_w$, $N_w(g) \geq |G|^k/|G| = |G|^{k-1}$. This can be expressed in a more invariant way by using the function P_w. In the case of a finite abelian group G and any $g \in G_w$,

then we have that $P_w(g) \geq 1/|G|$, and for all the elements $g \in G_w$,

$$P_w(g) = |S_w(1)|/|G|^k;$$

i.e. they have the same probability that a random tuble satisfies $w(g_1, \ldots, g_k) = g$.

The probabilities $P_w(1)$ have been studied in the literature mainly for a fixed word w and moving G, a strong result in this direction being that of Dixon, Pyber, Seress and Shalev in [9] who proved that for any non-trivial word $w \in F_\infty$, $P_w(1)$ tends to 0 with the order of the group, assuming that G is a non-abelian simple group. In the other direction, by fixing a group G and letting w range over all words, Amit showed in [10] that if G is a finite nilpotent group, there exists a constant $c > 0$ depending only on G such that for all $w \in F_\infty$, $P_w(1) > c$. He also conjectured that the same holds for finite solvable groups and for nilpotent groups he conjectured the following:

Conjecture 1. *Let G be a finite nilpotent group. Then for any w in k variables,*

$$N_w(1) \geq |G|^{k-1}; \tag{1.1}$$

or equivalently,

$$P_w(1) \geq 1/|G|. \tag{1.2}$$

He also asked if in turn, for a non-solvable finite group G, $P_w(1)$ could be made arbitrarily small for a suitable $w \in F_\infty$. Abért gave a positive answer to the last question in [11] showing something stronger; that if G is a finite just non-solvable group; i.e. every proper quotient of G is solvable but G itself is not, the set $\{P_w(1) \mid w \in F_\infty\}$ is dense in $[0, 1]$. On the other hand, Nikolov and Segal gave in [12] a characterization of finite solvable and nilpotent groups in terms of these probabilities:

Theorem 5 ([12])**.** *Let G be a finite group and let $\epsilon(G) = p^{-|G|}$ where p is the largest prime dividing $|G|$.*

(i) G is solvable if and only if $\inf_w P_w(1) > \epsilon(G)$, when w ranges over all words in F_∞.

(ii) G is nilpotent if and only if $\inf_{w,g} P_w(g) > \epsilon(G)$, when w ranges over all words in F_∞ and $g \in G_w$.

However, this bound $\epsilon(G)$ is far from what Amit conjectured for nilpotent groups. Their approach was to interpret the verbal mapping f_w as a polynomial mapping over a finite field. The 'co-ordinatization' used to achieve this is quite crude and probably loses a lot of information.

For example note that if G is non-nilpotent and $\gamma_k = [\dots[[[x_1, x_2], x_3], x_4], \dots, x_k]$ is the left-normed repeated commutator, then $\gamma_k(G) \neq 1$ for every k. Hence for each k there exists some non-trivial $h_k \in G_{\gamma_k}$. Since $\gamma_k(g_1, \dots, g_k) = 1$ if $g_i = 1$ for some i, then

$$\frac{1}{|G|^k} \leq P_{\gamma_k}(h_k) \leq \frac{(|G|-1)^k}{|G|^k} \underset{k \longrightarrow \infty}{\longrightarrow} 0. \tag{1.3}$$

Thus in the non-nilpotent case, $P_w(h)$ takes arbitrarily small positive values as w varies over all words.

In Chapters 2-5 we want to show some positive results towards Amit's conjecture. Amit conjectured that $N_w(1) \geq |G|^{k-1}$ for any finite nilpotent group G and any word w in k variables. We will use character theoretical arguments and general group theoretical arguments to tackle this problem in the case of p-groups of nilpotency class 2. We could expect that these groups, being so close to commutative, may behave not so differently to abelian groups when analysing word fibres; and they do. In this setting, we will consider the same question for general fibres and using basic linear algebra, we will give some positive results towards proving Amit's bound for the general fibres for p-groups of nilpotency class 2.

Hence we start by proving the following theorem:

Theorem A. *Let G be a finite group of nilpotency class 2 and let $w \in F_k$. Then $N_w(1) \geq |G|^{k-1}$.*

This result was independently proved by Levy in [1] using a similar procedure, although our approach to the concept of word equivalence is different.

To begin with, in Chapter 2 we will be looking for a set of representatives for words in this class of groups. For convenience, we will consider a word in the variables $x_1, \dots, x_k$ as an element in F_k, the free pro-p group of nilpotency class 2. Thus, if

$w \in F_k$ is a word, it can be represented in a unique way as

$$w = x_1^{z_1} \cdots x_k^{z_k} \prod_{1 \le i < j \le k} [x_i, x_j]^{z_{ij}},$$

where the exponents z_l, z_{ij} are p-adic integers. Two words $w, w' \in F_k$ will be *equivalent* if they belong to the same orbit under the action of the automorphism group of F_k and hence our next goal will be to find a set of representatives of the equivalence classes of words:

Theorem B. *The following words are a system of representatives of the action of* $\operatorname{Aut} F_k$ *on* F_k*:*

$$[x_1, x_2]^{p^{s_1}} [x_3, x_4]^{p^{s_2}} \cdots [x_{2r-1}, x_{2r}]^{p^{s_r}},\ 0 \le 2r \le k,\ 0 \le s_1 \le \cdots \le s_r, \quad (1.4)$$

$$x_1^{p^{s_1}} [x_1, x_2]^{p^{s_2}} [x_2, x_3]^{p^{s_3}} \cdots [x_{r-1}, x_r]^{p^{s_r}},\ 1 \le r \le k,\ 0 \le s_1,\ 0 \le s_2 \le \cdots \le s_r. \quad (1.5)$$

Since a finite nilpotent group is a direct product of its Sylow subgroups, it will suffice to show Theorem A for finite p-groups of nilpotency class 2 and any prime p. This is done in Theorem 10 using Theorem B strongly.

In Chapter 3 we study the functions N_w for the class of groups of nilpotency class 2. These results will lead to the conclusion that proving Amit's conjecture for this class of groups shouldn't have been surprising. We will start by showing the following theorem:

Theorem C. *Let* G *be a finite group of nilpotency class* 2 *and let* w *be a word in* k *variables. Then* N_w *is a generalized character of* G*.*

Recall that the class function N_w is a generalized character if $N_w^\chi \in \mathbb{Z}$ for any $\chi \in \operatorname{Irr}(G)$ where for any $g \in G$,

$$N_w(g) = \sum_{\chi \in \operatorname{Irr}(G)} N_w^\chi \cdot \chi(g),$$

and $N_w^\chi = (N_w, \chi)$ is the inner product. If $N_w^\chi \in \mathbb{N}$, we say N_w is a character and it is not hard to show that this is a sufficient condition to obtain Amit's bound,

$N_w(1) \geq |G|^{k-1}$. As a consequence, if N_w is a character,

$$N_w(1) \geq N_w(g) \tag{1.6}$$

for any $g \in G$. Conversely, if there exists some element $g \in G$ such that $N_w(g) > N_w(1)$, then N_w is not a character. In this direction, we prove the following result:

Theorem D. *Let G be a finite p-group of nilpotency class 2 such that p is odd and let w is a word in k variables. Then N_w is a character of G.*

In particular we obtain an improvement of Theorem A, namely, $N_w(1) \geq |G|^k/|G_w|$.

For 2-groups, there are easy examples where N_{x^2} fails to be a character one of them being the quaternion group $\mathcal{Q}_8$ of order 8. Note that $G = \mathcal{Q}_8$, $G_{x^2} = \{1, z\}$ where z is the unique involution. We note that $N_{x^2,G}(1) = 2$ whereas $N_{x^2,G}(z) = 6$ showing that N_w is not a character. Generalising what happens with the quaternion group, we actually characterize group-theoretically when this happens for the power words $w = x^n$ (always within the class of 2-groups of nilpotency class 2). This technical section was done with the collaboration of J. Sangroniz.

In Section 0.3, we introduce the concept of central product $T * H$ with amalgamated $Z(T)$ for 2-groups T and H with cyclic center and $|Z(T)| \leq |Z(H)|$. Using this construction, we prove the following theorem:

Theorem E. *Let G be a finite 2-group of nilpotency class 2. Then $N_{x^{2^r}}$ is a character of G if and only if G has no epimorphic image isomorphic to $\mathcal{D}_{2^{3r_1}} * \cdots * \mathcal{D}_{2^{3r_n}} * \mathcal{Q}_{2^{3r}}$, $0 \leq n$, $r_1 \leq \ldots \leq r_n \leq r$ where*

$$\mathcal{D}_{2^{3r}} = \langle x, y, z \,|\, x^{2^r} = y^{2^r} = z^{2^r} = 1, [x, z] = [y, z] = 1, [x, y] = z \rangle,$$

$$\mathcal{Q}_{2^{3r}} = \langle x, y, z \,|\, x^{2^r} = y^{2^r} = z^{2^{r-1}}, z^{2^r} = 1, [x, z] = [y, z] = 1, [x, y] = z \rangle.$$

We call $\mathcal{D}_{2^{3r}}$ the quasi-dihedral group of order 2^{3r} and note that it can be constructed as $\mathcal{D}_{2^{3r}} = \langle x, z \rangle \rtimes \langle y \rangle$ where $\langle x, z \rangle \cong C_{2^r} \times C_{2^r}$, $\langle y \rangle \cong C_{2^r}$ (C_n denotes a cyclic group of order n) and $x^y = xz$ and $z^y = z$. That is, $\mathcal{D}_{2^{3r}}$ is isomorphic to the Heisenberg group over $\mathbb{Z}/2^r\mathbb{Z}$; i.e. the set of 3×3 upper unitriangular matrices with elements in $\mathbb{Z}/2^r\mathbb{Z}$. On the other hand, we call $\mathcal{Q}_{2^{3r}}$ the quasi-quaternion group of order 2^{3r} and can be constructed as $\langle x, z \rangle \rtimes \langle y \rangle / \langle (x^2 z^{-1})^{2^{r-1}} \rangle$ where $\langle x, z \rangle \cong C_{2^{r+1}} \times C_{2^r}$,

$\langle y\rangle \cong C_{2^r}$ and $x^y = xz$ and $z^y = z$. One can check that, $\mathcal{Q}_{2^{3r}} = \langle x, y, z\rangle$ can be seen as a finite quotient of the pro-2 group $\mathrm{GL}_4(\mathbb{Z}/2^r\mathbb{Z})$ generated by the matrices

$$x = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad y = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad z = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

In Chapter 4, after proving that N_w are characters for p-groups G of nilpotency class 2, we briefly consider the conjecture $N_w(g) \geq |G|^{k-1}$ for any words w in k variables and $g \in G_w$ for this class of groups. This problem is much harder than the case $g = 1$ and only some partial results have been obtained. For instance if we consider the word $w_k = [x_1, y_1]\cdots[x_k, y_k]$, the disjoint product of k commutators, we obtain the following result. Recall first that for a finite p-group, the Frattini subgroup of G is defined as $\Phi(G) = G^p[G, G]$ and it is the set of non-generating elements of G. We will write $Z(G)$ for the center of G.

Theorem F. *Let G be a d-generated p-group with $\Phi(G) \leq Z(G)$ and $|G'| = p^{d(d-1)/2}$. Then for any $g \in G_{w_k}$, $N_{w_k}(g) \geq |G|^{2k-1}$.*

As a corollary, we confirm the conjecture of the general fibres if G is a free nilpotent p-group of nilpotency class 2 and exponent p. In the same chapter, we also give some other bounds for $N_w(g)$ in this class of groups.

In Chapter 5, we will consider p-groups of nilpotency class higher than 2. By giving some examples, we will show that in general N_w will not be a generalized character for an arbitrary word w. To start with, for odd primes p we construct the smallest p-groups for which $N_{x^p,G}$ fails to be a character. Recall that in the case of $p = 2$, $\mathcal{Q}_8$ is the smallest group satisfying that N_{x^2} is not a character.

Let p any odd prime now. If G is regular, then N_{x^p} is the regular character of G/G^p. Consequently, in order to find groups for which N_{x^p} is not a character, we need to consider non-regular p-groups of order at least p^{p+1}. We construct next a non-regular p-group G of minimal order; that is, of order p^{p+1}, for which N_{x^p} is not a character. Note that a non-regular p-group of minimal order has nilpotency class p. See Section 0.2 for more details on regular groups.

Proposition G. *For any odd prime p, N_{x^p} is not a character of*

$$G = \langle g_1, \ldots, g_{p-1} \rangle \rtimes \langle g_p \rangle / \langle g_{p-1}^p g_p^{-p} \rangle$$

where $\langle g_1, \ldots, g_{p-1} \rangle \cong C_p \times \cdots \times C_p \times C_{p^2}$, $\langle g_p \rangle \cong C_{p^2}$ and $g_i^{g_p} = g_i g_{i+1}$, $1 \leq i < p-2$, $g_{p-2}^{g_p} = g_{p-2} g_{p-1}^p$ and $g_{p-1}^{g_p} = g_{p-1} g_1^{-1}$.

First note that $|G| = p^{p+1}$. Checking that $|G : \Omega(G)| \neq |\mho(G)|$, we show that G is non-regular and at the same time, we prove that $N_{x^p}(1) = p^{p-1}$, whereas $N_{x^p}(z) = p^p + p^{p-1}$ for any non-trivial element $z \in Z(G) = G_{x^p} = \langle g_p^p \rangle$.

For words w in more than one variable, there are examples of groups G and words w where $N_{w,G}$ is not a generalized character, even among nilpotent groups. We will discuss such examples below in Proposition H. As for non-solvable examples one can take $G = \mathrm{PSL}_2(11)$ and the 2-Engel word $w = [x, y, y]$ (see [13] for another choice of w). Using the computing system [14] one can check that the coefficients N_w^χ for the two irreducible characters χ of degree 12 are $305 \pm 23\sqrt{5}$. More examples can be obtained using the following result by A. Lubotzky [15]: if G is a simple group and $1 \in A \subseteq G$ is a subset invariant under the group of automorphisms of G, then $A = G_w$ for some word w in two variables. Notice that if A contains an element a such that $a^i \notin A$, for some i coprime with the order of a, then $N_w(a^i) = 0$ but $N_w(a) \neq 0$, something that cannot happen if N_w is a generalized character (see Corollary 13). This proof, while effective, does not give a useful description to build such a word w.

We will also see the connection to P. Hall's conjecture on conciseness here. A word w is called *concise* if whenever G_w is finite, it always follows that the verbal subgroup $w(G)$ is finite. P. Hall asked whether every word is concise:

Question 1 (P.Hall)**.** *Let G be a group and w a word in F_k. If $|G_w| < \infty$, is $|w(G)| < \infty$?*

S. Ivanov [16] answered this question for arbitrary groups in the negative. He constructed a group H and a word $w(x, y) \in F_2$ such that $w(H)$ is infinite cyclic, but $w(x, y)$ has only one non-trivial value in H. Ivanov's example is not residually finite. It is still an open problem whether every word is concise in the class of **residually finite groups**. Recall that G is a residually finite group if for any $g \in G$ there exists a homomorphism f from G to a finite group H such that $f(g) \neq 1$. Examples of groups

that are residually finite are finite groups, free groups and finitely generated nilpotent groups. Subgroups of residually finite groups are residually finite, and direct products of residually finite groups are residually finite. Any inverse limit of residually finite groups is residually finite. In particular, all profinite groups are residually finite.

Recall that a word w is *rational* if for any $g \in G$, $N_w(g) = N_w(g^e)$ for every finite group G and for every e relatively prime to $|G|$. Note that this means that N_w is a generalized character for any finite group G (see Corollary 13). We say the 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. It is observed in [17] that if w is a weakly-rational word and G is a residually finite group in which w has at most m values, then the order of $w(G)$ is m-bounded; i.e. w is concise in the class of residually finite groups.

Recall that pro-p groups are residually finite. If we assume that for any finite p-group and any word w the class function N_w is a generalised character, this would imply that any word is concise in the family of pro-p groups. Since this is unexpected, looking for finite p-groups for which N_w is not a generalised character makes sense.

Some examples of p-groups where N_w is not a generalized character are provided by the free p-groups of nilpotency class 4 and exponent p and settles in the negative a question of Parzanchevski [18] who asked whether the functions N_w were always generalized characters for solvable or nilpotent groups.

Proposition H. *Let G be the rank 2 free p-group of nilpotency class 4, exponent p with $p > 2$ and $p \equiv 1 \pmod 4$ and let $w = [x, y, x, y]$. Then N_w is not a generalized character of G.*

In Chapter 6 we will move to study fibres in pro-p groups. We want to study a similar conjecture to Amit's in this setting. If we wanted to deduce something about the finite p-groups, a good approach could be to try to understand the fibres in the inverse limit of p-groups; i.e pro-p groups. Or putting some hypothesis in the pro-p case, we would like to know how much we could deduce about the finite images. In order to state a similar conjecture to Amit's, we need a new 'tool' to measure the fibres and we will use a dimension (0.3) introduced in the Section 0.5. Hence we will study the following the question:

Question 2. *Let G be a finitely generated pro-p group with the filtration $\{G_n\} = \{G^{p^n}\}_{n\in\mathbb{N}}$ and let w be a word in k variables. Is*

$$\mathrm{Dim}_{\{G_n\}} S_w(1) \geq \frac{k-1}{k}\,?$$

We will show that if G is a free pro-p group of finite rank this will not hold in general:

Theorem I. *Let L be the d-generated free pro-p group with $d \geq 2$, with a filtration $\{L_n\}$ given by the dimension subgroups of L and consider the word $w_k = \prod_{1\leq i\leq k}[x_i, y_i]$ for some $k \geq 1$. Then*

$$\mathrm{Dim}_{\{L_n\}} S_{w_k}(1) \leq 1/2.$$

Hence we get counter examples for Question 2 when G is a free pro-p group of finite rank.

A more interesting situation will be when G is a compact p-adic analytic group. We will only make an introduction on this area by underlining the requirements to get a positive answer to Question 2 in this setting. We believe this will be an interesting area to continue to do research on that will require to learn about other topics such as the resolution of singularities in the p-adic setting.

Chapter 2

Words in p-groups of nilpotency class 2

2.1 Introduction

As a first approach to study Amit's Conjecture 1 on finite nilpotent groups, we will consider finite groups of nilpotency class 2 since they are close to being abelian. If Conjecture 1 holds for two groups G_1 and G_2, then it holds for their direct product $G = G_1 \times G_2$ since the word equations can be solved componentwise. Let $\mathbf{g} = (g_1, ..., g_k)$ be a k-tuple in G. Then $\mathbf{g} = \mathbf{a} \cdot \mathbf{h}$ where $\mathbf{a} = (a_1, ..., a_k)$ and $\mathbf{h} = (h_1, ..., h_k)$ are k-tuples in G_1 and G_2, respectively. Therefore it is clear that $w(\mathbf{g}) = w(\mathbf{a}) \cdot w(\mathbf{h})$. Hence $N_{w,G}(1) = N_{w,G_1}(1) \cdot N_{w,G_2}(1)$ and the result follows since $|G| = |G_1| \cdot |G_2|$. Consequently, since any nilpotent group is the direct product of its Sylow subgroups, it reduces to show that Amit's conjecture holds for any finite p-group; in this case of nilpotency class 2.

