Enumerating fibres of commutator words over $p$-groups

Matthew Levy

Bielefeld University

Abstract

We enumerate the fibres of commutator word maps over $p$-groups of nilpotency class less than $p$ with exponent $p$. We also give some examples and enumerate the fibre sizes of all word maps over $p$-groups of class 2 with exponent $p$.

1 Introduction

Let $G$ be a finite group, $w(x_1,...,x_n)$ a group word and $w$ the associated word map $w: G^{(n)} \to G$. For $g \in G$ denote by $N^G_w(g)$ the number of solutions to $w = g$ and by $P^G_w(g)$ the probability that a random $n$-tuple $g = (g_1,...,g_n) \in G^{(n)}$ satisfies $w(g) = g$, i.e.

$$P^G_w(g) = \frac{N^G_w(g)}{|G|^n}.$$ 

The study of $P^G_w$ has attracted a lot of attention in recent years. For example, in [4], it was shown that for $1 \neq w$ and a finite simple group $G$, $P^G_w(1) \to 1$ as $|G| \to \infty$. Results in [10] provide sharp bounds on $P^G_w$ for general words $w$ and finite simple groups $G$. If $G$ is abelian, then the word map

$$w: G^{(n)} \to G,$$

is a homomorphism and it is clear that

$$N^G_w(1) = |\text{Ker } w| = \frac{|G|^n}{|\text{Im } w|} \geq |G|^{n-1}$$

and so $P^G_w(1) \geq \frac{1}{|G|^n}$. It is a conjecture of Alon Amit (see [1]) that if $G$ is a nilpotent group then $P^G_w(1) \geq \frac{1}{|G|^n}$. In [11] we prove Amit’s Conjecture in the special case where the nilpotency class is 2. Note that since the statistics $N^G_w(1)$ and $P^G_w(1)$ are multiplicative under direct products, we may reduce to the case where $G$ is a finite $p$-group. In this paper we study the fibre sizes of a particular class of words over $p$-groups. In Section 3 we show that this is enough to determine the fibre sizes of all word maps over $p$-groups of class 2 with exponent $p$.

For $t \in \mathbb{N}$, let $c_t$ denote the word map given by $c_t = [x_1,y_1]...[x_t,y_t]$ and, for $g \in G$, let $N^G_{c_t}(g)$ denote $N^G_{c_t}(g)$. Similarly let $P^G_{c_t}$ denote the $c_t$-distribution on
$G$, i.e.

$$P_t^G(g) = \frac{N_t^G(g)}{|G|^{2t}},$$

and let $U^G$ be the uniform distribution on $G$ (i.e. $U^G(g) = 1/|G|$). By a classical result of Frobenius from 1896 (see, for example, [7]) we have

$$N_t^G(g) = |G|^{2t-1} \sum_{\chi \in \text{Irr}(G), \chi \neq 1} \frac{\chi(g)}{\chi(1)^2},$$

where 1 is the identity element of $G$ and we sum over the irreducible complex characters of $G$. In the main result of this paper, Theorem 2.1, we give explicit formulae to compute the numbers $N_t^G(g)$, for finite $p$-groups $G$ of nilpotency class less than $p$ with exponent $p$, in terms of the number of rational points of certain algebraic varieties.

In [5] Garion & Shalev prove the following.

**Proposition 1.1** (Proposition 1.1 [5]). Let $G$ be a finite group. Then

$$||P_t^G - U^G||_1 \leq \left( \sum_{\chi \in \text{Irr}(G), \chi \neq 1} \chi(1)^{-2} \right)^{1/2},$$

where $||P_t^G - U^G||_1 = \sum_{g \in G} |P_t^G(g) - U^G(g)|$.

As the authors remark, this bound has no content when the sum on the right hand side is greater than or equal to 1. Since the non-trivial linear characters of $G$ contribute $|G/G'|^{-1}$ to the sum the result can only be useful for perfect groups. Since the maps $c_t$ take values in $G'$ it is not hard to adapt their proof and deduce the following.

**Proposition 1.2.** Let $G$ be a finite group. Then

$$||P_t^{G'} - U^{G'}||_1 \leq \left( \frac{|G'|}{|G|} \sum_{\chi \in \text{Irr}(G), \chi(1) \neq 1} \chi(1)^{-2t} \right)^{1/2}.$$  

If the right hand side in Proposition 1.2 is close to zero, then the fibres of the maps $c_t$ are roughly the same size and the values are uniformly distributed. The proof follows easily from the following lemmas.