The next section will be devoted to proving that for any finite p-group G of nilpotency class 2 and any word w in k variables, $N_w(1) \geq |G|^{k-1}$ holds. Consequently, with the remark above, we obtain the main result.

Theorem A. *Let G be a finite group of nilpotency class 2 and let w be any word in k variables. Then $N_w(1) \geq |G|^{k-1}$.*

2.2 Word representatives in pro-p groups of nilpotency class 2

The objects of interest in this section will be the words in the class of p-groups of nilpotency class 2. For convenience, we will consider a word in the variables $x_1, \dots, x_k$ as an element in the free pro-p group of nilpotency class 2 on the variables $x_1, \dots, x_k$, F_k. Thus, any word w in k variables can be represented in a unique way as

$$w = x_1^{z_1} \cdots x_k^{z_k} \cdot \prod_{1 \le i < j \le k} [x_i, x_j]^{z_{ij}},$$

where the exponents z_l, z_{ij} are p-adic integers. Of course, if G is a finite p-group (or pro-p group) of nilpotency class 2 and $(g_1, \dots, g_k) \in G^{(k)}$, it makes sense to evaluate w on $g_1, \dots, g_k$ by applying the homomorphism $\pi : F_k \to G$ given by $x_i \to g_i$. As in the preliminaries, we denote this element $w(g_1, \dots, g_k)$ and define the function $N_w = N_{w,G}$ by (0.2).

If σ is an automorphism of F_k, σ is determined by the images of the generators $x_1, \dots, x_k$, which we denote $w_1, \dots, w_k$. Then the image of $w \in F_k$ is the word $w(w_1, \dots, w_k)$, the result of evaluating w on $w_1, \dots, w_k$. Since σ is an automorphism, there exist $(w_1', \dots, w_k') \in F_k^{(k)}$ such that $w_i'(w_1, \dots, w_k) = x_i$, for $1 \le i \le k$, such that the inverse automorphism is given by $x_i \mapsto w_i$. If G is a finite p-group (or pro-p group) of nilpotency class 2, we can define the map $\phi : G^{(k)} \to G^{(k)}$ by $\phi(g_1, \dots, g_k) = (w_1(g_1, \dots, g_k), \dots, w_k(g_1, \dots, g_k))$ and it is clear that this map is a bijection with the inverse map given by $(g_1, \dots, g_k) \mapsto (w_1'(g_1, \dots, g_k), \dots, w_k'(g_1, \dots, g_k))$. If $w' = w(w_1, \dots, w_k)$, it is clear that $w'(g_1, \dots, g_k) = g$ if and only if $w(\phi(g_1, \dots, g_k)) = g$, thus ϕ is a bijection between the solutions of $w' = g$ and $w = g$ and in particular, $N_{w,G} = N_{w',G}$.

Definition 6. We will say that two words $w, w' \in F_k$ are *equivalent* if they belong to the same orbit under the action of the automorphism group of F_k.

Therefore we obtain the following result.

Proposition 7. *If $w, w' \in F_k$ are equivalent words, $N_{w,G} = N_{w',G}$ for any finite p-group G of nilpotency class 2.*

Hence our next goal is to find a set of representatives of the equivalence classes of words. The following results are well-known folklore. However, we could not find a specific reference for them and decided it was worth writing down some details.

Lemma 8. *Let F_k be the free pro-p group of nilpotency class 2 on the variables $x_1, \ldots, x_k$. Then, there are natural homomorphisms*

$$\mathrm{Aut}(F_k) \twoheadrightarrow \mathrm{Aut}(F_k/F_k') \cong \mathrm{GL}_k(\mathbb{Z}_p) \to \mathrm{Aut}(F_k') \tag{2.1}$$

where the composite map is the restriction.

Proof. Since F_k' is a characterisctic subgroup of F_k, any $\alpha \in \mathrm{Aut}(F_k)$ restricts to an automorphism in F_k'. But since $F_k' \subseteq Z(F_k)$, this restriction factorises through F_k/F_k' and $\mathrm{Aut}(F_k/F_k') \cong \mathrm{GL}_k(\mathbb{Z}_p)$.

Let $\alpha \in \mathrm{Aut}(F_k)$. Then α is determined by the images of the generators $\bar{x_1}, \ldots, \bar{x_k}$:

$$\begin{aligned} \bar{\alpha} : F_k/F_k' &\longrightarrow F_k/F_k' \\ \bar{x_i} &\longrightarrow \prod_{1 \le j \le k} \bar{x_j}^{e_{ij}} \end{aligned} \tag{2.2}$$

for some p-adic integers e_{ij}. Consequently, there exists an isomorphism from $\mathrm{Aut}(F_k/F_k')$ to $\mathrm{GL}_k(\mathbb{Z}_p)$ such that $\bar{\alpha}$ is mapped to $X = (e_{ij})$.

It is convenient to identify F_k' with the group of $k \times k$ antisymmetric matrices over $\mathbb{Z}_p$, $\mathcal{A}_k$. Noting that F_k' is generated by commutators, for any element $w \in F_k'$, $w = \prod_{1 \le i < j \le k} [x_i, x_j]^{z_{ij}} \mapsto A$, where $A \in \mathcal{A}_k$ has entries z_{ij} for $1 \le i < j \le k$. Then, for $X \in \mathrm{GL}_k(\mathbb{Z}_p)$, the action of X on $\mathcal{A}_k$ is given by $A \mapsto X^t A X$ and it is coincides exactly with the restriction of $\alpha \in \mathrm{Aut}(F_k)$ to $\mathrm{Aut}(F_k')$. To see this,

$$\alpha([x_i, x_j]) = [\alpha(x_i), \alpha(x_j)] = \left[\prod_{1 \le r \le k} x_r^{e_{ir}}, \prod_{1 \le s \le k} x_s^{e_{js}} \right] = \prod_{1 \le r < s \le k} [x_r, x_s]^{e_{ir}e_{js} - e_{is}e_{jr}}.$$

Consequently, for any element $w = \prod_{1\leq i<j\leq k}[x_i, x_j]^{z_{ij}} \in F_k'$, we obtain that

$$\begin{aligned}\alpha(w) &= \prod_{1\leq i<j\leq k} \alpha([x_i, x_j])^{z_{ij}} = \prod_{1\leq i<j\leq k} \left(\prod_{1\leq r<s\leq k} [x_r, x_s]^{z_{ij}(e_{ir}e_{js}-e_{is}e_{jr})} \right) \\ &= \prod_{1\leq r<s\leq k} [x_r, x_s]^{\sum_{1\leq i<j\leq k} z_{ij}(e_{ir}e_{js}-e_{is}e_{jr})} = \prod_{1\leq r<s\leq k} [x_r, x_s]^{\sum_{1\leq i,j\leq k} e_{ir}z_{ij}e_{js}}.\end{aligned}$$

By the identification of F_k' with $\mathcal{A}_k$, $\alpha(w)$ corresponds to the matrix A' such that

$$A'_{r,s} = \sum_{1\leq i,j\leq k} e_{ir}z_{ij}e_{js} = (X^tAX)_{r,s},\ \forall r < s.$$

Consequently, $A' = X^tAX$ as we wanted to show. □

Recall also that the affine subgroups $\mathrm{Aff}_{k-1}(\mathbb{Z}_p)$ consist of the matrices $\left(\begin{smallmatrix} 1 & 0 \\ u^t & X \end{smallmatrix}\right)$, $u \in \mathbb{Z}_p^{(k-1)}$ (t means transposition), $X \in \mathrm{GL}_{k-1}(\mathbb{Z}_p)$. The action of X on $\mathcal{A}_k$ is better understood if we interpret A as an alternating bilinear form on the free $\mathbb{Z}_p$-module $\mathbb{Z}_p^{(k)}$. Additionally note that under a change of basis, the matrix A is now transformed into PAP^t, where P is the matrix associated to the change of basis, writing the coordinates of the vectors in the new basis as rows of P.

Lemma 9. (*i*) *Any orbit of the action of* $\mathrm{GL}_k(\mathbb{Z}_p)$ *on* $\mathcal{A}_k$ *contains a unique diagonal block matrix with diagonal non-zero blocks* $p^{s_i}H$, $H = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, $1 \leq i \leq r$ *and* $0 \leq s_1 \leq \cdots \leq s_r$ *(*$0 \leq r \leq k/2$*).*

(*ii*) *Any orbit of the action of the affine group* $\mathrm{Aff}_{k-1}(\mathbb{Z}_p)$ *on* $\mathcal{A}_k$ *contains a unique tridiagonal matrix* A' *(that is, all the entries* a'_{ij} *of* A' *with* $|i-j| > 1$ *are zero) with the non-zero entries above the main diagonal* $a'_{i,i+1} = p^{s_i}$, $1 \leq i \leq r$, *and* $0 \leq s_1 \leq s_2 \leq \cdots \leq s_r$ *(*$0 \leq r < k$*).*

Proof. We consider a basis $\{e_1, \ldots, e_k\}$ (for instance, the canonical basis) in the free $\mathbb{Z}_p$-module $\mathbb{Z}_p^{(k)}$ and the alternating bilinear form $(,)$ defined by the matrix A with respect to this basis. There is nothing to prove if A is a zero matrix, so we can suppose that $(e_i, e_j) \neq 0$ for some $1 \leq i < j \leq k$ and we can assume that its p-adic valuation is minimum among the valuations of all the (non-zero) (e_r, e_s). After reordering the basis, we can suppose that $i = 1$ and $j = 2$ and moreover, by multiplying e_1 or e_2 by a p-adic unit, we can suppose that $(e_1, e_2) = p^{s_1}$ for some $s_1 \geq 0$. Notice that any (non-zero) (u, v) has p-adic valuation greater than or equal to p^{s_1}.

Now for each $i \geq 3$ we set $e_i' = e_i + \alpha_i e_1 + \beta_i e_2$, where $\alpha_i, \beta_i \in \mathbb{Z}_p$ are chosen so that $(e_i', e_1) = (e_i', e_2) = 0$. The elements α_i, β_i exist because the valuation of (e_1, e_2) is less than or equal to the valuations of (e_i, e_2) and (e_i, e_1). By replacing e_i by e_i' we can suppose that $\langle e_1, e_2 \rangle$ is orthogonal to $\langle e_3, \ldots, e_k \rangle$. Proceeding inductively, we obtain a basis $\{e_1', \ldots, e_k'\}$ such that, for some $0 \leq r \leq k/2$, the subspaces $\langle e_{2i-1}', e_{2i}' \rangle$ are pairwise orthogonal for $1 \leq i \leq r$, the remaining vectors are in the kernel of the form and $(e_{2i-1}', e_{2i}') = p^{s_i}$, $1 \leq i \leq r$, with $0 \leq s_1 \leq \ldots \leq s_r$. It is clear that with respect to this new basis the matrix associated to the form $(\ ,\ )$ has the desired form.

To prove uniqueness suppose that A and A' are diagonal block matrices with (non-zero) diagonal blocks $p^{s_1}H, \ldots, p^{s_r}H$, $0 \leq s_1 \leq \ldots \leq s_r$, and $p^{s_1'}H, \ldots, p^{s_t'}H$, $0 \leq s_1 \leq \ldots \leq s_t$, respectively, and $A' = X^t A X$ for some $X \in \mathrm{GL}_k(\mathbb{Z}_p)$. The matrices A, A' and X can be viewed as endomorphisms of the abelian groups $R_n = (\mathbb{Z}/p^n\mathbb{Z})^{(k)}$, $n \geq 1$. Since X defines in fact an automorphism of R_n the image subgroups of A and A' (as endomorphisms of R_n) have the same order. For A this order is p^{2s}, where $s = \sum_{s_i \leq n}(n - s_i)$, and similarly for A'. We conclude that, for any $n \geq 1$, $\sum_{s_i \leq n}(n - s_i) = \sum_{s_i' \leq n}(n - s_i')$, whence $r = t$ and $s_i = s_i'$ for all $1 \leq i \leq r$; that is, $A = A'$.

For the existence part in (ii) we have to show that, given an alternating form $(\ ,\ )$ on $\mathbb{Z}_p^{(k)}$ and a basis $\{e_1, \ldots, e_k\}$, there exists another basis $\{e_1', \ldots, e_k'\}$ such that $e_1' \in e_1 + \langle e_2, \ldots, e_k \rangle$, $\langle e_2', \ldots, e_k' \rangle = \langle e_2, \ldots, e_k \rangle$ and $(e_i', e_j') = 0$ for $|i - j| > 1$, $(e_i, e_{i+1}) = p^{s_i}$, $0 \leq s_1 \leq \ldots \leq s_r$, $(e_i, e_{i+1}) = 0$, $r < i < k$. We can suppose that $(,)$ is not the trivial form and then consider the minimum valuation s_1 of all the (non-zero) (e_i, e_j). If this minimum is attained for some (e_1, e_j) we interchange e_2 and e_j. Otherwise this minimum is attained for some (e_i, e_j), $2 \leq i < j \leq k$ and $(e_1 + e_i, e_j)$ still has valuation s_1 (because the valuation of (e_1, e_j) is strictly greater than s_1). By replacing e_1 by $e_1 + e_i$, interchanging e_2 and e_j , and adjusting units, we can suppose that $(e_1, e_2) = p^{s_1}$. Now we can replace e_i, $i \geq 3$, by $e_i' = e_i + \alpha_i e_2$, where α_i is chosen so that $(e_1, e_i') = 0$. Thus we can assume $(e_1, e_i) = 0$ for $i \geq 3$. Now we iterate the procedure with the basis elements $e_2, \ldots, e_k$.

We prove uniqueness with a similar counting argument as in (i) but by considering the order of the images of the subgroup of R_n, $S_n = \{0\} \times (\mathbb{Z}/p^n\mathbb{Z})^{(k-1)}$. So we assume that $A' = X^t A X$ with A and A' as in (ii) and $X \in \mathrm{Aff}_{k-1}(\mathbb{Z}_p)$. Notice that, as an automorphism of R_n, X fixes S_n, so the images of S_n by A and A' must have the

same order. These orders are p^s and $p^{s'}$, where $s = \sum_{s_i \leq n}(n - s_i)$ and similarly for s', so $s = s'$ and, since this must happen for any $n \geq 1$, it follows that $s_i = s_i'$ for all i; that is, $A = A'$. □

Theorem B. *The following words are a system of representatives of the action of* $\operatorname{Aut} F_k$ *on* F_k*:*

$$[x_1, x_2]^{p^{s_1}} \cdots [x_{2r-1}, x_{2r}]^{p^{s_r}},\ 2r \leq k,\ 0 \leq s_1 \leq \ldots \leq s_r, \quad (2.3)$$

$$x_1^{p^{s_1}} [x_1, x_2]^{p^{s_2}} [x_2, x_3]^{p^{s_3}} \cdots [x_{r-1}, x_r]^{p^{s_r}},\ 1 \leq r \leq k,\ 0 \leq s_1,\ 0 \leq s_2 \leq \ldots \leq s_r. \quad (2.4)$$

Proof. As explained in Lemma 8, the action of $\operatorname{Aut} F_k$ on F_k' can be suitably identified with the action of $\mathrm{GL}_k(\mathbb{Z}_p)$ on $\mathcal{A}_k$, thus it follows directly from part (i) of the previous lemma that the words (2.3) are representatives for the orbits contained in F_k'.

Now suppose $w \in F_k \backslash F_k'$. Then $w = (x_1^{z_1} \cdots x_k^{z_k})^{p^{s_1}} \prod_{1 \leq i < j \leq k} [x_i, x_j]^{z_{ij}}$, where $s_1 \geq 0$ and some z_i is a p-adic unit. After applying the inverse of the automorphism $x_1 \mapsto x_1^{z_1} \cdots x_k^{z_k}$, $x_i \mapsto x_1$, $x_j \mapsto x_j$, for $j \neq 1, i$, we can assume that $x_1^{z_1} \cdots x_k^{z_k} = x_1$. Now we consider the action of the stabilizer of x_1, $\operatorname{Aut}_{x_1} F_k$. The image of this subgroup by the first map in (2.1) is $\mathrm{Aff}_{k-1}(\mathbb{Z}_p)$, so we can identify the action of $\operatorname{Aut}_{x_1} F_k$ on F_k' with the action of $\mathrm{Aff}_{k-1}(\mathbb{Z}_p)$ on $\mathcal{A}_k$. If follows from Lemma 9 (ii) that w is equivalent to a word in (2.4). Notice also that if $w' = \sigma(w)$ for two of these words w and w' and some $\sigma \in \operatorname{Aut} F_k$, it would follow by passing to F_k/F_k' that $\sigma(\bar{x}_1)^{p^{s_1}} = \bar{x}_1^{p^{s_1'}}$. Since σ induces automorphisms of $(F_k/F_k')^{p^s}$ and this chain of subgroups of F_k/F_k' is strictly decreasing, we conclude that $s_1 = s_1'$. But F_k/F_k' is torsion-free, so σ fixes $\bar{x}_1$, that is, $\sigma(x_1) = x_1 z$ for some $z \in F_k'$. Composing σ with the automorphism $x_1 \mapsto x_1 z^{-1}$, $x_i \mapsto x_i$, $i \geq 2$, we can suppose that $\sigma \in \operatorname{Aut}_{x_1} F_k$. Thus, the two matrices in $\mathcal{A}_k$ associated to $x_1^{\mathrm{fl} p^{s_1}} w$ and $x_1^{\mathrm{fl} p^{s_1}} w'$ are in the same orbit by $\mathrm{Aff}_{k-1}(\mathbb{Z}_p)$, and so they coincide by Lemma 9 (ii). We conclude that $w = w'$. □

Theorem 10. *Let* G *be a finite* p*-group of nilpotency class* 2 *and* w *a word in* k *variables. Then* $N_w(1) \geq |G|^{k-1}$.