**Lemma 1.3.** Let $G$ be a finite group. Then

$$\sum_{g \in G'} P_t^G(g)^2 = \frac{1}{|G'|} + \frac{1}{|G|} \sum_{\chi \in \text{Irr}(G), \chi(1) \neq 1} \chi(1)^{-2t}.$$  

**Proof.** The proof follows from Lemma 2.1 in [5] and noting that $P_t^G(g) = 0$ for $g \notin G'$.

**Lemma 1.4.** Let $G$ be a finite group. Then

$$\sum_{g \in G'} \left( P_t^G(g) - \frac{1}{|G'|} \right)^2 = \frac{1}{|G|} \sum_{\chi \in \text{Irr}(G), \chi(1) \neq 1} \chi(1)^{-2t}.$$  


Proof. By Lemma 1.3,

\[
\sum_{g \in G'} \left( P_t^G(g) - \frac{1}{|G'|} \right)^2 = \sum_{g \in G'} P_t^G(g)^2 - \frac{2}{|G'|} \sum_{g \in G'} P_t^G(g) + \frac{1}{|G'|}
\]

\[
= \frac{1}{|G'|} \sum_{\chi \in \text{Irr}(G), \chi(1) \neq 1} \chi(1)^{-2t}
\]

since \( \sum_{g \in G'} P_t^G(g) = 1 \).

\[\square\]

Proof of Proposition 1.2. This follows from the Cauchy-Schwarz inequality,

\[
(||P_t^G - U^G||^1_1)^2 = \left( \sum_{g \in G'} \left( P_t(g) - \frac{1}{|G'|} \right) \right)^2 \leq |G'| \sum_{g \in G'} \left( P_t(g) - \frac{1}{|G'|} \right)^2
\]

and the previous lemma.

\[\square\]

In Section 2 we will develop formulae for the fibre sizes of the word maps \( c_t \) over \( p \)-groups of nilpotency class less than \( p \) with exponent \( p \). Moreover, these results extend, more generally, to \( p \)-groups obtained by ‘base extension’. In Section 3 we will determine the fibre sizes of all word maps over \( p \)-groups of class 2 with exponent \( p \). We will then give some examples in Section 4.

2 Enumerating sizes of fibres

Let \( G \) be a finite \( p \)-group and, for each \( i \in \mathbb{N} \), write \( \text{Irr}^i(G) = \{ \text{irreducible complex characters of } G \text{ of degree } p^i \} \) and \( \text{Irr}(G) \) for the set of all irreducible complex characters. For a complex variable \( s \) and \( g \in G \) write

\[\zeta_G^i(s, g) = \sum_{\chi \in \text{Irr}^i(G)} \frac{\chi(g)}{\chi(1)^s}.\]

(2)

We will also write

\[\zeta_G(s, g) = \sum_{\chi \in \text{Irr}(G)} \frac{\chi(g)}{\chi(1)^s} = \sum_{i \in \mathbb{N}} \zeta_G^i(s, g).\]

(3)

It is clear from equations (1) and (3) that

\[N_t^G(g) = |G|^{2t-1} \zeta_G(t, g)\]

and that

\[P_t^G(g) = \frac{1}{|G|} \zeta_G(t, g)\]
A twisted zeta function, is studied by Jaikin-Zapirain c.f. [3, Theorem 1.2] where he shows that it is a rational function in $p^{-s}$ for any $g \in G$ where $G$ is a FAb uniform pro-$p$ group.

We also note that the twisted zeta function in equation (3) is multiplicative under direct products in the following sense: for $g_1 \in G_1$ and $g_2 \in G_2$ where $G_1$ and $G_2$ are groups we have

$$\zeta_{G_1 \times G_2}(s, g_1 g_2) = \zeta_{G_1}(s, g_1) \cdot \zeta_{G_2}(s, g_2).$$

In [12] O’Brien & Voll use the Kirillov orbit method to enumerate the irreducible complex characters, of each degree, of finite $p$-groups of nilpotency class less than $p$. If the group $G$ is of exponent $p$, then the number of characters, of each degree, of $G$ can be described in terms of the number of rational points of certain algebraic varieties. We can analogously compute the sums $\zeta_G(s, g)$ by counting the numbers of rational points of the algebraic varieties considered by O’Brien & Voll that intersect a hyperplane characterized by $g$.