Proof. We can suppose that w is as in the last theorem. Write $k_0 = \lfloor k/2 \rfloor$ and fix $(g_2, g_4, \ldots, g_{2k_0}) \in G^{(k_0)}$. Then the map $G' \times G^{(k-k_0-1)} \to G'$ given by $(x_1, x_3, \ldots, x_{2(k-k_0)-1}) \mapsto w(x_1, g_2, x_3, \ldots)$ is a group homomorphism whose kernel has size at least $|G|^{k-k_0-1}$. Since there are $|G|^{k_0}$ choices for $(g_2, g_4, \ldots, g_{2k_0})$, we get at least $|G|^{k-1}$ solutions to the equation $w(x_1, \ldots, x_k) = 1$. □

Chapter 3

The functions N_w from a character-theoretical point of view

3.1 N_w is a generalized character

In this section, unless otherwise stated, we consider an arbitrary finite group G and a word w that is thought now as an element in the free group with, say, free generators $x_1, \ldots, x_k$. Note $N_w = N_{w,G}$ is a (non-negative) integer valued class function since it is constant on the conjugacy classes. The set of complex irreducible characters of G, $\mathrm{Irr}(G)$; is an orthonormal basis for the vector space of the complex class functions and N_w can be written as a linear combination of the irreducible characters of G:

$$N_w = \sum_{\chi \in \mathrm{Irr}(G)} N_w^\chi \chi, \tag{3.1}$$

where

$$N_w^\chi = (N_w, \chi) = \frac{1}{|G|} \sum_{g \in G} N_w(g)\overline{\chi(g)} = \frac{1}{|G|} \sum_{(g_1,\ldots,g_k) \in G^{(k)}} \overline{\chi\big(w(g_1, \ldots, g_k)\big)} \tag{3.2}$$

are unique for any $\chi \in \mathrm{Irr}(G)$. Note that for the trivial character 1_G of G and for any word w,

$$N_w^{1_G} = \frac{1}{|G|} \sum_{g \in G} N_w(g)\overline{1_G(g)} = \frac{1}{|G|} \sum_{g \in G} N_w(g) = |G|^{k-1}. \tag{3.3}$$

If $N_w^\chi \in \mathbb{N}$ (resp. $N_w^\chi \in \mathbb{Z}$) for all $\chi \in \mathrm{Irr}(G)$, then N_w is a *character* (or *generalized character*) in G. In this section we first give a characterization for N_w to be a generalized character. (We have already used before that a necessary condition is that $N_w(g) = N_w(g^i)$ for any i coprime with the order of g and we are going to see that this condition is in fact sufficient). The proof is standard once we know that the coefficients N_w^χ are algebraic integers. To prove this, Amit and Vishne point out in [19] that one can use the arguments of Stanley in [20] and build on the result of Solomon which says that $N_w(g)$ is always a multiple of $|C_G(g)|$ (see [21]):

Proposition 11 ([20])**.** *Let G be a finite group and $w \in F_k$, $k > 1$. Then N_w^ψ is an algebraic integer for any $\psi \in \mathrm{Irr}(G)$; more specifically, $N_w^\psi \in \mathbb{Z}[\xi]$ where ξ is a $|G|$-th primitive root of unity.*

Proof. Let $\{h_1, \ldots, h_s\}$ be a set of representatives for the conjugacy classes C_i in G. For each C_i, we will denote by χ_{C_i} the characteristic function of C_i; that is, $\chi_{C_i}(g) = 1$ if $g \in C_i$ and $\chi_{C_i}(g) = 0$ otherwise. By Solomon in [21], we have $\frac{|C_i|}{|G|} N_w(h_i) \in \mathbb{N}$. Hence note that N_w is an integral combination of χ_{C_i} and so, using the orthogonality relations,

$$\begin{aligned} N_w(g) &= \sum_{i=1}^{s} N_w(h_i)\chi_{C_i}(g) = \sum_{i=1}^{s} \frac{|C_i|}{|G|} N_w(h_i)\left(\frac{|G|}{|C_i|}\chi_{C_i}(g)\right) \\ &= \sum_{i=1}^{s} \frac{|C_i|}{|G|} N_w(h_i)\left(\sum_{\psi\in\mathrm{Irr}(G)} \overline{\psi(h_i)} \cdot \psi(g)\right) \\ &= \sum_{\psi\in\mathrm{Irr}(G)} \left(\sum_{i=1}^{s} \frac{|C_i|}{|G|} N_w(h_i) \cdot \overline{\psi(h_i)}\right)\psi(g), \end{aligned}$$

where $N_w^\psi = \sum_{i=1}^{s} \frac{|C_i|}{|G|} N_w(h_i) \cdot \overline{\psi(h_i)} \in \mathbb{Z}[\xi]$ as we wanted. □

The following well-known lemma wich can be found in [19] characterizes when the coefficients for a rational valued class-function are rational:

Lemma 12. *Let f be a rational-valued class function of a group G. Then f is a $\mathbb{Q}$-linear combination of irreducible characters if and only if $f(g) = f(g^i)$ for any $g \in G$ and i coprime to the order of G.*

Proof. Write $f = \sum_{\chi\in\mathrm{Irr}(G)} a_\chi \chi$ with $a_\chi \in \mathbb{Q}$, and σ is an automorphism of the cyclotomic extension of $\mathbb{Q}(\xi)/\mathbb{Q}$ sending $\xi \mapsto \xi^i$, where ξ is a primitive $|G|$-th root of

unity. Besides, for every $g \in G$, there exists a representation of G affording χ which is diagonalizable with eigenvalues that are powers of ξ (see [22]). Hence,

$$\chi(g) = \sum_{j=1}^{\chi(1)} \xi^{i_j};$$

and we have,

$$f(g) = f(g)^\sigma = \sum_{\chi \in \mathrm{Irr}(G)} a_\chi \chi^\sigma(g) = \sum_{\chi \in \mathrm{Irr}(G)} a_\chi \chi(g^i) = f(g^i).$$

Conversely, if $f(g) = f(g^i)$,

$$f(g) = f(g)^{\sigma^{-1}} = f(g^i)^{\sigma^{-1}} = (\sum_{\chi \in \mathrm{Irr}(G)} a_\chi \chi(g^i))^{\sigma^{-1}} = \sum_{\chi \in \mathrm{Irr}(G)} a_\chi^{\sigma^{-1}} \chi(g).$$

Since the irreducible characters form a basis for the space of class functions, we conclude that $a_\chi = a_\chi^{\sigma^{-1}}$ for any automorphism σ, so $a_\chi \in \mathbb{Q}$. □

Using the previous lemma and that N_w^χ are algebraic integers, we see that the necessary condition for being a generalized character is actually sufficient:

Corollary 13. *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 $N_w(g) = N_w(g^i)$ for any $g \in G$ and i coprime with the order of G.*

Hence we are ready to prove the main result of this section:

Theorem C. *Let G be a finite group of nilpotency class 2 and w a word. Then N_w is a generalized character of G.*

Proof. By Proposition B we can suppose that w has the form (2.3) or (2.4). Without loss of generality G is a finite p-group. Now we observe that, if i is coprime to p, the map $(g_1, g_2, \ldots, g_k) \mapsto (g_1^i, g_2, g_3^i, \ldots)$ is a bijection from the set of solutions of $w = g$ to the set of solutions of $w = g^i$, so in particular $N_w(g) = N_w(g^i)$ and the result follows using the previous lemma. □

3.2 The functions N_w for odd p-groups of nilpotency class 2

Now that we have proved that N_w is a generalized character for p-groups of nilpotency class 2, a natural question to study is whether the function N_w is a character.

Lemma 14. *Let G be a finite group and w a word in k variables for which N_w is a character in G. Then $N_w(1)$ reaches the maximum among all values of N_w and besides, $N_w(1) \geq |G|^k/|G_w|$.*

Proof. Using that for any $\chi \in \mathrm{Irr}(G)$, $|\chi(g)| \leq \chi(1)$, we obtain

$$N_w(g) = |N_w(g)| \leq \sum_{\chi \in \mathrm{Irr}(G)} |N_w^\chi| \cdot |\chi(g)| \leq \sum_{\chi \in \mathrm{Irr}(G)} N_w^\chi \chi(1) = N_w(1),$$

to conclude that $N_w(1)$ reaches the maximum among the values of N_w. Finally, $|G|^k = \sum_{g \in G_w} N_w(g) \leq |G_w|\, N_w(1)$, and so $N_w(1) \geq |G|^k/|G_w|$. □

We recall briefly that for some words w the functions N_w are known to be characters for any finite group. The study of the numbers N_w^χ goes back to Frobenius [23] who showed that for any finite group G, $N_{[x,y]}^\chi = \frac{|G|}{\chi(1)} \in \mathbb{N}$ (this is basically [22, Chapter 3.10]). This classical result due to Frobenius can be extended in various ways: when w is an admissible word (i.e. a word in which all the variables appear exactly twice, once with exponent 1 and once with -1) [24]. Or when $w = [w', y]$, where y is a variable which does not occur in w'. Before proceeding recall the formula for the convolution of two class functions f_1, f_2, defined by

$$(f_1 * f_2)(g) = \frac{1}{|G|} \sum_{h \in G} f_1(h) \cdot \overline{f_2(h^{-1}g)}$$

and that for $\chi \in \mathrm{Irr}(G)$,

$$f_1 * \chi = \frac{(f_1, \chi)}{\chi(1)} \cdot \chi. \tag{3.4}$$

The following results can be deduced from [22]:

Lemma 15. *Let G be any finite group and w be a word in k variables and y not appearing in w. Then $N_{[y,w]}$ is a character in G.*

Proof. For any $g \in G$,

$$\begin{aligned} N_{[y,w]}(g) &= \sum_{h\in G} N_w(h)\cdot \sharp\{a\in G : [a,h]=g\} = \sum_{h\in G} N_w(h)\cdot \sharp\{a\in G : h^{-a}=gh^{-1}\} \\ &= \sum_{h\in G} N_w(h)\cdot |C_G(h)|\cdot \delta_{gh^{-1}\in Cl_G(h^{-1})} = \sum_{h\in G} N_w(h)\cdot \sum_{\chi\in \mathrm{Irr}(G)} \chi(gh^{-1})\cdot \overline{\chi(h^{-1})} \\ &= |G|\cdot \sum_{\chi\in \mathrm{Irr}(G)} (\chi * N_w\chi)(g) = \sum_{\chi\in \mathrm{Irr}(G)} \frac{|G|}{\chi(1)}(\chi, N_w\chi)\cdot \chi(g); \end{aligned}$$

hence $N^{\chi}_{[y,w]} = \frac{|G|}{\chi(1)}(\chi, N_w\chi) = \frac{|G|}{\chi(1)}\sum_{\psi\in\mathrm{Irr}(G)} N^{\psi}_w(\chi,\psi\chi) \in \mathbb{N}$ since $\psi\chi$ is a character again. □

Note that $N_{[y,w]}(g) = N_{[w,y]}(g^{-1})$ and so this proves that for the lower central words γ_k, N_{γ_k} is a character for any finite group G (see [25]).

Lemma 16. *If N_w and $N_{w'}$ are characters (or generalized characters) for some disjoint words w and w', then so is $N_{w\cdot w'}$ and besides $N^{\chi}_{w\cdot w'} = \frac{|G|}{\chi(1)} N^{\chi}_w N^{\chi}_{w'}$.*

Proof. Using (3.4) and the orthogonality relations,

$$\begin{aligned} N_{w\cdot w'}(g) &= \sum_{h\in G} N_w(h)\cdot N_{w'}(h^{-1}g) = \sum_{h\in G} \Big(\sum_{\chi\in\mathrm{Irr}(G)} N^{\chi}_w\cdot\chi(h)\Big)\cdot\Big(\sum_{\psi\in\mathrm{Irr}(G)} N^{\psi}_{w'}\cdot\psi(h^{-1}g)\Big) \\ &= |G| \sum_{\chi,\psi\in\mathrm{Irr}(G)} N^{\chi}_w\cdot N^{\psi}_{w'}\cdot(\chi*\psi)(g) = |G| \sum_{\chi,\psi\in\mathrm{Irr}(G)} N^{\chi}_w\cdot N^{\psi}_{w'}\frac{(\chi,\psi)}{\chi(1)}\cdot\chi(g) \\ &= \sum_{\chi\in\mathrm{Irr}(G)} \frac{|G|}{\chi(1)}\cdot N^{\chi}_w\cdot N^{\chi}_{w'}\cdot\chi(g), \end{aligned}$$

and hence $N^{\chi}_{w\cdot w'} = \frac{|G|}{\chi(1)}\cdot N^{\chi}_w\cdot N^{\chi}_{w'}$. □

A result of Frobenius and Schur (see Chapter 4, [22]) implies that $N^{\chi}_{x^n}$ is a generalized character. The simplest example where N_{x^n} is not a character is the word $w = x^2$ for the quaternion group $\mathcal{Q}_8 = \langle -1, i, j, k \,|\, i^2 = j^2 = k^2 = ijk = -1, (-1)^2 = 1\rangle$. Consequently, the *Frobenius–Schur indicator* of χ can be used to describe $N^{\chi}_{x^2}$; that is, $N^{\chi}_{x^2} = \mathcal{FS}_{\chi} \in \{-1, 0, 1\}$. Note $N^{\chi}_{x^2} = -1$ when χ takes real values but is not afforded by a real representation. In the case of $\mathcal{Q}_8$, there is a 2-dimensional complex representation satisfying this condition and we get $N_{x^2,\mathcal{Q}_8}(1) = 2 < 6 = N_{x^2,\mathcal{Q}_8}(-1)$, which also shows using Lemma 14 that N_{x^2} is not a character for $\mathcal{Q}_8$ since $N_{x^2,\mathcal{Q}_8}(1)$ is not the maximum fibre. Chapter 4 will be devoted to show more examples of words and

groups for which N_w is not a generalized character either.

In contrast to the previous example, the goal of this section is to show that $N_{w,G}$ is a genuine character of a p-group G of nilpotency class 2 when p is odd. We begin with a general result.

Lemma 17. *Let $N \triangleleft G$ for a finite group G. Consider $\chi \in \mathrm{Irr}(G)$ with $N \subseteq Ker(\chi)$ and $w \in F_k$. Then*

$$N_{w,G}^{\chi} = |N|^{k-1} N_{w,G/N}^{\hat{\chi}},$$

where $\hat{\chi}$ is the character of G/N defined naturally by χ.

Proof.
$$\begin{aligned} N_{w,G}^{\chi} &= \frac{1}{|G|} \sum_{g \in G} N_{w,G}(g)\, \overline{\chi(g)} = \frac{1}{|G|} \sum_{gN \in G/N} \sum_{n \in N} N_{w,G}(gn)\, \overline{\chi(gn)} \\ &= \frac{|N|}{|G|} \sum_{gN \in G/N} \tilde{N}_w(gN)\, \overline{\hat{\chi}(gN)} = (\tilde{N}_w, \hat{\chi})_{G/N}, \end{aligned}$$

where $\tilde{N}_w$ is the average function defined by $\tilde{N}_w(gN) = \frac{1}{|N|} \sum_{n \in N} N_w(gn)$ viewed as a function on G/N, and hence is it clear that for such a function $\tilde{N}_w = |N|^{k-1} N_{w,G/N}$, and so the result follows. □

Lemma 18. *Let G be a finite p-group of nilpotency class 2 and let χ be a faithful irreducible character of G. Then $\chi(1)\chi = \eta^G$ for some η faithful linear character of $Z(G)$.*

Proof. We recall that a group G with faithful irreducible character χ has cyclic center, $Z = Z(G) = Z(\chi)$. Consider the restriction of χ to Z, χ_Z. From Lemma 2.27 [22], $\chi_Z = \chi(1)\eta$ for some faithful linear character in $\eta \in \mathrm{Irr}(Z)$. Using the Frobenius Reciprocity, we know $(\eta^G, \chi) = (\eta, \chi_Z)$ (see Lemma 5.2 in [22]). Hence, $\eta^G = \chi(1)\chi$. □

We introduce a result that will be used in Lemma 20:

Lemma 19. *Let ω be a primitive p^s-th root of unity. Then*

$$\sum_{\substack{1 \le i \le p^s \\ (i,p)=1}} \omega^i = \begin{cases} 1 & \text{if } s = 0 \\ -1 & \text{if } s = 1 \\ 0 & \text{if } s \ge 2. \end{cases}$$

Proof. From [26], we deduce that

$$\sum_{\substack{1\leq i\leq p^s\\(i,p)=1}} \omega^i = \mu(p^s),$$

where μ is the Möbius function. Since

$$\mu(m) = \begin{cases} 0 & \text{if } p^2|m \text{ for some prime } p \\ (-1)^s & \text{otherwise,} \end{cases}$$

for any $m \in \mathbb{Z}$ with s prime divisors. the result follows. □

Now we can characterize the conditions so that $N_w^\chi \in \mathbb{N}$ for a faithful irreducible character χ.

Lemma 20. *Let G be a finite p-group of nilpotency class 2 and w a word. If χ is a faithful irreducible character, then $N_w^\chi \in \mathbb{N}$ if and only if $N_w(1) \geq N_w(z)$, for all $z \in Z(G) = Z$ of order p.*

Proof. First note that $Z(G) = Z(\chi)$ is cyclic and by Lemma 18, we have $\chi(1)\chi = \eta^G$, where η is a faithful linear character of $Z(\chi)$. Then

$$N_w^\chi = \frac{1}{\chi(1)}(N_w, \eta^G) = \frac{1}{\chi(1)}(N_{w|Z}, \eta)_Z \in \mathbb{Z}$$

Let $Z(G) = \langle z_1 \mid z_1^{p^r} = 1\rangle$. Then $z = z_1^{p^{r-1}}$ and using Corollary 13 we have

$$(N_{w|Z}, \eta)_Z = \frac{1}{|Z|}\sum_{1\leq i\leq p^r} N_w(z_1^i)\epsilon^i = \frac{1}{|Z|}\sum_{1\leq j\leq r} N_w(z_1^{p^j})\Big(\sum_{\substack{1\leq i\leq p^{r-j}\\(i,p)=1}} (\epsilon^{p^j})^i\Big), \tag{3.5}$$

where $\epsilon = \overline{\eta(z_1)}$ is a primitive p^r-th root of the unity. Notice that the innermost sum of (3.5) is the sum of all the primitive p^{r-j}-th roots of unity. This is always zero except in the cases when $p^{r-j} = 1$ or $p^{r-j} = p$, in which cases, using Lemma 19, the sum is 1 or -1, respectively.

We conclude that

$$(N_{w|Z}, \eta)_Z = \frac{1}{|Z|}(N_w(1) - N_w(z_1^{p^{r-1}})) = \frac{1}{|Z|}(N_w(1) - N_w(z)),$$

and the result follows. □

Using the previous lemma, we characterize when N_w is a character for a finite p-group of nilpotency class 2.

Proposition 21. *Let G be a finite p-group of nilpotency class 2 and $w \in F_k$. Then N_w is a character if and only if for any (non-trivial) epimorphic image of G, say G_1, with cyclic centre; $N_{w,G_1}(1) \geq N_{w,G_1}(z)$, where z is any central element of G_1 of order p.*

Proof. To prove the sufficiency part, let $\chi \in \mathrm{Irr}(G)$, $N = Ker(\chi)$ and $G_1 = G/N$. If $\chi = 1_G$, from (3.3) we know $N_w^{1_G} = |G|^{k-1} \in \mathbb{N}$. Hence assume $\chi \neq 1_G$. By hypothesis $N_{w,G_1}(1) \geq N_{w,G_1}(z)$, for all z central elements of G_1 of order p. We can view χ as a faithful character $\hat{\chi}$ of G_1 and then Lemma 20 implies that $N_{w,G_1}^{\hat{\chi}} \in \mathbb{N}$. Using Lemma 17, $N_w^{\chi} \in \mathbb{N}$, which means that N_w is a character.

Conversely, suppose that N_w is a character, that is, all the coefficients $N_w^{\chi} \in \mathbb{N}$, and consider an epimorphic image $G_1 = G/N$ with cyclic center and a central element $z \in G_1$ of order p. Then G has an irreducible character χ with kernel N that is faithful when considered as a character $\hat{\chi}$ of G_1 (see Theorem 2.32 [22]). Using Lemma 17, $N_{w,G_1}^{\hat{\chi}} \in \mathbb{N}$. Then by Lemma 20, $N_{w,G_1}(1) \geq N_{w,G_1}(z)$ holds. □

Theorem D. *Let G be a finite p-group of nilpotency class 2, p odd, and let w a word in k variables. Then N_w is a character of G.*

Proof. By the last result, it suffices to show that if G has cyclic center Z and $z \in Z$ has order p, $N_w(1) \geq N_w(z)$. We can assume that w has the form (2.4) (if w is as in (2.3), skip the next two paragraphs).

If $Z^{p^{s_1}} \neq 1$, we can write $z = z_1^{p^{s_1}}$ for some $z_1 \in Z$ and then the map $(g_1, g_2, \ldots, g_k) \mapsto (g_1 z_1, g_2, \ldots, g_k)$ is a bijection between the sets of solutions of $w = 1$ and $w = z$, which means exactly that $N_w(1) = N_w(z)$.

Now we suppose that $Z^{p^{s_1}} = 1$ and note that, since G has nilpotency class 2 and p is odd,

$$(xy)^{p^{s_1}} = x^{p^{s_1}} y^{p^{s_1}} [y, x]^{\binom{p^{s_1}}{2}} = x^{p^{s_1}} y^{p^{s_1}}. \tag{3.6}$$

Therefore if we fix $g_2, g_4, \ldots \in G$, the map $(g_1, g_3 \ldots) \mapsto w(g_1, g_2, \ldots, g_k)$ is a group homomorphism $\phi_{g_2,g_4,\ldots}$. Obviously there is a bijection between the kernel of this homomorphism and the set of solutions of $w = 1$ with $x_{2i} = g_{2i}$. As for the solutions of $w = z$ with $x_{2i} = g_{2i}$, either this set is empty or else its elements are in one-to-one correspondence with the elements in a coset of the kernel of $\phi_{g_2,g_4,\ldots}$. In any case, considering only solutions with $x_{2i} = g_{2i}$, the number of solutions of $w = 1$ is greater that or equal to the number of solutions of $w = z$. Varying $g_2, g_4, \ldots$, we conclude $N_w(1) \geq N_w(z)$, as desired. □

3.3 The functions N_{x^n} for p-groups of nilpotency class 2

This technical section was done with the collaboration of J. Sangroniz. Here, we study the functions N_{x^n} for 2-groups of nilpotency class 2 and characterize when this function is a character. As we already pointed out in Section 3.2, the function N_{x^2,Q_8} is not a character and in fact for each $r \geq 1$ we can define a 2-group $\mathcal{Q}_{2^{3r}}$ of order 2^{3r}, which is the usual quaternion group Q_8 when $r = 1$, such that $N_{x^{2^r},\mathcal{Q}_{2^{3r}}}$ is not a character. We shall see in Theorem E that this group is in some sense involved in G whenever $N_{x^{2^r},G}$ is not a character. We shall also need to introduce another family of groups, denoted $\mathcal{D}_{2^{3r}}$, that, for $r = 1$, is the usual dihedral group of order 8.

Definition 22. Let $r \geq 1$. We define the *quasi dihedral* and *quasi quaternion* group, $\mathcal{D}_{2^{3r}}$ and $\mathcal{Q}_{2^{3r}}$, as

$$\mathcal{D}_{2^{3r}} = \langle x, y, z \,|\, x^{2^r} = y^{2^r} = z^{2^r} = 1, [x, z] = [y, z] = 1, [x, y] = z \rangle, \tag{3.7}$$

$$\mathcal{Q}_{2^{3r}} = \langle x, y, z \,|\, x^{2^r} = y^{2^r} = z^{2^{r-1}}, z^{2^r} = 1, [x, z] = [y, z] = 1, [x, y] = z \rangle. \tag{3.8}$$

Note that the quasi-dihedral group $\mathcal{D}_{2^{3r}}$ of order 2^{3r} can be constructed as

$$\mathcal{D}_{2^{3r}} = \langle x, z \rangle \rtimes \langle y \rangle,$$

where $\langle x, z \rangle \cong C_{2^r} \times C_{2^r}$, $\langle y \rangle \cong C_{2^r}$ and $x^y = xz$ and $z^y = z$. That is, $\mathcal{D}_{2^{3r}}$ is isomorphic to the Heisenberg group over $\mathbb{Z}/2^r\mathbb{Z}$; i.e. the set of 3×3 upper unitriangular matrices with elements in $\mathbb{Z}/2^r\mathbb{Z}$. On the other hand, the quasi-quaternion group

$\mathcal{Q}_{2^{3r}}$ of order 2^{3r} can be constructed as

$$\langle x, z\rangle \rtimes \langle y\rangle / \langle (x^2 z^{-1})^{2^{r-1}}\rangle,$$

where $\langle x, z\rangle \cong C_{2^{r+1}} \times C_{2^r}$, $\langle y\rangle \cong C_{2^r}$ and $x^y = xz$ and $z^y = z$. One can check that, $\mathcal{Q}_{2^{3r}} = \langle x, y, z\rangle$ can be seen as a finite quotient of the pro-2 group $\mathrm{GL}_4(\mathbb{Z}/2^r\mathbb{Z})$ generated by the matrices

$$x = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad y = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad z = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Proposition 23. *If $G = \mathcal{D}_{2^{3r}}$ or $\mathcal{Q}_{2^{3r}}$, then G has order 2^{3r}, exponent 2^{r+1} and $G' = Z(G) = \langle z\rangle$ is cyclic of order 2^r. Moreover, if $t = z^{2^{r-1}}$ is the central involution, in the (quasi) dihedral case $N_{x^{2^r}}(1) = 3 \cdot 2^{3r-2}$ and $N_{x^{2^r}}(t) = 2^{3r-2}$, whereas in the quaternion case the numbers are in reverse order: $N_{x^{2^r}}(1) = 2^{3r-2}$ and $N_{x^{2^r}}(t) = 3 \cdot 2^{3r-2}$. Consequently, by Lemma 20, $N_{x^{2^r}}$ is not a character of $\mathcal{Q}_{2^{3r}}$.*

Proof. In both cases, it is not hard to show that G has order 2^{3r}, exponent 2^{r+1} and $G' = Z(G) = \langle z\rangle$ is cyclic of order 2^r. Besides, note $G_{x^{2^r}} = \{1, t\}$.

If $G = \mathcal{D}_{2^{3r}}$, for any $a, b, c \in \mathbb{Z}/2^r\mathbb{Z}$, $(x^a y^b z^c)^{2^r} = [x, y]^{ab\cdot\binom{2^r}{2}} = t^{ab\cdot(2^r-1)}$. Consequently, $(x^a y^b z^c)^{2^r} = 1$ if and only if $a \cdot b \equiv 0 \pmod 2$ and hence, $N_{w,G}(1) = 2^{3r-2} \cdot 3$. Therefore, $N_{w,G}(t) = 2^{3r-2}$. If we consider $G = \mathcal{Q}_{2^{3r}}$, for any $a, b, c \in \mathbb{Z}/2^r\mathbb{Z}$, $(x^a y^b z^c)^{2^r} = t^{a+b}[x^a, y^b]^{\binom{2^r}{2}} = t^{a+b+ab\cdot(2^r-1)}$. Consequently, $(x^a y^b z^c)^{2^r} = 1$ if and only if $a, b \equiv 0 \pmod 2$. Hence, $N_{w,G}(1) = 2^{3r-2}$ and therefore, $N_{w,G}(t) = 2^{3r-2} \cdot 3$. □

If T and H are 2-groups with cyclic center and $|Z(T)| \leq |Z(H)|$, we shall denote by $T * H$ the central product of T and H with $Z(T)$ amalgamated with the corresponding subgroup of $Z(H)$ following the definition in Section 0.3. We also showed that if all generators of $Z(T)$ are in the same orbit under the action of the automorphism group of T (or if a similar situation holds for H), the group $T * H$ is unique up to isomorphism. This is exactly what happens if $T = \mathcal{D}_{2^{3r}}$ or $T = \mathcal{Q}_{2^{3r}}$. The main objective of this section will be to prove the following theorem:

Theorem E. *Let G be a finite 2-group of nilpotency class 2. Then $N_{x^{2^r}}$ is a character of G if and only if G has no epimorphic image isomorphic to $\mathcal{D}_{2^{3r_1}} * \cdots * \mathcal{D}_{2^{3r_n}} * \mathcal{Q}_{2^{3r}}$, $n \geq 0$, $r_1 \leq \ldots \leq r_n \leq r$.*

For a p-group G, from Section 0.2 we know that $\Omega_r(G)$ is the subgroup generated by elements of order at most p^r; that is,

$$\Omega_r(G) = \langle x \in G \mid x^{p^r} = 1 \rangle. \tag{3.9}$$

Lemma 24. *Let G be a finite 2-group of nilpotency class 2 with cyclic centre Z of order 2^r. Suppose $\Omega_{r+1}(G)' = Z$. Then $G = T * H$, where T is isomorphic to $\mathcal{D}_{2^{3r}}$ or $\mathcal{Q}_{2^{3r}}$ and H has cyclic center of order 2^r.*

Proof. Since G has nilpotency class 2, $\Omega_{r+1}(G)'$ is generated by the commutators of elements of order at most 2^{r+1} and it is cyclic, because it is contained in Z, which is cyclic, so it is generated by one of these commutators, say $[x, y]$. The orders of x and y have to be 2^r or 2^{r+1} (because $[x, y]$ has order 2^r). If both have order 2^r it is clear that $T = \langle x, y \rangle$ is isomorphic to $\mathcal{D}_{2^{3r}}$ and, if both have order 2^{r+1}, is isomorphic to $\mathcal{Q}_{2^{3r}}$ (notice that $G^{2^r} \subseteq Z$, so $x^{2^r} = y^{2^r}$). On the other hand, if one is of order 2^r and the other of order 2^{r+1}, the product would have order 2^r and T is isomorphic to $\mathcal{D}_{2^{3r}}$ again.

We take $H = C_G(T)$ and it suffices to check that $G = TC_G(T)$ (since $T \cap C_G(T) = Z(T)$ has order 2^r, and so it is the centre of G). Indeed, the conjugacy class of x has order $|[x, G]| = |G'| = |Z| = 2^r$ and the same for y, so

$$|G : C_G(T)| = |G : C_G(x) \cap C_G(y)| \leq |G : C_G(x)| \cdot |G : C_G(y)| = 2^{2r}.$$

But

$$|TC_G(T) : C_G(T)| = |T : T \cap C_G(T)| = |T : Z(T)| = 2^{2r},$$

so $G = TC_G(T)$, as claimed. □

As it happens with the usual dihedral and quaternion groups (see Lemma 1.3.17 in [5]), we prove the following lemma:

Lemma 25. *Let $(\mathcal{D}_1, \mathcal{D}_2)$ and $(\mathcal{Q}_1, \mathcal{Q}_2)$ be two pairs of quasi dihedral and quasi quaternion groups of order 2^{3r}, respectively. Then their amalgamated central products $\mathcal{D}_1 * \mathcal{D}_2$ and $\mathcal{Q}_1 * \mathcal{Q}_2$ are isomorphic.*

Proof. Let $\mathcal{Q}_1 = \langle q_1, q_2, [q_1, q_2]\rangle$ and $\mathcal{Q}_2 = \langle q_3, q_4, [q_3, q_4]\rangle$ be two quasi quaternion groups of order 2^{3r} using the presentation in (3.8). Note that the center of $\mathcal{Q}_1 * \mathcal{Q}_2$ is generated by $z = [q_1, q_2] = [q_3, q_4]$. Let $d_1 = q_1q_4$, $d_2 = q_1q_3^{-1}$, $d_3 = q_2q_3q_4$ and $d_4 = q_1^{-1}q_2^{-1}q_3^{-1}q_4^{-1}$. Using the relations of $\mathcal{Q}_{2^{3r}}$ given in (3.8), it follows that $d_i^{2r} = 1$ for $i = 1, 2, 3, 4$ and $[d_1, d_2] = [d_3, d_4] = z \neq 1$.

Hence $\mathcal{D}_1 = \langle d_1, d_2, [d_1, d_2]\rangle$ and $\mathcal{D}_2 = \langle d_3, d_4, [d_3, d_4]\rangle$ are quasi dihedral subgroups of order 2^{3r} in $\mathcal{Q}_1 * \mathcal{Q}_2$, $\mathcal{D}_1 \cap \mathcal{D}_2 = \langle z\rangle$, and $[\mathcal{D}_1, \mathcal{D}_2] = 1$. Therefore $\mathcal{D}_1 * \mathcal{D}_2 \cong \mathcal{Q}_1 * \mathcal{Q}_2$. □

Using this result and iterating Lemma 24, we get the following result.

Proposition 26. *Let G be a finite 2-group of nilpotency class 2 with cyclic centre of order 2^r. Then G is isomorphic to a group $\mathcal{D}_{2^{3r}} * \overset{n}{\cdots} * \mathcal{D}_{2^{3r}} * H$ or $\mathcal{D}_{2^{3r}} * \overset{n}{\cdots} * \mathcal{D}_{2^{3r}} * \mathcal{Q}_{2^{3r}} * H$, $n \geq 0$, where H has cyclic center of order 2^r and $\Omega_{r+1}(H)'$ is properly contained in the centre of H.*

Now suppose that $G = T * H$ where $T = \mathcal{D}_{2^{3r}}$ or $\mathcal{Q}_{2^{3r}}$ and H is 2-group of nilpotency class 2 with cyclic centre of order 2^r. For any $g \in T$, $g^{2^r} = 1$ or $g^{2^r} = t$, where t is the unique central involution. Thus if $h \in H$, $(gh)^{2^r} = 1$ if and only if $g^{2^r} = h^{2^r}$ both taking the value 1 or t. Similarly, $(gh)^{2^r} = t$ if and only if $g^{2^r} = 1$ and $h^{2^r} = t$ or the other way round. This means that

$$N_{x^{2^r},G}(1) = (N_{x^{2^r},T}(1)N_{x^{2^r},H}(1) + N_{x^{2^r},T}(t)N_{x^{2^r},H}(t))/2^r,$$

$$N_{x^{2^r},G}(t) = (N_{x^{2^r},T}(1)N_{x^{2^r},H}(t) + N_{x^{2^r},T}(t)N_{x^{2^r},H}(1))/2^r.$$

Consequently,

$$N_{x^{2^r},G}(1) = 2^{2r-2}(3N_{x^{2^r},H}(1) + N_{x^{2^r},H}(t)) \text{ or } N_{x^{2^r},G}(1) = 2^{2r-2}(N_{x^{2^r},H}(1) + 3N_{x^{2^r},H}(t)),$$

$$N_{x^{2^r},G}(t) = 2^{2r-2}(3N_{x^{2^r},H}(t) + N_{x^{2^r},H}(1)) \text{ or } N_{x^{2^r},G}(t) = 2^{2r-2}(N_{x^{2^r},H}(t) + 3N_{x^{2^r},H}(1)),$$

depending on whether $T = \mathcal{D}_{2^{3r}}$ or $T = \mathcal{Q}_{2^{3r}}$, respectively. It follows then that in the former case, $N_{x^{2^r},G}(1) \geq N_{x^{2^r},G}(t)$ if and only if $N_{x^{2^r},H}(1) \geq N_{x^{2^r},H}(t)$; whereas in the latter case, this holds if and only if $N_{x^{2^r},H}(1) \leq N_{x^{2r},H}(t)$ (the same equivalences hold if inequalities are replaced by equalities). Similarly, if $T = \mathcal{D}_{2^{3r}} * \overset{n}{\cdots} * \mathcal{D}_{2^{3r}}$ or $\mathcal{D}_{2^{3r}} * \overset{n}{\cdots} * \mathcal{D}_{2^{3r}} * \mathcal{Q}_{2^{3r}}$ with $n \geq 0$, for any central product $G = T * H$ such that

H is a 2-group of nilpotency class 2 with cyclic centre of order 2^r, in the former case, $N_{x^{2^r},G}(1) \geq N_{x^{2^r},G}(t)$ if and only if $N_{x^{2^r},H}(1) \geq N_{x^{2^r},H}(t)$; whereas in the latter case, this holds if and only if $N_{x^{2^r},H}(1) \leq N_{x^{2^r},H}(t)$. The combination of this with Proposition 26 reduces our problem to groups G with $\Omega_{r+1}(G)'$ properly contained in the center, which is the situation considered in the next lemma.

Lemma 27. *Let G be a finite 2-group of nilpotency class 2 with cyclic centre of order 2^r and let t be the unique central involution. Suppose that $\Omega_{r+1}(G)'$ is properly contained in $Z = Z(G)$. Then $N_{x^{2^r},G}(1) > N_{x^{2^r},G}(t)$ if and only if G has exponent 2^r. Otherwise, $N_{x^{2^r},G}(1) = N_{x^{2^r},G}(t)$.*

Proof. Since $(G')^{2^r} \subseteq Z^{2^r} = 1$, it is clear that raising to the 2^{r+1}-th power is a group endomorphism of G:

$$(xy)^{2^{r+1}} = x^{2^{r+1}} y^{2^{r+1}} [y,x]^{\binom{2^{r+1}}{2}} = x^{2^{r+1}} y^{2^{r+1}} [y,x]^{2^r(2^{r+1}-1)} = x^{2^{r+1}} y^{2^{r+1}}. \tag{3.10}$$

Moreover, $\Omega_{r+1}(G)'$ is contained in Z^2, so $(\Omega_{r+1}(G)')^{2^{r-1}} = 1$ and raising to the 2^r-th power is a group endomorphism of $\Omega_{r+1}(G)$ with kernel $\Omega_r(G) = \{x \in G \mid x^{2^r} = 1\}$. It is clear now that $N_{x^{2^r},G}(1) = |\Omega_r(G)|$ and $N_{x^{2^r},G}(t) = |\Omega_{r+1}(G)| - |\Omega_r(G)|$ (for any element x in $\Omega_{r+1}(G) \backslash \Omega_r(G)$, x^{2^r} is a central involution, since $[G^{2^r}, G] = (G')^{2^r} = 1$, so it is t), and so $N_{x^{2^r},G}(1) > N_{x^{2^r},G}(t)$ if and only if $|\Omega_{r+1}(G) : \Omega_r(G)| < 2$, that is $\Omega_{r+1}(G) = \Omega_r(G) = G$; i.e. G has exponent 2^r. Otherwise, $1 \neq \Omega_{r+1}(G)^{2^r} = \{x^{2^r} \mid x \in \Omega_{r+1}(G)\}$, thus $t \in \Omega_{r+1}(G)^{2^r}$ is in the image of the 2^r-th power endomorphism of $\Omega_{r+1}(G)$. It is clear now that $N_{x^{2^r},G}(1) = |\Omega_r(G)| = N_{x^{2^r},G}(t)$. □

Proposition 28. *Let G be a finite 2-group of nilpotency class 2 with cyclic centre of order 2^r and let t be the unique central involution. Then $N_{x^{2^r},G}(1) < N_{x^{2^r},G}(t)$ if and only if G is isomorphic to a group $\mathcal{D}_{2^{3^r}} * \overset{n}{\cdots} * \mathcal{D}_{2^{3^r}} * \mathcal{Q}_{2^{3^r}} * H$, $n \geq 0$, where H has cyclic center of order 2^r and exponent 2^r.*

Proof. By Proposition 26, G has two possible decompositions as a central product with one factor H satisfying the hypotheses of Lemma 27. If $\mathcal{Q}_{2^{3^r}}$ does not occur in the decomposition of G, we know that $N_{x^{2^r},G}(1) < N_{x^{2^r},G}(t)$ if and only if $N_{x^{2^r},H}(1) < N_{x^{2^r},H}(t)$, which according to Lemma 27, never happens. Thus $\mathcal{Q}_{2^{3^r}}$ does occur in the decomposition of G and in this case, we know that $N_{x^{2^r},G}(1) < N_{x^{2^r},G}(t)$ if and only if $N_{x^{2^r},H}(1) > N_{x^{2^r},H}(t)$, which, by Lemma 27, is equivalent to H having exponent 2^r. □

It is not difficult to classify the groups H in the previous proposition.