We now fix a $p$-group $G$ of nilpotency class less than $p$ with exponent $p$ and an element $g \in G$.

The Lazard correspondence establishes an order-preserving bijection between finite $p$-groups of nilpotency class $c < p$ and finite nilpotent Lie rings of $p$-power order and class $c < p$; cf. [2, Example 10.24]. Let $c < p$ be the nilpotency class of $G$. Let $\mathfrak{g} = \log(G)$ be the finite Lie ring associated to $G$ by the Lazard correspondence. The Kirillov orbit method gives a correspondence between characters of $G$ and orbits in $\hat{\mathfrak{g}} := \text{Hom}(\mathfrak{g}, \mathbb{C}^*)$, the Pontryagin dual of $\mathfrak{g}$, under the co-adjoint action of $G$ on $\mathfrak{g}$; cf. [3, Theorem 2.6] or [6, Theorem 4.4]. Under this correspondence each orbit $\Omega$ of size, say, $p^{2i}$ gives rise to a character $\chi_{\Omega}$ of degree $p^i$ and all characters are of this form. We have

$$\zeta_{\Omega}(s, g) = \sum_{\Omega \subseteq \hat{\mathfrak{g}}, |\Omega| = p^{2i}} \frac{\chi_{\Omega}(g)}{\chi_{\Omega}(1)^s},$$

where we sum over orbits $\Omega$ of $\hat{\mathfrak{g}}$ and $\chi_{\Omega}$ is the character of $G$ that corresponds to the orbit $\Omega$. For each $\omega \in \Omega$ we denote $\chi_{\omega} = \chi_{\Omega}$.

For each $\omega \in \hat{\mathfrak{g}}$ we write $B_{\omega}$ for the bi-additive, skew-symmetric form $B_{\omega} : \mathfrak{g} \times \mathfrak{g} \to \mathbb{C}^*$, $(u, v) \mapsto \omega([u, v])$ and $\text{Rad}(B_{\omega})$ for the radical of $B_{\omega}$. Note that the centre $\mathfrak{z}$ of $\mathfrak{g}$ is contained in $\text{Rad}(B_{\omega})$ and the form $B_{\omega}$ only depends on the restriction of $\omega$ to $\mathfrak{g}'$. From [12] we have, for each $i$,

$$\zeta_{\Omega}(s, g) = p^{-2i} \sum_{\omega \in \hat{\mathfrak{g}}, |\mathfrak{g} : \text{Rad}(B_{\omega})| = p^{2i}} \frac{\chi_{\omega}(g)}{\chi_{\omega}(1)^s} = p^{-2i} \sum_{\omega \in \hat{\mathfrak{g}}, |\mathfrak{g} : \text{Rad}(B_{\omega})| = p^{2i}} \frac{\chi_{\omega}(g)}{\chi_{\omega}(1)^s} = p^{-2i} \sum_{\omega \in \hat{\mathfrak{g}}, |\mathfrak{g} : \text{Rad}(B_{\omega})| = p^{2i}} \frac{\chi_{\omega}(g)}{\chi_{\omega}(1)^s}.$$
where $\Omega_\omega$ is the orbit containing $\omega$ and we identify $g$ with an element of $g = \text{log}(G)$. Hence

$$G^i_G(s, g) = |g| \cdot p^{-i(3+s)} \sum_{\omega \in \hat{\omega}} \sum_{\nu \in \Omega_\omega} \nu(g).$$

Theorem B in [12] gives a geometric characterization of this sum in terms of the numbers of certain rational points of rank varieties of matrices of linear forms. Assume that $g$ is a compact discrete valuation ring of characteristic zero with maximal ideal $p$ and residue field $k = o/p$ of characteristic $p$. Suppose that $g$ is a finite, nilpotent $o$-Lie algebra of class $e < p$ and that both $g/\hat{g}$ and $g'$ are annihilated by $p$. Set $a := r_k(g/\hat{g})$ and $b := r_k(g')$ and fix bases $e = \{e_1, ..., e_a\}$ and $f = \{f_1, ..., f_b\}$ for $g/\hat{g}$ and $g'$ respectively. Choose structure constants $\lambda^k_{ij} \in k$ such that