Lemma 29. *Let H be a finite 2-group of nilpotency class 2 with cyclic center of order 2^r and exponent 2^r. Then $H \cong \mathcal{D}_{2^{3r_1}} * \cdots * \mathcal{D}_{2^{3r_n}} * C_{2^r}$ with $r_1 \leq \ldots \leq r_n < r$.*

Proof. Suppose $H' = \langle [x,y] \rangle \neq 1$ has order 2^s. Since $(xy)^{2^r} = 1$, (3.10) implies $s < r$. The elements x^{2^s} and y^{2^s} are central with orders at most 2^{r-s}, so they lie in $\langle z^{2^s} \rangle$, where $Z(H) = \langle z \rangle$, and, for suitable i and j, xz^i and yz^j have order exactly 2^s. By replacing x and y by these elements, we can suppose that $T = \langle x, y \rangle \cong \mathcal{D}_{2^{3s}}$. Arguing as in the last part of the proof of Lemma 24, we conclude $H = TC_H(T)$ and $T \cap C_H(T) = Z(T)$ is cyclic of order 2^s. Since $Z(H) \leq C_H(T)$, the hypotheses still hold in $C_H(T)$, so we can apply induction. □

The last two results show that, with the hypotheses of Proposition 28, $N_{x^{2^r}}(1) < N_{x^{2^r}}(t)$ if and only if $G \cong \mathcal{D}_{2^{3r_1}} * \cdots * \mathcal{D}_{2^{3r_n}} * \mathcal{Q}_{2^{3r}}$, $n \geq 0$, $r_1 \leq \ldots, \leq r_n \leq r$. Notice simply that the cyclic factor of H is absorbed by $\mathcal{Q}_{2^{3r}}$.

Theorem E. *Let G be a finite 2-group of nilpotency class 2. Then $N_{x^{2^r}}$ is a character of G if and only if G has no epimorphic image isomorphic to $\mathcal{D}_{2^{3r_1}} * \cdots * \mathcal{D}_{2^{3r_n}} * \mathcal{Q}_{2^{3r}}$, $n \geq 0$, $r_1 \leq \ldots \leq r_n \leq r$.*

Proof. If G has an epimorphic image G_1 of the indicated type, then by the last remark, $N_{x^{2^r},G_1}(1) < N_{x^{2^r},G_1}(t)$, where t is the central involution in G_1, and by Proposition 21, $N_{x^{2^r}}$ is not a character of G. Conversely, if $N_{x^{2^r}}$ is not a character of G, by the same lemma, G has an epimorphic image G_1 with cyclic center such that $N_{x^{2^r},G_1}(1) < N_{x^{2^r},G_1}(t)$. We claim that Z, the center of G_1, has order 2^r (and then, again by the last remark, G_1 is the desired epimorphic image). The map $x \mapsto x^{2^r}$ cannot be a group endomorphism of G_1 since this would immediately imply that either $N_{x^{2^r},G_1}(t) = 0$ or else $N_{x^{2^r},G_1}(1) = N_{x^{2^r},G_1}(t)$. Using (3.10), we deduce that $(G_1')^{2^{r-1}} \neq 1$ and $Z^{2^{r-1}} \neq 1$, that is $|Z| \geq 2^r$. If $|Z| > 2^r$, $t = z^{2^r}$ for some $z \in Z$ and then $N_{x^{2^r},G_1}(1) = N_{x^{2^r},G_1}(t)$ because $x \mapsto xz$ maps bijectively the solutions of $x^{2^r} = 1$ to the solutions of $x^{2^r} = t$. Thus $|Z| = 2^r$ and the proof is complete. □

Chapter 4

General word fibres for p-groups of nilpotency class 2

We are interested in studying whether Amit's conjecture 1 has a positive solution when considering non-empty fibres in the class of p-groups of nilpotency class 2. We will first give some bounds and positive results towards extending Amit's conjecture for general fibres in this class of groups. The rest of the chapter will be devoted to studying this question and to giving some positive results in this direction.

4.1 Some bounds for specific words

In this section we will again consider finite p-groups of nilpotency class 2 and will study general fibre sizes for specific words. Before proceeding, we introduce a basic lemma that will be useful.

Lemma 30. *Let g be a fixed element of a group G of nilpotency class 2. Then $[g,G] = \{[g,h] \mid h \in G\}$ is a normal subgroup of G and every element of $[g,G]$ can be represented in $|C_G(g)|$ different ways in the form $[g,h]$ with $h \in G$. Hence $|[g,G]| = |G : C_G(g)|$.*

Proof. The map $h \to [g,h]$ is a homomorphism with image $[g,G]$ and kernel $C_G(g)$. □

Proposition 31. *Let G be a finite p-group of nilpotency class at most 2 and let $w \in F_k'$. Then $N_w(g) \geq |G|^{\lfloor \frac{k}{2} \rfloor}$ for any $g \in G_w$.*

Note that the approach in Theorem 10 would give a weaker bound in the case when k is even. For example, consider the word w_k which for any $k \geq 1$ will denote

$$w_k(x_1, y_1, \ldots, x_k, y_k) = [x_1, y_1] \cdots [x_k, y_k], \tag{4.1}$$

the product of k disjoint commutators. In theorem 10, we fix a tuple $(h_1, h_2, \ldots, h_k) \in G^{(k)}$ and consider the map $G^{(k)} \to G'$ given by $(g_1, g_2, \ldots, g_k) \mapsto w_k(g_1, h_1, g_2, h_2, \ldots, g_k, h_k)$ which is a group homomorphism whose kernel has size at least $|G|^k/|G'|$. In a group homomorphism all fibres have the same size. However, it may happen that for our fix tuple $(h_1, h_2, \ldots, h_k) \in G^{(k)}$, the fibre of a specific $g \in G_w$ is empty. Consequently, we can not continue with the argument used in Theorem 10 where we vary the tuple $(h_1, h_2, \ldots, h_k) \in G^{(k)}$ obtaining $|G|^{(k)}$ such maps which would give us the aimed bound. The problem here is that we don't know how many of the $|G|^k$ tuples $(h_1, h_2, \ldots, h_k)$ would give maps with non-empty fibres for g.

However, since $g \in G_w$, there exists $(a_1, b_1, \ldots, a_k, b_k) \in G^{(2k)}$ in the fibre of g. We can consider the tuple $(b_1, b_2, \ldots, b_k) \in G^{(k)}$ and the map $G^{(k)} \to G'$ given by $(g_1, g_2, \ldots, g_k) \mapsto w_k(g_1, b_1, g_2, b_2, \ldots, g_k, b_k)$ which is a group homomorphism whose kernel has size at least $|G|^k/|G'|$. The fibre of g has the same size as the kernel, and hence $N_{w_k}(g) \geq |G|^k/|G'|$, which is not as good as $N_{w_k}(g) \geq |G|^k$ obtained in Proposition 31.

Proof. Using Theorem B, without loss of generality w is of the form $\prod_{1 \leq i \leq r} [x_{2i-1}, x_{2i}]^{p^{s_i}}$ with $0 \leq s_1 \leq \cdots \leq s_r$ for some $r \leq \lfloor k/2 \rfloor$. Suppose $g \in G_w$ such that $w(a_1, \ldots, a_k) = g$ and write $w'(x_1, \ldots, x_{k-2}) = \prod_{1 \leq i \leq r-1} [x_{2i-1}, x_{2i}]^{p^{s_i}}$. If $k = 2$, $w(x, y) = [x, y]^{p^{s_1}}$ and if $w(a, b) = g$, we have that $w(a \cdot [a, G], b \cdot C_G(a)) = g$ giving $N_w(g) \geq |[a, G] \cdot |C_G(a)|| = |G|$, as we wanted to show.

Suppose now $k > 2$. Then

$$N_w(g) = \sharp\{(g_1, \ldots, g_k) \in G^{(k)} \mid w'(g_1, \ldots, g_{k-2}) = g[g_{2r}^{p^{s_r}}, g_{2r-1}]\}.$$

From Lemma 30 each element of the commutator subgroup $[g_{2r}^{p^{s_r}}, G]$ is of the form $[g_{2r}^{p^{s_r}}, g]$, and there are $|C_G(g_{2r}^{p^{s_r}})|$ choices of g giving rise to the same element. If we

write $N = [a_{2r}^{p^{sr}}, G]$, $(a_1N, \ldots, a_{2r-2}N)$ is a solution to $w' = gN$ in G/N. Hence

$$\begin{aligned} N_w(g) &\geq |C_G(a_{2r}^{p^{sr}})| \cdot \sharp\{(g_1, \ldots, g_{k-2}) \in G^{(k-2)} \mid w'(g_1, \ldots, g_{k-2}) \in gN\} \\ &= |C_G(a_{2r}^{p^{sr}})| \cdot |N|^{k-2} \cdot \sharp\{(g_1N, \ldots, g_{k-2}N) \in (G/N)^{(k-2)} \mid w'(g_1N, \ldots, g_{k-2}N) = gN\} \\ &= |C_G(a_{2r}^{p^{sr}})| \cdot |N|^{k-2} \cdot N_{w',G/N}(gN). \end{aligned}$$

We can apply the inductive hypothesis to w' in $k-2$ variables obtaining $N_{w',G/N}(gN) \geq |G/N|^{\lfloor \frac{k}{2} \rfloor - 1}$ and the result follows:

$$\begin{aligned} N_w(g) &\geq |C_G(a_{2r}^{p^{sr}})| \cdot |N|^{k-2} \cdot |G/N|^{\lfloor \frac{k}{2} \rfloor - 1} \geq |C_G(a_k^{p^{sr}})| \cdot |N|^{\lfloor \frac{k}{2} \rfloor - 1} \cdot |G|^{\lfloor \frac{k}{2} \rfloor - 1} \\ &\geq |C_G(a_k^{p^{sr}})| \cdot |N| \cdot |G|^{\lfloor \frac{k}{2} \rfloor - 1} = |G|^{1 + \lfloor \frac{k}{2} \rfloor - 1} = |G|^{\lfloor \frac{k}{2} \rfloor}. \square \end{aligned}$$

Corollary 32. *Let G be a finite p-group of nilpotency class at most 2 and consider the word w_k in $2k$ variables, then*

$$N_{w_k}(g) \geq |G|^{2k-l}$$

for $g \in G_{w_l}$, with $1 < l \leq k$.

Proof. We will use induction on k. For $l = k$, we use Proposition 31 to conclude $N_{w_k}(g) \geq |G|^k$ for any $g \in G_{w_k}$, as we wanted. By the inductive hypothesis suppose $N_{w_t}(g) \geq |G|^{2t-l}$ for $1 \leq l \leq t < k$. If $g \in G_{w_l}$, there exists $\mathbf{g} = (g_1, h_1, \ldots, g_l, h_l, 1, 1, \ldots, 1, 1)$ such that $w_k(\mathbf{g}) = g$. It gives

$$\begin{aligned} N_{w_k}(g) &= \sharp\{(g_1, h_1, \ldots, g_k, h_k) \in G^{(2k)} \mid [g_1, h_1] \cdots [g_{k-1}, h_{k-1}] = g[h_k, g_k]\} \\ &= \sum_{h_k \in G} |C_G(h_k)| \cdot \sharp\{(g_1, h_1, \ldots, g_{k-1}, h_{k-1}) \in G^{(2(k-1))} \mid \prod_{i=1}^{k-1} [g_i, h_i] \in g[h_k, G]\}. \end{aligned}$$

If we write $N_{h_k} = [h_k, G]$,

$$\begin{aligned} N_{w_k}(g) &= \textstyle\sum_{h_k \in G} |C_G(h_k)| \cdot |N_{h_k}|^{2(k-1)} \cdot \sharp\{(g_1N_{h_k}, \ldots, h_{k-1}N_{h_k}) \in (G/N_{h_k})^{(2(k-1))} \mid \prod_{i=1}^{k-1} [g_iN_{h_k}, h_iN_{h_k}] = gN_{h_k}\} \\ &= \sum_{h_k \in G} |C_G(h_k)| \cdot |N_{h_k}|^{2(k-1)} \cdot N_{w_{k-1}, G/N_{h_k}}(gN_{h_k}). \end{aligned}$$

Using induction on k, $N_{w_{k-1},G/N_{h_k}}(gN_{h_k}) \geq |G/N_{h_k}|^{2(k-1)-l}$ and the result follows:

$$\begin{aligned} N_{w_k}(g) &\geq \sum_{h_k \in G} |C_G(h_k)| \cdot |N_{h_k}|^{2(k-1)} \cdot |G/N_{h_k}|^{2(k-1)-l} \\ &= |\,G\,|^{2(k-1)-l} \sum_{h_k \in G} \frac{|G|^l}{|C_G(h_k)|^{l-1}} = |\,G\,|^{2k-1-l} \sum_{h_k \in G} \Big(\frac{|G|}{|C_G(h_k)|}\Big)^{l-1} \geq |\,G\,|^{2k-l}.\square \end{aligned}$$

From a different point of view, if we want to use character theoretical arguments, it is very useful to know $\mathrm{cd}(G) = \{\chi(1) \,|\, \chi \in \mathrm{Irr}(G)\}$, the set of degrees of irreducible complex characters of a group. The following results are deduced from [27] and will imply that any p-group having only two different character degrees satisfies Amit's conjecture 1 for a general non-empty fibre; that is, $N_{w_k}(g) \geq |G|^{2k-1}$ for any $g \in G_{w_k}$.

Lemma 33. *Let G be a finite p-group such that $\mathrm{cd}(G) = \{1, m\}$, $m > 1$. If $1 \neq g \in G'$ then,*

$$N_{w_k}(g) = \frac{|G|^{2k}}{|G'|}\Big(1 - \frac{1}{m^{2k}}\Big)$$

and

$$|G|^{2k-1} \leq N_{w_k}(g) \leq \frac{|G|^{2k}}{|G'|}\Big(1 - \frac{1}{|G : Z(G)|^k}\Big).$$

Proof. For $1 \neq g \in G_{w_k}$, using the second orthogonality relations, we have

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

Besides, noting that the number of irreducible linear characters is $|G : G'|$ and that if χ is linear, then $\chi(g) = \chi(1)$ since $G' \leq \ker \chi$, we get

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

Therefore,

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

Using Lemma 16 we deduce $N_{w_k}^{\chi} = \left(\frac{|G|}{\chi(1)}\right)^{2k-1}$ for any $\chi \in \mathrm{Irr}(G)$,

$$\begin{aligned} N_{w_k}(g) &= \sum_{\chi \in \mathrm{Irr}(G)} \left(\frac{|G|}{\chi(1)}\right)^{2k-1} \cdot \chi(g) \\ &= \sum_{\chi \in \mathrm{Irr}(G):\chi(1)=1} |G|^{2k-1} + \sum_{\chi \in \mathrm{Irr}(G):\chi(1)=m} \left(\frac{|G|}{m}\right)^{2k-1} \cdot \chi(g) \\ &= |G|^{2k-1} \cdot |G:G'| + \left(\frac{|G|}{m}\right)^{2k-1} \cdot \left(\frac{-|G:G'|}{m}\right) = \frac{|G|^{2k}}{|G'|} \cdot \left(1 - \frac{1}{m^{2k}}\right), \end{aligned}$$

showing the first result.

To obtain the lower bound, we note that since $m \geq 2$, $\left(1 - \frac{1}{m^{2k}}\right) \geq 3/4$ and since G is non-abelian $|G : G'| \geq 2$, proving that $N_{w_k}(g) \geq |G|^{2k-1}$. To get the upper bound, we only note that the character degrees cannot exceed $|G : Z(G)|^{1/2}$. □

Lemma 34. *Let G be a finite group of nilpotency class 2 and $|G'| = p$, p a prime number. Then any nonlinear irreducible character χ vanishes outside of $Z(G)$.*

Proof. Consider $g \in G \backslash Z(G)$. So there exists some $x \in G$ such that $t = [x, g] \neq 1$. Since $|G'| = p$, t is a generator of G'. Let $\chi \in \mathrm{Irr}(G)$ such that $\chi(1) \neq 1$. Then there exists a complex representation ρ affording χ, and by Lemma 2.27 in [22] we have that $\rho(t) = \epsilon I$ where $\epsilon \in \mathbb{C}$. In the case when $\epsilon = 1$, $t \in \ker \rho$ and therefore $G' \leq \ker \rho$ which is a contradiction with $G' = \bigcap\{\ker \chi \,|\, \chi \in \mathrm{Irr}(G), \chi(1) = 1\}$ (see Corollary 2.23 in [22]).

Therefore $\epsilon \neq 1$ and since

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

we obtain that $\chi(g) = 0$, and the claim holds. □

Corollary 35. *Let G be a finite group of nilpotency class 2 and $|G'| = p$, p a prime number. Then if $g \in G'$, $N_{w_k}(g) \geq |G|^{2k-1}$.*

Proof. For $g = 1$, the result is true by Frobenius [23] using that $N_{w_k}^{\chi} = \left(\frac{|G|}{\chi(1)}\right)^{2k-1}$ or following Chapter 2. From Lemma 34 we know that any nonlinear irreducible character χ vanishes outside of $Z(G)$ and putting this together with Corollary 2.30

in [22], this implies that $\chi(1)^2 = |G : Z(G)|$. Therefore G has just two irreducible complex character degrees, i.e. $\mathrm{cd}(G) = \{1, |G : Z(G)|^{1/2}\}$. Now the assertion holds using Lemma 33. □

4.2 p-groups with central Frattini subgroup

The previous section served as a motivation to try to extend Amit's conjecture to general fibres in the class of finite groups of nilpotency class 2. Recall that for a finite p-group, the Frattini subgroup of G is defined as $\Phi(G) = G^p[G, G]$ and it is the set of non-generating elements of G. In this section we will consider non-abelian p-groups G such that $\Phi(G) \subseteq Z(G)$. This implies, G has nilpotency class 2 and $G/Z(G)$ is elementary abelian. Consequently, the derived subgroup $G' = [G, G]$ is elementary abelian. In particular, we will show that Amit's conjecture is true for the word $w_k = \prod_{i=1}^{k}[x_i, y_i]$ if $k \geq d_0 = \lfloor d/2 \rfloor$, where d is the number of a (minimal) generating set of G and G is the free d-generated group of exponent p and nilpotency class 2.