$$[e_i, e_j] = \sum_{k=1}^{b} \lambda^k_{ij} f_k$$

and $\lambda^k_{ij} = -\lambda^k_{ji}$ for all $i, j \in \{1, ..., a\}$ and $k \in \{1, ..., b\}$. Let $Y = (Y_1, ..., Y_b)$ be independent variables and define the ‘commutator matrix’ (with respect to $e$ and $f$) $B(Y) \in \text{Mat}_a(k[Y])$ given by

$$B(Y)_{ij} := \sum_{k=1}^{b} \lambda^k_{ij} Y_k$$

for all $i, j \in \{1, ..., a\}$. For $y = (y_1, ..., y_b) \in K^b$, where $K$ is any finite extension of $k$, write $B(y) \in \text{Mat}_a(K)$ for the matrix obtained by evaluating the variables $Y_i$ at $y_i$. Note that the matrices $B(y)$ are skew-symmetric, have even rank and that $\text{det}(B(Y))$ is a square in $k[Y]$, whose square root $\text{Pf}(B(Y)) := \sqrt{\text{det}(B(Y))}$ is the Pfaffian of $B(Y)$. If $a$ is odd then $\text{Pf}(B(Y)) = 0$.

Fix a non-trivial additive character $\phi : k \to \mathbb{C}^\times$. For $a \in k$ define $\phi_a(x) = \phi(ax)$. The map $a \mapsto \phi_a$ is an isomorphism between $k$ and its Pontryagin dual $\hat{k}$. We have an isomorphism between $g'$ and its dual $\hat{g}'$ and also a canonical isomorphism between $g'$ and its linear dual $\text{Hom}_k(g', k)$. We now fix an isomorphism $\psi_1 : \hat{g}' \to \text{Hom}_k(g', k)$. The dual $k$-basis $f' = (f'_k)$ for $\text{Hom}_k(g', k)$ gives a coordinate system

$$\psi_2 : \text{Hom}_k(g', k) \to k^b;$$

$$y = \sum_{k=1}^{b} y_k f'_k \mapsto y = (y_1, ..., y_b).$$

Set $\psi := \psi_2 \circ \psi_1 : \hat{g}' \to k^b$, an isomorphism. Under this isomorphism we may identify elements $y \in k^b$ with elements $\omega y \in \hat{g}'$.

Assume that $\mathcal{O}$ is an unramified extension of $o$, with maximal ideal $\mathfrak{p}$. Write $g(\mathcal{O})$ for $g \otimes_o \mathcal{O}$ and $f(\mathcal{O})$ for $f \otimes_o \mathcal{O}$. We identify the residue field $\mathcal{O}/\mathfrak{p}$, a finite extension of $k$, with $\mathbb{F}_q$. The derived $\mathcal{O}$-Lie algebra $g(\mathcal{O})'$ as well as the quotient $g(\mathcal{O})/g(\mathcal{O})'$ are annihilated by $\mathfrak{p}$. We denote the corresponding bases, $e \otimes_k 1$ for $g(\mathcal{O})/g(\mathcal{O})'$ and $f \otimes_k 1$ for $g(\mathcal{O})'$, obtained by this base extension by $e$ and
for each $i$ a finite, unramified extension of $\mathcal{O}$ of class $\sum \omega$. Assume that $\omega$ and $G$ are defined in equations (5) and (6).

We write $K_G^i(g) = \# \{ b \in \mathbb{F}_q^i : \text{rk}(B(b)) = 2i, g \in \text{Ker}(\omega_y) \}$ and $V_G^i(g) = \# \{ b \in \mathbb{F}_q^i : \text{rk}(B(b)) = 2i, \text{ord}(\omega_y(g)) \neq 1 \}$. Note that $\sum_i K_G^i(1) = q^i$ and $V_G^i(1) = 0$ for all $i$ whilst for $1 \neq g \in G$ we have $\sum_i K_G^i(g) = q^i - 1$.