4.2.1 Words in the exterior square of a vector space

Amit's conjecture for free p-groups of exponent p and nilpotency class 2 leads naturally to an analogous problem in the setting of the exterior square of a vector space. Thus in this section V will denote a d-dimensional vector space over a finite field $K = \mathbb{F}_q$, although we will be primarily interested in the case when $q = p$ is a prime number. To make this section self-contained, we have included all the details although they can be obvious for experts in the field.

We fix a basis $\{e_1, \ldots, e_d\}$ of V and construct as usual the exterior square $\bigwedge^2 = \bigwedge^2 V$, which is independent of the basis. As defined in, the product of k disjoint commutators will be denoted

$$w_k(x_1, \ldots, x_{2k}) = [x_1, x_2] \cdots [x_{2k-1}, x_{2k}].$$

When considering the word $w_k(x_1, \ldots, x_{2k})$ in the exterior square, the word will be

re-interpreted as

$$w_k(v_1, \dots, v_{2k}) = v_1 \wedge v_2 + \cdots + v_{2k-1} \wedge v_{2k},$$

for any $v_i \in V$. It will be clear depending on the context which expression we will be using.

Then, for a fixed $\omega \in \bigwedge^2$ and $k \geq 0$, it is natural to consider the number $N_{w_k}(\omega) = N_{w_k,V}(\omega)$ of solutions $(v_1, \dots, v_{2k}) \in V^{(2k)}$ of the equation

$$w_k(v_1, \dots, v_{2k}) = v_1 \wedge v_2 + \cdots + v_{2k-1} \wedge v_{2k} = \omega.$$

The set of values of w_k, that is, the set $\{w_k(v_1, \dots, v_{2k}) \mid v_i \in V\} \subseteq \bigwedge^2$ will be denoted $(\bigwedge^2 V)_{w_k}$, or simply $\bigwedge^2_{w_k}$. Our goal is to find a lower bound for the numbers $N_{w_k}(\omega)$ when $\omega \in \bigwedge^2_{w_k}$. Note that if $k \leq l$, $\bigwedge^2_{w_k} \subseteq \bigwedge^2_{w_l}$.

Definition 36. For any $r \geq 1$, we will denote $\bigwedge^{2*}_{w_k} = \bigwedge^2_{w_k} \setminus \bigwedge^2_{w_{k-1}}$ and we will say that any element $\omega \in \bigwedge^{2*}_{w_r}$ has *rank* r. We shall write $\operatorname{rk}\omega$ for this number.

It is almost immediate from the definition of $\bigwedge^2$ that any element has rank at most $d-1$ but in fact this number can be reduced to $d_0 = \lfloor d/2 \rfloor$ (the integer part of $d/2$; d_0 will always have this meaning in the sequel), as we shall see now.

There is a one-to-one correspondence between $\bigwedge^2$ and $\mathcal{A}_d$, the set of $d \times d$ antisymmetric matrices over the field K, given by $\sum_{1 \leq i < j \leq d} a_{ij}(e_i \wedge e_j) \mapsto A$, where $A \in \mathcal{A}_d$ has entries a_{ij} for $1 \leq i < j \leq d$. Given $2k$ vectors $v_1, \dots, v_{2k} \in V$ we consider the $2k \times d$ coordinate matrix X. Then a routine computation shows that the antisymmetric matrix corresponding to $\omega = w_k(v_1, \dots, v_{2k}) \in \bigwedge^2$ is $X^t J_k X$, where the superscript t indicates matrix transposition and J_k is the $2k \times 2k$ block-diagonal matrix with repeated diagonal block $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. The next result now follows easily:

Proposition 37. *Let $\omega = w_k(v_1, \dots, v_{2k}) \in \bigwedge^2$ and $A \in \mathcal{A}_d$ the corresponding antisymmetric matrix. Then*

(i) $\operatorname{rk} A = 2 \operatorname{rk}\omega$. *In particular any element in $\bigwedge^2$ has rank at most d_0.*

(ii) $\operatorname{rk}\omega = k$ *if and only if $\{v_1, \dots, v_{2k}\}$ is linearly independent.*

Proof. For (i) it suffices to show that $\operatorname{rk}\omega \leq k$ if and only if $\operatorname{rk} A \leq 2k$. As shown before, if $\omega \in \bigwedge^2_{w_k}$, $A = X^t J_k X$ for some $2k \times d$ matrix X, whence $\operatorname{rk} A \leq \operatorname{rk} X \leq 2k$. Conversely, if $\operatorname{rk} A = 2r \leq 2k$ then, by elementary linear algebra, $A = P^t \left(\begin{smallmatrix} J_r & 0 \\ 0 & 0 \end{smallmatrix}\right) P$ for some invertible $d \times d$ matrix P, and so $A = X^t J_r X$, where X is the $2r \times d$ matrix formed by the first $2r$ rows of P. Therefore, using again the comment above, $\operatorname{rk}\omega \leq 2r \leq 2k$.

For (ii) we write again $A = X^t J_k X$, where X is the coordinate matrix of $v_1, \ldots, v_{2k}$. Since $\operatorname{rk} A = 2\operatorname{rk}\omega$ and $\operatorname{rk} X \leq 2k$, it is clear that if ω has rank k, X must have maximal rank $2k$, that is, the vectors $v_1, \ldots, v_{2k}$ are linearly independent. Conversely, if X has rank $2k$, we can add rows to X to obtain an invertible $d \times d$ matrix P. Then $A = P^t \left(\begin{smallmatrix} J_k & 0 \\ 0 & 0 \end{smallmatrix}\right) P$ and, since P is invertible, the rank of A is $2k$. □

The group $\mathrm{GL}(V)$ acts in a natural way on $\bigwedge^2$ preserving the rank. Notice that Proposition 37 (ii) implies the converse, that elements of the same rank are in the same orbit, or equivalently, that the orbits of this action are the sets $\bigwedge^{2\,*}_{w_r}$, $0 \leq r \leq d_0$. In particular, since the functions N_{w_k} are constant on the orbits of $\mathrm{GL}(V)$, $N_{w_k}(\omega) = N_{w_k}(\omega')$ for elements ω and ω' of the same rank.

Proposition 37 and some elementary matrix computations yield the exact value of $N_{w_r}(\omega)$ for the elements $\omega \in \bigwedge^2$ of rank r.

Corollary 38. *Let $\omega \in \bigwedge^2$ be an element of rank r. Then $N_{w_r}(\omega) = |\operatorname{Sp}_{2r}(K)| = q^{r^2} \prod_{1 \leq i \leq r}(q^{2i} - 1)$, where $\operatorname{Sp}_{2r}(K)$ is the Symplectic group of degree $2r$ over K.*

Proof. We can assume that $\omega = w_r(e_1, \ldots, e_{2r})$. Then $N_{w_r}(\omega)$ is exactly the number of $2r \times d$ matrices X such that $\left(\begin{smallmatrix} J_r & 0 \\ 0 & 0 \end{smallmatrix}\right) = X^t J_r X$. Writing $X = (X_1 | X_2)$ with X_1 of size $2r \times 2r$ and X_2 of size $2r \times (d - 2r)$, this relation is equivalent to $X_1^t J_r X_1 = J_r$, $X_1^t J_r X_2 = 0$ and $X_2^t J_r X_2 = 0$. But then this means that X_1 is a symplectic matrix and $X_2 = 0$, so the result follows. □

Next we will show that $N_{w_k}(\omega) \geq N_{w_k}(\omega')$ if $k \leq d_0$ and $\operatorname{rk}\omega \leq \operatorname{rk}\omega'$. This means that if $\omega \in \bigwedge^2_{w_k}$, that is ω has rank less than or equal to k, $N_{w_k}(\omega) \geq N_{w_k}(\omega')$ with ω' of rank k. Then we can use the last corollary to conclude the following result.

Theorem 39. *Let $k \leq d_0$ and $\omega \in \bigwedge^2_{w_k}$. Then*

$$N_{w_k}(\omega) \geq |\operatorname{Sp}_{2k}(K)| = q^{k^2} \prod_{1 \leq i \leq k} (q^{2i} - 1).$$

We fix $k \leq d_0$ and elements ω_r of rank r for $0 \leq r \leq d_0$. We have to show that

$$N_{w_k}(\omega_r) \geq N_{w_k}(\omega_{r+1}), \text{ if } 0 \leq r < k. \tag{4.2}$$

Notice that for $r \geq k$, (4.2) says nothing since $N_{w_k}(\omega_{r+1}) = 0$. We argue by induction on k. If $k = 1$, $r = 0$ and we have to argue that $N_{w_1}(0) \geq N_{w_1}(\omega_1) = q(q^2 - 1)$ (this value is obtained from Corollary 38). But $N_{w_1}(0) = q^{d+1} + q^d - q$ (because $u \wedge v = 0$ if and only if $\{u, v\}$ is linearly dependent) and $d = 2d_0 \geq 2k = 2$, so the inequality follows easily.

Let $k \geq 2$. We can write $N_{w_k} = N_{w_1} * N_{w_{k-1}}$ as the convolution of the functions N_{w_1} and $N_{w_{k-1}}$. Since the functions N_{w_i} are constant on the sets $\bigwedge^{2*}_{w_r}$, we have then

$$N_{w_k}(\omega_r) = N_{w_1}(0)N_{w_{k-1}}(\omega_r) + \sum_{i=0}^{d_0} m_{i,r} N_{w_1}(\omega_1) N_{w_{k-1}}(\omega_i),$$

where $m_{i,r} = |\{(\omega', \omega'') \in \bigwedge^{2*}_{w_1} \times \bigwedge^{2*}_{w_i} \mid \omega' + \omega'' = \omega_r\}|$. There is a well-known formula for $|\bigwedge^{2*}_{w_r}|$, the number of $d \times d$ antisymmetric matrices of rank $2r$, (see for instance Theorem 3 in [28]):

$$|\bigwedge^{2*}_{w_r}| = q^{r(r-1)} \frac{\sum_{i=0}^{2r-1}(q^{d-i} - 1)}{\sum_{i=0}^{r-1}(q^{2i} - 1)}. \tag{4.3}$$

If ω' has rank 1 and ω'' rank i, then the rank of $\omega' + \omega''$ is $i - 1$, i or $i + 1$ (this is clear if one thinks in terms of antisymmetric matrices: the sum of two antisymmetric matrices with ranks 2 and $2i$ is $2(i-1)$, $2i$ or $2(i+1)$). Thus

$$\begin{aligned} N_{w_k}(\omega_r) \;=\; & N_{w_1}(0)N_{w_{k-1}}(\omega_r) + N_{w_1}(\omega_1)\big(m_{r-1,r}N_{w_{k-1}}(\omega_{r-1}) + \\ & m_{r,r}N_{w_{k-1}}(\omega_r) + m_{r+1,r}N_{w_{k-1}}(\omega_{r+1})\big), \end{aligned} \tag{4.4}$$

(of course we have to interpret $m_{-1,0} = m_{d_0+1,d_0} = 0$).

Next we compute the numbers $m_{i,r}$.

Lemma 40. *Let $0 \leq r \leq d_0$. Then*

$$m_{r-1,r} \;=\; \frac{q^{2(r-1)}(q^{2r} - 1)}{q^2 - 1},$$

$$\begin{aligned} m_{r,r} &= \frac{(q^d-1)(q^{d-1}-1)}{q^2-1} - m_{r-1,r} - m_{r+1,r}, \\ m_{r+1,r} &= \frac{q^{4r}(q^{d-2r}-1)(q^{d-2r-1}-1)}{q^2-1}. \end{aligned}$$

Proof. We begin by proving the formula for $m_{r+1,r}$. This is the number of pairs $(\omega', \omega'') \in \bigwedge^{2*}_{w_1} \times \bigwedge^{2*}_{w_{r+1}}$ such that $\omega' + \omega'' = \omega_r$, which is the number of elements ω' of rank 1 such that $\omega' - \omega_r$ has rank $r+1$. Writing $\omega' = u \wedge v$ and $\omega_r = w_r(v_1, \ldots, v_{2r})$, by Proposition 37 (ii), this happens if and only if $\{u, v, v_1, \ldots, v_{2r}\}$ is linearly independent or, equivalently, $\{\overline{u}, \overline{v}\}$ is linearly independent in $V/\langle v_1, \ldots, v_{2r}\rangle$. Thus the number of pairs (u, v) is $q^{4r}(q^{d-2r}-1)(q^{d-2r}-q)$ and we get the desired number $m_{r+1,r}$ by dividing this number by $N_{w_1}(\omega_1) = q(q^2-1)$.

To compute $m_{r-1,r}$ we count the number of triplets $(\omega', \omega'', \omega''') \in \bigwedge^{2*}_{w_1} \times \bigwedge^{2*}_{w_{r-1}} \times \bigwedge^{2*}_{w_r}$ such that $\omega' + \omega'' = \omega'''$. This number is the number of pairs (ω', ω'') such that $\omega' + \omega'' \in \bigwedge^{2*}_{w_r}$ and also the number of pairs (ω', ω''') such that $\omega' + \omega''' \in \bigwedge^{2*}_{w_{r-1}}$. Therefore $|\bigwedge^{2*}_{w_r}| m_{r-1,r} = |\bigwedge^{2*}_{w_{r-1}}| m_{r,r-1}$. Now using the formula in (4.3) it turns out that $|\bigwedge^{2*}_{w_{r-1}}|/|\bigwedge^{2*}_{w_r}| = q^{-2(r-1)}(q^{2r}-1)/(q^{d-2r+2}-1)(q^{d-2r+1}-1)$. Finally we use the formula for $m_{r,r-1}$ that we have computed before.

For the second formula we note again that if $\omega' + \omega'' = \omega_r$ with ω' of rank 1, then ω'' has rank $r-1$, r or $r+1$, thus $m_{r-1,r}+m_{r,r}+m_{r+1,r}$ is the number of pairs $(\omega', \omega'') \in \bigwedge^{2*}_{w_1} \times \bigwedge^{2}$ such that $\omega' + \omega'' = \omega_r$. This number is $|\bigwedge^{2*}_{w_1}| = (q^d-1)(q^{d-1}-1)/(q^2-1)$, the number of rank 2 antisymmetric matrices (again, by the formula in [28]). □

Now using the second formula in Lemma 40 we re-write (4.4):

$$\begin{aligned} N_{w_k}(\omega_r) &= N_{w_1}(0)N_{w_{k-1}}(\omega_r) + N_{w_1}(\omega_1)m_{r-1,r}\big(N_{w_{k-1}}(\omega_{r-1}) - N_{w_{k-1}}(\omega_r)\big) \\ &+N_{w_1}(\omega_1)m_{r+1,r}\big(N_{w_{k-1}}(\omega_{r+1}) - N_{w_{k-1}}(\omega_r)\big) + N_{w_1}(\omega_1)|\bigwedge^{2*}_{w_1}| N_{w_{k-1}}(\omega_r). \quad (4.5) \end{aligned}$$

Using (4.5), we write the difference $N_{w_k}(\omega_r) - N_{w_k}(\omega_{r+1})$ in terms of $N_{w_{k-1}}$ and N_{w_1}:

$$N_{w_k}(\omega_r) - N_{w_k}(\omega_{r+1}) = \sum_{i=r-1}^{r+1} A_{k,i}\big(N_{w_{k-1}}(\omega_i) - N_{w_{k-1}}(\omega_{i+1})\big), \quad (4.6)$$

such that

$$\begin{aligned} A_{k,r-1} &= N_{w_1}(\omega_1)m_{r-1,r}\,, \\ A_{k,r} &= N_{w_1}(0) + N_{w_1}(\omega_1)(|\textstyle\bigwedge_{w_1}^{2*}| - m_{r+1,r} - m_{r,r+1})\,, \\ A_{k,r+1} &= N_{w_1}(\omega_1)m_{r+2,r+1}\,. \end{aligned}$$

By the inductive hypothesis the three differences between the values of $N_{w_{k-1}}$ in (4.6) are non-negative, so (4.2) will follow if we show that $A_{k,r} \geq 0$. Using Lemma 40 and the known formulas for $N_{w_1}(0)$ and $N_{w_1}(\omega_1)$, one gets $A_{k,r} = p^{2r+1}(p^d + p^{r-1} - p^{2r+2} - p^{2r} + 1)$. But $r < d_0$, that is $d \geq 2r+2$; therefore $A_{k,r} \geq p^{2r+1}(p^{2r}(p-1)+1)$, which is certainly positive.

4.2.2 Amit's conjecture for general fibres

Now putting all the information from Subsection 4.2.1 together, we will make the last steps to prove Theorem 41 and F which answers Amit's conjecture to any non-empty fibre in some special cases.

Let $V = G/\Phi(G)$ be viewed as an $\mathbb{F}_p$-vector space, and fix a basis $\overline{x}_1, \ldots, \overline{x}_d$. There is a natural surjective linear map π from $\bigwedge^2 V$ to G' mapping $\overline{x}_i \wedge \overline{x}_j$ to $[x_i, x_j]$, $1 \leq i < j \leq d$. Of course π maps $\bigwedge_{w_k}^2$ onto G_{w_k}, so it follows from Proposition 37 (i) that $G_{w_k} = G'$ for $k \geq d_0$. Now it is easy to show that if Amit's conjecture is true for w_{d_0} it is also true for any w_k with $k > d_0$. Indeed we write $N_{w_k} = N_{w_{d_0}} * N_{w_{k-d_0}}$ and notice that, since we are assuming that $N_{w_{d_0}}(x) \geq |G|^{2d_0-1}$ for any $x \in G'$, if $g \in G'$,

$$\begin{aligned} N_{w_k}(g) &= \sum_{y \in G_{w_{k-d_0}}} N_{w_{d_0}}(gy^{-1})N_{w_{k-d_0}}(y) \geq |G|^{2d_0-1} \sum_{y \in G_{w_{k-d_0}}} N_{w_{k-d_0}}(y) \\ &= |G|^{2d_0-1}|G|^{2(k-d_0)} = |G|^{2k-1}. \end{aligned}$$

So in order to prove Amit's conjecture for w_k we can always assume that $1 \leq k \leq d_0$.

It is clear that if $g \in G'$ and $\pi(\omega) = g$, the solutions of $w_k(v_1, \ldots, v_{2k}) = \omega$ in V are lifted to solutions of $w_k(x_1, \ldots, x_{2k}) = g$ in G and of course, all solutions of the equation in G occur in this way, so

$$N_{w_k}(g) = |\Phi(G)|^{2k} \sum_{\omega \in \pi^{-1}(g)} N_{w_k,V}(\omega)$$

and Amit's conjecture for general fibres which says that $N_w(g) \geq |G|^{k-1}$ for any $g \in G_w$ and w any word in k variables, can be written now as

$$|\Phi(G)| \sum_{\omega \in \pi^{-1}(g)} N_{w_k,V}(\omega) \geq |G : \Phi(G)|^{2k-1} = p^{d(2k-1)} \tag{4.7}$$

for $g \in G_{w_k}$. Only $\omega \in \pi^{-1}(g) \cap \bigwedge^2_{w_k}$ will contribute to the sum in (4.7) and for them we can use Theorem 39 to estimate $N_{w_k,V}(\omega)$:

$$N_{w_k,V}(\omega) \geq p^{k^2} \prod_{i=1}^{k} (p^{2i} - 1) > p^{k^2} \prod_{i=1}^{k} p^{2i-1} = p^{2k^2}.$$

Since $|G'| = p^{d(d-1)/2}/|\ker \pi| \leq |\Phi(G)|$, the inequality

$$p^{\frac{d(d-1)}{2} + 2k^2 - d(2k-1)} |\pi^{-1}(g) \cap \textstyle\bigwedge^2_{w_k}| \geq |\ker \pi| \tag{4.8}$$

implies (4.7). If $k = d_0$, $|\pi^{-1}(g) \cap \bigwedge^2_{w_k}| = |\pi^{-1}(g)| = |\ker \pi|$ and (4.8) holds because the exponent of p is non-negative. Thus we have the following result.

Theorem 41. *Let G be a d-generated p-group with $\Phi(G) \leq Z(G)$. Then for any $k \geq \lfloor d/2 \rfloor$ and $g \in G'$, $N_{w_k}(g) \geq |G|^{2k-1}$.*

Another situation in which $|\pi^{-1}(g) \cap \bigwedge^2_{w_k}| = |\ker \pi|$ is when π is an isomorphism, so we also have the following result.

Theorem F. *Let G be a d-generated p-group with $\Phi(G) \leq Z(G)$ and $|G'| = p^{d(d-1)/2}$. Then for any $g \in G_{w_k}$, $N_{w_k}(g) \geq |G|^{2k-1}$.*

Notice that the last theorem applies in particular to the free p-groups of nilpotency class 2 and exponent p.

Chapter 5

p-groups of nilpotency class $c \geq 3$

In the previous chapters, we focused on p-groups of nilpotency class 2 for which we proved Amit's conjecture. We also gave some evidence that the conjecture might hold for a general non-empty fibre in this setting. More generally, we showed that for any word w, N_w is a generalized character and if p is odd, even something stronger; that N_w is a genuine character. Being able to say anything about Amit's conjecture in the setting of finite p-groups of nilpotency class higher than 2 seems unapproachable at this point. However, a good start to show that the behaviour might be different in these cases will be showing that N_w will not be a generalized character in general. We will give some examples in this direction and hence we might expect a different outcome also regarding Amit's conjecture.

5.1 Smallest p-groups for which N_{x^p} is not a character

The simplest example of a p-group for which N_w is not a character is $\mathcal{Q}_8$, the quaternion group of order 8, and the word $w = x^2$. For $G = \mathcal{Q}_8$, note that $G_{x^2} = \{1, z\}$ where z is the unique involution. $N_{x^2,G}(1) = 2$ whereas $N_{x^2,G}(z) = 6$, and Lemma 14 implies that N_w is not a character. This is the smallest p-group for which N_{x^p} is not a character when $p = 2$. For odd primes p, we will construct the smallest

p-groups satisfying this property. Recall that it is a well-known result that in general the functions N_{x^n} are generalized characters (see Problem 4.7 in [22]).

Let p any odd prime now. We know that if G is regular, then N_{x^p} is the regular character of G/G^p. Consequently, in order to find groups for which N_{x^p} is not a character, we need to consider non-regular p-groups of order at least p^{p+1}. We will construct a non-regular p-group G of minimal order; that is, of order p^{p+1}, for which N_{x^p} is not a character. Note that a non-regular p-group of minimal order has nilpotency class p. See Section 0.2 for more details on regular groups.

Proposition G. *For any odd prime p, N_{x^p} is not a character of*

$$G = \langle g_1, \ldots, g_{p-1} \rangle \rtimes \langle g_p \rangle / \langle g_{p-1}^p g_p^{-p} \rangle$$

where $\langle g_1, \ldots, g_{p-1} \rangle \cong C_p \times \cdots \times C_p \times C_{p^2}$, $\langle g_p \rangle \cong C_{p^2}$ and $g_i^{g_p} = g_i g_{i+1}$, $1 \leq i < p-2$, $g_{p-2}^{g_p} = g_{p-2} g_{p-1}^p$ and $g_{p-1}^{g_p} = g_{p-1} g_1^{-1}$.

Proof. First note that G has order p^{p+1}. In order to show that G is non-regular, we observe that $|G : \Omega(G)| \neq |\mho(G)|$ since $\Omega(G) = \langle g_1, g_2, \ldots, g_{p-1}^{-p} \rangle$ and $\mho(G) = \langle g_p^p \rangle$. From one side, we note that $N_{x^p}(1) = |\Omega(G)| = p^{p-1}$. From the other hand, since for any non-trivial element $z \in \mho(G) = Z(G)$, $N_{x_p}(z)$ have the same size, one gets $N_{x_p}(z) = p^p + p^{p-1}$. Hence, by Lemma 14, we show that N_{x^p} is not a character of G. □

5.2 p-group and P. Hall's conjecture

In the previous section our example was a word in only one variable. In this section on the other hand, we will focus on words with at least two variables. There are examples of groups G and words w where $N_{w,G}$ is not a generalized character, even among nilpotent groups. For non-solvable examples, one can take $G = \mathrm{PSL}_2(11)$

and the 2-Engel word $w = [x, y, y]$. Another example with the same group can be obtained with the word $w = x^2y^2xy^{-1}$ and the two characters of degree 12 have coefficients $7 \pm \sqrt{5}$, see Section 2.1 in [13]. Using the computing system [14] one can check that the coefficients N_w^χ for the two irreducible characters χ of degree 12 are $305 \pm 23\sqrt{5}$. More examples can be obtained using the following result by Lubotzky (see Theorem 1 in [15]): if G is a simple group and $1 \in A \subseteq G$ is a subset invariant under the group of automorphisms of G, then $A = G_w$ for some word w in two variables. Notice that if A contains an element a such that $a^i \notin A$, for some i coprime with the order of a, then $N_w(a^i) = 0$ but $N_w(a) \neq 0$, something that cannot happen if N_w is a generalized character. This proof, while effective, does not give a useful description to build such a word w.

5.2.1 P. Hall's conjecture

We present this section to motivate the fact that we shouldn't expect N_w to be a generalized character for general p-groups. For this, we will introduce the concept of conciseness and also talk about P. Hall's conjecture.

A word w is called *concise* in G if whenever G_w is finite, it always follows that the verbal subgroup $w(G)$ is finite. More generally, a word w is said to be concise in a class of groups $\mathcal{X}$ if whenever the set of w-values is finite for a group $G \in \mathcal{X}$, it always follows that $w(G)$ is finite. A word w is said to be *boundedly concise* in a class of groups $\mathcal{X}$ if for every integer m there exists a number $\nu = \nu(\mathcal{X}, w, m)$ such that whenever $|G_w| \leq m$ for a group $G \in \mathcal{X}$, it always follows that $|w(G)| \leq \nu$.

P. Hall asked whether every word is concise (see [17]):

Question 3 (P.Hall)**.** *Let G be a group and w a word in k variables. If $|G_w| < \infty$,*

is $|w(G)| < \infty$*?*

S. Ivanov [16] answered this question for arbitrary groups in the negative. He constructed a group H and a word $w(x, y) \in F_2$ such that $w(H)$ is infinite cyclic, but $w(x, y)$ has only one non-trivial value in H. Ivanov's example is not residually finite and it is still an open problem whether every word is concise in the class of **residually finite groups**. More information about this topic can be found in [29] and [17]. Recall that G is a residually finite group if for any $g \in G$ there exists a homomorphism f from G to a finite group H such that $f(g) \neq 1$. Examples of groups that are residually finite are finite groups, free groups and finitely generated nilpotent groups. Subgroups of residually finite groups are residually finite, and direct products of residually finite groups are residually finite. Any inverse limit of residually finite groups is residually finite. In particular, all profinite groups are residually finite.

A word w is *rational* if for any $g \in G$, $N_w(g) = N_w(g^e)$ for every finite group G and for every e relatively prime to $|G|$. Note that this means that N_w is a generalized character (see Corollary 13). We say that w is *weakly-rational* 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 (note that the e-th power map is a bijection on G). Lemma 1 in [17] gives an alternative characterisation for rational and weakly-rational words:

Lemma 42. *The word w is weakly rational if and only if for every finite group G with $g \in G_w$, $g^e \in G_w$ whenever e is relatively prime to the order of g. The word w is rational if and only if in every finite group G, $N_w(g) = N_w(g^e)$ for every $g \in G$ and every e relatively prime to the order of g.*

Clearly rational implies weakly rational. It is shown in [17] that if w is a weakly-rational word and G is a residually finite group in which w has at most m values, then the order of $w(G)$ is m-bounded; i.e. w is concise in the class of residually finite

groups. Pro-p groups are residually finite groups. If we assume that for any finite p-group and any word w the class function N_w is a generalised character, this would imply that any word is concise in the family of pro-p groups, which is not expected. Hence looking for finite p-groups for which N_w is not a generalised character makes sense.

5.2.2 Example of a p-group where N_w is not a generalized character

Some examples of p-groups for which N_w is not a generalized character are provided by the free p-groups of nilpotency class 4 and exponent p. This settles in the negative a question of Parzanchevski [18] who asked if the functions N_w were always generalized characters for solvable or nilpotent groups.

Proposition H. *Let G be the rank 2 free p-group of nilpotency class 4, exponent p with $p > 2$ and $p \equiv 1 \pmod 4$ and let $w = [x, y, x, y]$. Then N_w is not a generalized character of G.*

Proof. Using the Lazard correspondence (see details in [30], Chaper 10.2), the Hausdorff Formula and its inverse set up a correspondence between p-group of class nilpotency class less than p and lie rings of nilpotency class less than p whose additive group is a finite p-group. The correspondence preserves invariants such as the orders and the nilpotency classes of the objects involved. Consequently, we can work with the elements in the Lie ring $L(G)$ to prove our result.

We realize these nilpotent groups, as $1 + J$, where $J = I/I^4$ and I is the ideal generated by X and Y in the algebra of polynomials in the non-commuting indeterminates X and Y with coefficients in $\mathbb{F}_p$. If $x = 1+X$ and $y = 1+Y$ and $u = [x, y, x, y]$, then certainly $u \in G_w$ but we claim that if i is not a quadratic residue modulo p,

then $u^i \notin G_w$ (so $N_w(u) \neq 0$ but $N_w(u^i) = 0$). For $p > 3$, $\gamma_4(G) = 1 + \gamma_4(J)$, where $\gamma_4(J)$ is the fourth term in the descending central series of the Lie algebra J, (see [30, Chapter 10.2]). Now $u^i \in G_w$ if and only if

$$i[X, Y, X, Y] = [aX + bY, cX + dY, aX + bY, cX + dY]$$

for some $a, b, c, d \in \mathbb{F}_p$. Or equivalently, the following system has solutions $a, b, c, d \in \mathbb{F}_p$ such that

$$\begin{cases} ac(ad - bc) \equiv 0 \pmod{p} \\ bd(ad - bc) \equiv 0 \pmod{p} \\ (ad + bc)(ad - bc) \equiv i \pmod{p}. \end{cases}$$

One can check that this system has no solution if i is not a quadratic residue modulo p and hence $N_w(u) \neq 0$ and $N_w(u^i) = 0$ implying that N_w is not a generalized character of G. □

Chapter 6

Fibres in pro-p groups

6.1 Introduction

Let G be a pro-p group and w a word in k variables. For any $g \in G$, we can consider $S_w(g)$, the fibre of g in $G^{(k)}$. In the previous chapters, we considered finite p-groups and could study the fibre sizes. Besides we noted that N_w is a class function in G and in the cases when N_w is a character, we showed that $S_w(1)$ is the maximum fibre concluding that $N_w(1) \geq |G|^{k-1}$ (see Chapter 3). In this chapter, we want to study 'how big' a word fibre is in a pro-p group. We want to study whether a similar conjecture to Amit's in finite nilpotent groups can be expected in pro-p groups. However, we need a way to measure the fibres.

If we consider G a compact topological group, then G has a left Haar measure, which is a Borel measure μ such that $\mu(U) > 0$ for each non-empty open set U of G. Observe that $\mu(E) = \mu(gE)$ for each Borel set E of G and any $g \in G$. Also note that μ is unique if we impose the normalization condition $\mu(G) = 1$. On $G^{(k)}$, we impose $\mu^{(k)}$ the product measure. Note that $S_w(g) = f_w^{-1}(g)$ where $f_w : G^{(k)} \to G$ is a continuous function. Hence $S_w(g)$ is closed and hence measurable. If we view $\mu^{(k)}$

as a probability measure, then

$$P_w(g) = \mu^{(k)}(S_w(g)),$$

were $P_w(g)$ is the probability that a random tuple $\mathbf{g} = (g_1, \ldots, g_k) \in G^{(k)}$ satisfies $w(\mathbf{g}) = g$. If we consider $w = [x, y]$, N_w is a character for any finite group G. What is more, from [31], we know that $P_{[x,y]}(1) \leq 5/8$ for any finite non-abelian group G as well as for any non-abelian compact topological group. Furthermore, for non-abelian finite p-groups, $P_{[x,y]}(1) \leq (p^2 + p - 1)/p^3$.

It seems natural to want to measure the fibres of G with this measure but for most of the cases the Haar measure of subsets is 0. Consequently, if we want to compare somehow the size of a subset with the whole group we will have to construct another tool to do it. Let G be now a finitely generated pro-p group. While there is the canonical measure on pro-p groups, there is no canonical metric. We saw at the Preliminaries that every filtration (namely, descending chain of normal subgroups which form a base for the neighbourhoods of the identity) $\{G_n\}$ of G, gives rise to an invariant metric on G by setting $d(x, y) = \inf\{|G : G_n|^{-1} \,|\, xy^{-1} \in G_n\}$ sine $|G| = \infty$. Besides, every subset S of a metric space has a well defined Hausdorff dimension which is denoted by $\mathrm{hdim}(S)$. The aim in the following sections will be to use the Hausdorff dimension as the means to measure the size of the fibres $S_w(g)$ in $G^{(k)}$.

For any word w in k variables, using the definition 0.4 introduced at the Preliminaries, the dimension of the closed subset $S_w(1)$ of a finitely generated pro-p group G with a filtration $\{G_n\}$ is

$$\mathrm{Dim}_{\{G_n\}}(S_w(1)) = \liminf_{n\to\infty} \frac{\log_p |S_w(1)_{\pi_n^{(k)}}|}{\log_p |G^{(k)}_{\pi_n^{(k)}}|} = \liminf_{n\to\infty} \frac{\log_p |S_w(1)G_n^{(k)}/G_n^{(k)}|}{\log_p |(G/G_n)^{(k)}|}. \qquad (6.1)$$

Suppose we could show that for some word w in k variables, N_w is a character for

all finite p-groups. Using Lemma 14, we deduce $|S_{w,(G/G_n)^{(k)}}| \geq |G/G_n|^{k-1}$. Note this would not be enough to show $|S_w(1)_{\pi_n^{(k)}}| \geq |G/G_n|^{k-1}$ since $S_w(1)_{\pi_n^{(k)}} \subseteq S_{w,(G/G_n)^{(k)}}(\bar{1})$. However, can we find another approach to show that for any finitely generated pro-p group G with the natural filtration $\{G_n\} = \{G^{p^n}\}_{n\in\mathbb{N}}$,

$$\mathrm{Dim}_{\{G_n\}} S_w(1) \geq (k-1)/k? \tag{6.2}$$

In the following sections, we will discuss this question for free pro-p groups of finite rank and for p-adic analytic groups.

6.2 Free pro-p groups

Free groups play an important role in pro-p group theory as in abstract group theory. Free pro-p groups are defined, like free abstract groups, by a universal property, and epimorphism from them provide a useful means for studying arbitrary pro-p groups.

Let L be the free pro-p group on d generators. Before proceeding recall the following results:

Theorem 43 ([32], Corollary 7.7.5; [33], Chap. I, Corollary 3)**.** *All closed subgroup of a free pro-p groups are free pro-p.*

Theorem 44 ([8], D6 Lemma; [33], Chap. I, Proposition 24)**.** *Every generating set of a free pro-p group contains a free basis.*

Let $\{L_n\}_{n\geq 1}$ be the dimension subgroups of L; this is the fastest descending chain of open normal subgroups of L such that

$$[L_n, L] \leq L_{n+1}, \ L_n^p \leq L_{pn}$$

for each n. Let w be a word in k variables. As defined in (0.3) at the Preliminaries,

the dimension of the closed subset $S_w(1)$ of $L^{(k)}$ using this filtration is

$$\mathrm{Dim}_{\{L_n\}} S_w(1) = \liminf_{n\to\infty} \frac{\log_p |S_w(1)_{\pi_n}|}{\log_p |L^{(k)}_{\pi_n}|}.$$

Note that for any closed set $S \subseteq L$, since $|(S^{*k})_{\pi_n^{(k)}}| \leq |S_{\pi_n}|^k$ for any $k \in \mathbb{N}$, then $\mathrm{Dim}(S^{*k}) \leq k \cdot \mathrm{Dim}\, S$.

We will show that there exist words w in k variables for which

$$\mathrm{Dim}_{\{L_n\}} S_w(1) < \frac{k-1}{k}.$$

Definition 45. The *rank* of a free pro-p group L is the minimal cardinality of a set of generators for L.

For any topological group G, the minimal cardinality of a topological generating set for G is denoted by $d(G)$. Note also that $d(G)$ is also the dimension of $G/\Phi(G)$ as a vector space. In general, for a finitely generated pro-p group, $\mathrm{rk}\, G \geq d(G)$. If G is also powerful, then it is shown in Theorem 3.8 in [8] that $\mathrm{rk}\, G = d(G)$.

Proposition 46. *Let $L = \langle g_1, h_1, \ldots, g_k, h_k\rangle$ be a subgroup of a free pro-p group G such that $w_k(g_1, h_1, \ldots, g_k, h_k) = 1$. Then L has rank at most k.*

Proof. We will prove the lemma by induction on k. The case $k = 1$ is clear. Since L is a closed subgroup in a free pro-p subgroup, by Theorem 43 it is free. Now by Theorem 44, any generating set of a free pro-p group contains a free generating subset. Let $S \subseteq \{g_1, h_1 \ldots, g_k, h_k\}$ freely generate L. We put $S_i = S \cap \{g_i, h_i\}$. We divide the proof in two cases.

Case 1: there exists $1 \leq i \leq k$ such that $|S_i| = 1$.

Without loss of generality we may assume that $i = k$ and $h_k \in S$. Consider $N = \langle h_k\rangle^L$ the normal closure in L. Since $h_k \in S$, it implies L/N is free.

$$w_{k-1}(g_1N, h_1N \ldots, g_{k-1}N, h_{k-1}N) = 1N,$$

and so, by induction, the group T generated by $\{g_1N, h_1N, \ldots, g_{k-1}N, h_{k-1}N\}$ has rank at most $k-1$. Hence

$$\mathrm{rk}(L) \leq \mathrm{rk}(T) + |S_k| \leq k - 1 + 1 = k.$$

Case 2: There is no $1 \leq i \leq k$ such that $|S_i| = 1$.

In this case there exists $A \subseteq \{1, \ldots, k\}$ such that $S = \{g_a, h_a : a \in A\}$. Note that without loss of generality we may assume that $A = \{1, \ldots, r\}$ because

$$\prod_{1\leq i\leq k} [g_i, h_i] = \prod_{1\leq i\leq s-1} [g_i, h_i] \cdot \left([g_{s+1}, h_{s+1}][g_s^{[g_{s+1},h_{s+1}]}, h_s^{[g_{s+1},h_{s+1}]}]\right) \cdot \prod_{s+2\leq i\leq k} [g_i, h_i].$$

If $r > k/2$, it would imply that $\prod_{1\leq i\leq r}[g_i, h_i]$ could be expressed as a product of $k - r < r$ commutators. But since $\langle g_i, h_i : 1 \leq i \leq r\rangle$ is a free generating subset for L, we get a contradiction. Consequently $r \leq k/2$, and so

$$\mathrm{rk}(L) \leq 2 \cdot \frac{k}{2} = k. \qquad \square$$

We found out a posteriori that Mel'nikov had already proved in [34] a specific case of our lemma; i.e if $u_1, \ldots, u_n$ are elements of a free pro-p group satisfying the relation

$$[u_1, u_2][u_3, u_4] \cdots [u_{m-1}, u_m] u_{m+1}^{\alpha_1} \cdots u_n^{\alpha_{n-m}} = 1$$

where $0 < m = 2k < n$, $\alpha_i \in p\mathbb{Z}_p$ for $i = l, 2, ., n - m$, then the rank of the subgroup generated by $u_1, u_2, \ldots, u_n$ does not exceed $n/2$.

Using the Lemma 46 we deduce the following result:

Theorem I. *Let L be the d-generated free pro-p group and $\{L_n\}_{n\in\mathbb{N}}$ the filtration in L given by its dimension subgroups. Then*

$$\mathrm{Dim}_{\{L_n\}} S_{w_k}(1) \leq 1/2.$$

wherenever $d > k$.

This result implies that $\mathrm{Dim}_{\{L_n\}} S_w(1) \geq (k-1)/k$ doesn't hold for free pro-p groups in general. The theorem shows that for the words w_k in $2k$ variables, as soon as $k \geq 2$ the bound is not satisfied.

Proof. Our approach is to find a set S such that $S_{w_k} \subseteq S$ and $\mathrm{Dim}_{\{L_n\}} S \leq 1/2$. Let $(g_1, \ldots, g_{2k}) \in L^{(2k)}$ be such that $w_k(g_1, \ldots, g_{2k}) = 1$. Then $\langle g_1, \ldots, g_{2k} \rangle$ is a free subgroup of L and by Lemma 46, it has rank at most k. Hence
$\{(g_1, \ldots, g_{2k}) \in L^{(2k)} \,|\, w_k(g_1, \ldots, g_{2k}) = 1\} \subseteq \{(g_1, \ldots, g_{2k}) \in L^{(2k)} \mid \mathrm{rk}\langle g_1, \ldots, g_{2k} \rangle \leq k\}$.

For each $(h_1, \ldots, h_k) \in L^{(k)}$, we can define

$$S(h_1, \ldots, h_k) = \{(g_1, \ldots, g_{2k}) \in L^{(2k)} \,|\, \langle g_1, \ldots, g_{2k} \rangle = \langle h_1, \ldots, h_k \rangle\}.$$

Note that, $S_{w_k}(1) \subseteq S = \bigcup_{(h_1,\ldots,h_k) \in L^{(k)}} S(h_1, \ldots, h_k)$.

Consider $\{L_n\}$ the filtration for L provided by the n-th dimension subgroups L_n of F. Hence,

$$\mathrm{Dim}\, S_{w_k}(1) = \liminf_{n \to \infty} \frac{\log_p |S_{w_k}(1)_{\pi_n^{(2k)}}|}{\log_p |(L/L_n)^{(2k)}|}.$$

From one side, from Lemma 4.3 in [29] we have that

$$\log_p(|L : L_n|^{2k}) = \frac{2k \cdot d^n}{(d-1)(n-1)}(1 + o(1)).$$

From the other hand, note that
$S(h_1, \ldots, h_k)_{\pi_n} \subseteq \{(g_1 L_n, \ldots, g_{2k} L_n) \in (L/L_n)^{(2k)} \,|\, \langle g_1 L_n, \ldots, g_{2k} L_n \rangle = \langle h_1 L_n, \ldots, h_k L_n \rangle\}$.

For each fixed k-tuple $(h_1 L_n, \ldots, h_k L_n) \in (L/L_n)^{(k)}$, it is easy to see that the number of k-tuples $(g_{k+1} L_n, \ldots, g_{2k} L_n) \in (L/L_n)^{(k)}$ such that $\langle g_{k+1} L_n, \ldots, g_{2k} L_n \rangle \subseteq \langle h_1 L_n, \ldots, h_k L_n \rangle$ is at most $|F_k L_n : L_n|$, where we write F_k for any free pro-p subgroup of rank k of L. We can then also define its dimension subgroups by $L_n(F_k)$. With this notation, note $|F_k L_n : L_n| \leq |F_k : L_n(F_k)|$, and hence $|S_{i\pi_n}| \leq |L/L_n|^k \cdot |F_k/L_n(F_k)|^k$.

Consequently, again using Lemma 4.3 in [29] we deduce that

$$\mathrm{Dim}_{\{L_n\}} S_{w_k}(1) \leq \liminf_{n\to\infty} \frac{\frac{kd^n}{(d-1)(n-1)}(1+o(1))}{\frac{2k\cdot d^n}{(d-1)(n-1)}(1+o(1))} + \frac{\frac{k\cdot k^n}{(k-1)}(1+o(1))}{\frac{2k\cdot d^n}{(d-1)(n-1)}(1+o(1))} = 1/2,$$

since $\liminf_{n\to\infty} \frac{(n-1)(d-1)}{2(k-1)} \cdot \left(\frac{k}{d}\right)^n = 0$. □

6.3 p-adic analytic groups

In this section we want to start the study of the same question in the setting of p-adic analytic groups; i.e. does $\mathrm{Dim}_{\{G_n\}} S_{w_k}(1) \geq (2k-1)/2k$ for the natural filtration $\{G^{p^n}\}$ of G? This is just a first approach to work on this question. We have put together some basic results and conclusions in this context.

First recall that a p-adic analytic group is a p-adic analytic manifold which is also a group.

Theorem 47 (Theorem 8.1, [8]). *A topological group G has the structure of a p-adic analytic group if and only if G has an open subgroup which is a powerful finitely generated pro-p group.*

From Theorem 4.5 in [8], we have that a powerful finitely generated pro-p group is *uniform* if and only if it is torsion-free. And Theorem 8.18 in [8], adds that any topological group containing an open subgroup which is a uniform pro-p group is a p-adic analytic group. From Definition 4.7 in [8] we also now that if G is a pro-p group of finite rank, the dimension of G is $\dim(G) = \dim(H)$ where H is any open uniform subgroup of G. What is more, $\dim(G)$ is indeed the dimension of G as a p-adic analytic group (see Theorem 8.36 in [8]). Another important result for our interest will be the following

Theorem 48 (Theorem 4.9, [8]). *Let G be a uniform pro-p group and $\{a_1, \ldots, a_d\}$ a topological generating set for G, where $d = \dim(G)$. Then the mapping*

$$(\lambda_1, \ldots, \lambda_d) \to a_1^{\lambda_1} \cdots a_d^{\lambda_d}$$

from $\mathbb{Z}_p^{(d)}$ to G is a homeomorphism.

Looking for better algebraic properties of the system of coordinates for G, we introduce a new group structure on G. For any $x, y \in G$,

$$x +_n y = (x^{p^n} y^{p^n})^{p^{-n}};$$

and so the map $x \to x^{p^{-n}}$ becomes an isomorphism from G_{n+1} onto $(G, +_n)$ where G_n are the subgroups of the lower central series of G, (see Definition 1.1 in [8]). As a consequence, we define a new operation:

Proposition 49 (Proposition 4.13, [8]). *The set G with the operation $+$ defined as follows;*

$$x + y = \lim_{n \to \infty} x +_n y;$$

is an abelian group, with identity element 1 and inversion given by $x \to x^{-1}$.

Proposition 50 (Proposition 4.16, [8]). *With the original topology of G, $(G, +)$ is a uniform pro-p group of dimension $d = \dim(G)$. Moreover, any set of topological generators for G is a set of topological generators for $(G, +)$.*

Since $(G, +)$ is a pro-p group, Section 1.3. in [8] shows that it admits a natural action by $\mathbb{Z}_p$. Besides, since $(G, +)$ is abelian, using Proposition 1.26, this makes into a $\mathbb{Z}_p$-module.

Theorem 51 (Theorem 4.17, [8]). *Let G be a uniform pro-p group of dimension d, and let $\{a_1, \ldots, a_d\}$ be a topological generating set for G. Then $(G, +)$ is a free $\mathbb{Z}_p$-module on the basis $\{a_1, \ldots, a_d\}$.*

An important result on the Hausdorff dimension of p-adic analytic groups is Theorem 1.1 in [7]:

Theorem 52. *Let G be a p-adic analytic pro-p group with the natural filtration $\{G_n\}$ given by the p^n-th powers; i.e. $G_n = G^{p^n}$, and let $H \leq_c G$ be a closed subgroup of G. Then*

$$\operatorname{hdim}_{\{G_n\}} H = \frac{\dim H}{\dim G},$$

where $\dim G$ denotes the dimension of G as a p-adic Lie group.

First of all note that $S_w(1)$ is a closed set in $G^{(k)}$. If $\dim G = d$ and w is a word in k variables, what are the conditions so that $\operatorname{Dim} S_w(1) \geq d \cdot (k-1)$? Does Theorem 52 hold if we substitute closed subgroups by closed sets? If this last question were true, and we could prove that $\operatorname{Dim} S_w(1) \geq d \cdot (k-1)$, we would conclude

$$\operatorname{Dim}_{\{G_n\}} S_w(1) = \frac{\dim S_w(1)}{\dim G^{(k)}} \geq \frac{d \cdot (k-1)}{d \cdot k} = (k-1)/k.$$

Although not necessary, these would be sufficient conditions to prove $\operatorname{Dim}_{\{G_n\}} S_w(1) \geq (k-1)/k$ in this setting.

To start with, we consider $G = \mathbb{Z}_p^{(d)}$. Since for any word w in k variables, $S_w(1)$ is the kernel of the homomorphism $f_w : G^{(k)} \to G$ defined by $(g_1, \ldots, g_k) \to w(g_1, \ldots, g_k)$, then it is a submanifold in $G^{(k)}$. Consequently, we deduce the following result:

Proposition 53. *Let $G = \mathbb{Z}_p^{(d)}$ with the filtration $\{G^{p^n}\}$ and let w be a word in k variables. Then*

$$\operatorname{Dim}_{\{G^{p^n}\}} S_w(1) = \frac{\dim S_w(1)}{k \cdot \dim G}.$$

Another result towards having a positive answer to our question is the following:

Proposition 54. *Let G be a p-adic analytic pro-p group of dimension d and w a*

word in k variables. If for any open uniform subgroup H of G,

$$\mathrm{Dim}_{\{H^{p^n}\}} S_{w,H}(1) \geq (d-1)/d; \tag{6.3}$$

then $\mathrm{Dim}_{\{H^{p^n}\}} S_{w,G}(1) \geq (d-1)/d$.

Proof. Let H be an open uniform pro-p subgroup of G and let $H_n = H^{p^n}$ be the usual filtration. Using the definition in (6.1), and since H can be regarded as a $\mathbb{Z}_p$-module by Theorem 51,

$$\mathrm{Dim}_{\{H_n\}} S_{w,H^{(k)}}(1) = \liminf_{n\to\infty} \frac{\log_p |S_{w,H^{(k)}}(1) H_n^{(k)} : H_n^{(k)}|}{\log_p |(H : H_n)^{(k)}|} \geq (d-1)/d.$$

Let $\lambda_n = \frac{\log_p |S_{w,H}(1) H_n^{(k)} : H_n^{(k)}|}{\log_p |(H:H_n)^{(k)}|}$. If consider the same filtration for G, one gets

$$\begin{aligned}
\mathrm{Dim}_{\{H_n\}} S_{w,G}(1) &\geq \liminf_{n\to\infty} \frac{\log_p |S_{w,H}(1) H_n^{(k)} : H_n^{(k)}|}{\log_p |(G : H_n)^{(k)}|} \\
&= \liminf_{n\to\infty} \frac{\log_p |S_{w,H}(1) H_n^{(k)} : H_n^{(k)}|}{\log_p |(H : H_n)^{(k)}|} \cdot \frac{\log_p |(H : H_n)^k|}{\log_p |(G : H_n)^k|} \\
&= \liminf_{n\to\infty} \lambda_n \cdot \frac{\log_p |(H : H_n)^k|}{\log_p |(G : H_n)^k|} \geq (d-1)/d,
\end{aligned}$$

since $\liminf_{n\to\infty} \frac{\log_p |H:H_n|}{\log_p |G:H_n|} = \liminf_{n\to\infty} \frac{nd}{c+nd} = 1$ with $c = \log_p |G : H|$. □

Consequently, future work could be started by studying whether the hypothesis of Proposition 54 holds for any uniform pro-p group; that is, studying whether for any uniform pro-p group H with the filtration $\{H_n\} = \{H^{p^n}\}$,

$$\mathrm{Dim}_{\{H^{p^n}\}} S_{w,H}(1) \geq (d-1)/d.$$

Bibliography

[1] M. Levy, "On the probability of satisfying a word in nilpotent groups of class 2," *arxiv.org/abs/1101.4286*, 2011.

[2] D. Segal, *Words: notes on verbal width in groups*, vol. 361 of *LMS Lect. Notes*. Cambridge Univ. Press, Cambridge, 2009.

[3] P. Hall, "A contribution to the theory of groups of prime power order," *Proc. London Math. Soc.*, vol. 36, pp. 29–95, 1933.

[4] G. A. Fernández-Alcober, "An introduction to finite p-groups:regular p-groups and groups of maximal class." Notes for XVI Escola de Álgebra.

[5] G. Michler, *Theory of finite simple groups*. Cambridge Univ. Press, Cambridge, 2006.

[6] A. G. Abercrombie, "Subgroups and subrings of profinite rings," *Math. Proc. Cambridge Philos. Soc.*, vol. 116, 1994.

[7] Y. Barnea and A. Shalev, "Hausdorff dimension, pro-p groups, and Kac-Moody algebras," *Trans. Amer. Math. Soc.*, vol. 349, pp. 5073–5091, 1997.

[8] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal, *Analytic pro-p groups*. Cambridge Univ. Press, Cambridge, 2nd ed., 1999.

[9] J. D. Dixon, L. Pyber, Á. Seress, and A. Shalev, "Residual properties of free groups and probabilistic methods," *J. Reine Angew. Math.*, vol. 556, pp. 159–172, 2003.

[10] A. Amit, "On equations in nilpotent groups." (unpublished), 2006.

[11] M. Abért, "On the probability of satisfying a word in a group," *J. Group Theory*, vol. 9, pp. 685–694, 2006.

[12] N. Nikolov and D. Segal, "A characterization of finite soluble groups," *Bull. London Math. Soc.*, vol. 39, pp. 209–213, 2007.

[13] O. Parzanchevski and G. Schul, "On the Fourier expansion of word maps," *Bull. London Math. Soc.*, vol. 46, pp. 91–102, 2014.

[14] The GAP group, GAP – Groups, Algorithm and Programming, Version 4.8.6; 2016. (http://www.gap-system.org).

[15] A. Lubotzky, "Images of word maps in finite simple groups," *Glasg. Math. J.*, vol. 56, pp. 465–469, 2014.

[16] S. V. Ivanov, "P. Hall's conjecture on the finiteness of verbal subgroups," *Izv. Vyssh. Uchem. Zaved*, vol. 325, pp. 60–70, 1989.

[17] R. Guralnick and P. Shumyatsky, "On rational and concise words," *J. Algebra*, vol. 429, pp. 213–217, 2015.

[18] O. Parzanchevski. Private communication, 2014.

[19] A. Amit and U. Vishne, "Characters and solutions to equations in finite groups," *J. Algebra Appl.*, vol. 10, pp. 675–686, 2011.

[20] R. P. Stanley, *Enumerative combinatorics*, vol. 2. Cambridge Univ. Press, Cambridge, 1999.

[21] L. Solomon, "The solution of equations in groups," *Arch. Math. (Basel)*, vol. 20, pp. 241–247, 1969.

[22] I. M. Isaacs, *Character Theory of Finite Groups*. AMS/Chelsea, Providence, Reprint of 1976 edition, 2006.

[23] G. Frobenius, "Über gruppencharaktere," *Sitzber. Königlich Preuss. Akad. Wiss. Berlin*, pp. 985–1021, 1896.

[24] A. K. Das and R. K. Nath, "On Solutions of a Class of Equations in a Finite Group," *Comm. Algebra*, vol. 37, pp. 3904–3911, 2009.

[25] S. P. Strunkov, "On the theory of equations in finite groups," *Izv. Math.*, vol. 59, pp. 1273–1282, 1995.

[26] P. Moree and H. Hommerson, "Value distribution of Ramanujan sums and of cyclotomic polynomial coefficients," *arxiv.org/abs/math/0307352*, 2003.

[27] M. R. Pournaki and R. Sobhani, "Probability that the commutator of two group elements is equal to a given element," *J. Pure Appl. Algebra*, vol. 212, pp. 727–734, 2008.

[28] L. Carlitz, "Representations by skew forms in a finite field," *Arch. Math. (Basel)*, vol. 5, pp. 19–31, 1954.

[29] A. Jaikin-Zapirain, "On the verbal width of finitey generated pro-p groups," *Revista Mat. Iberoamericana*, vol. 24, pp. 617–630, 2008.

[30] E. I. Khukhro, *p-automorphisms of Finite p-Groups*, vol. 246. Cambridge Univ. Press, Cambridge, 1998.

[31] W. H. Gustafson, "What is the probability that two group elements commute?," *Amer. Math. Monthly*, vol. 80, pp. 1031–1034, 1973.

[32] L. Ribes and P. A. Zalesskii, *Profinite Groups*, vol. 40 of *Ergebnisse der Math.* Springer-Verlag, Berlin, 2000.

[33] J.-P. Serre, *Galois cohomology.* Springer-Verlag, Berlin, 1997.

[34] O. V. Mel'nikov, "Products of powers and commutators in free pro-p-groups," *Mat. Zametki*, vol. 40, pp. 433–441, 1986.