We write $K_G^i(g)$ and $V_G^i(g)$ for the vectors $(K_G^i(g)_1)$ and $(V_G^i(g)_1)$, respectively. The numbers $\omega_y(g)$ are $p$-th roots of unity. Since the sum of the $q - 1$ Galois conjugates of non-trivial $q$-th roots of unity is $-1$ we have the following:

**Theorem 2.1.** Let $\mathfrak{o}$ be a compact discrete valuation ring of characteristic zero with residue field $k$ of characteristic $p$ and let $\mathfrak{g}$ be a finite, nilpotent $\mathfrak{o}$-Lie algebra of class $c < p$. Assume that $\mathfrak{g}' \cong k^b$ and $\mathfrak{g}/\mathfrak{j} \cong k^a$ as $k$-vector spaces. Let $\mathfrak{D}$ be a finite, unramified extension of $\mathfrak{o}$, with residue field isomorphic to $\mathbb{F}_q$. Write $G := G(\mathfrak{D})$ for the group associated with $\mathfrak{g}(\mathfrak{D})$ under the Lazard correspondence. Then, for each $i$,

$$
\zeta_G^i(s, g) = |G/G'| p^{-i(1+s)} \sum_{y \in \mathbb{F}_q^i, \text{rk}(B(y)) = 2i} \omega_y(g).
$$

This follows immediately from the discussion above.

**3 Nilpotent class 2 groups**

Let $G$ be a finite group, $w(x_1, \ldots, x_n)$ a group word and $w$ the associated word map. Recall that $N_w^G(g)$ is the number of solutions to $w = g$ and that $P_w^G(g)$ is the probability that a random $n$-tuple $g = (g_1, \ldots, g_n) \in G^n$ satisfies $w(g) = g$. The following corollary follows immediately from the results in [11].

**Corollary 3.1 ([11]).** Let $G$ be a finite $p$-group of nilpotency class 2 with exponent $p$ and let $w$ be a group word. Then there exists a word $v$ of the following form:

i) $v = x$; or

ii) $v = c_t$ for some $t$.  

6
such that $P^G_w(g) = P^G_v(g)$ for all $g \in G$.

By Theorem 2.1 we have determined the fibre sizes of all word maps over all $p$-groups of nilpotency class 2 with exponent $p$:

**Corollary 3.2.** Let $p$ be an odd prime and let $G$ be a finite $p$-group of nilpotency class 2 with exponent $p$ and let $w$ be a group word. Then either

i) $P^G_w(g) = \frac{1}{|G|}$ for all $g \in G$; or

ii) $P^G_w(g) = \frac{1}{|G|} \zeta_G(t, g)$ for some $t$ depending on $w$.

4 Examples

We compute the sums $\zeta_G(s, g)$ for various relatively free $p$-groups with exponent $p$. Note that for $i = 0$, the only vector $y$ giving rise to a matrix $B(y)$ such that $\text{rk}(B(y)) = 0$ (see equations (4) and (3)) is $y = 0$. Suppose that $i \neq 0$. Since the rank of the matrix $B(y)$, for given $y \in \mathbb{F}_q^b$, is invariant under scalar multiplication the rank of the matrix $B(y)$ with $y = (y_1 : \ldots : y_b) \in \mathbb{P}^{b-1}(\mathbb{F}_q)$ is well defined. Under the Lazard correspondence we may identify $1 \neq g \in G$ with an element $g \in g' \cong \mathbb{F}_q^b$, the associated Lie algebra, and similarly identify $g$ with $\tilde{g} \in \mathbb{P}^{b-1}(\mathbb{F}_q)$. Since the matrix $B$ is skew-symmetric its determinant $\det(B)$ is a square whose square root $\text{Pf}(B) := \sqrt{\det(B)}$ is the Pfaffian of $B$. If $a$ is odd, then $\text{Pf}(B) = 0$. Assume that $\text{Pf}(B) \neq 0$. Then $\text{Pf}(B)$ defines a hypersurface in $\mathbb{P}^{b-1}$ and the $\mathbb{F}_q$-rational points $y$ of this hypersurface correspond to matrices $B(y)$ of a certain non-maximal rank. The $\mathbb{F}_q$-rational points which do not lie on the hypersurface will be of maximal rank $a$. We refer to points $\tilde{y} \in \mathbb{P}^{b-1}(\mathbb{F}_q)$ as being ‘of rank $2i$’ for some $i$ if the associated matrix $B(\tilde{y})$ is of rank $2i$. The condition $g \in \text{Ker}(\omega_y)$ in the definition of $\zeta_G(s, g)$ (see equation (3)) defines a hyperplane $H_g$ given by the dot product $\tilde{g}, \tilde{y} = 0$ in $\mathbb{P}^{b-1}(\mathbb{F}_q)$. We may thus talk about the ‘hyperplane defined by $g$’ as $H_g$. The numbers $\zeta_G(s, g)$ are simply the number of $\mathbb{F}_q$-rational points of this hyperplane which intersect the hypersurface defined by $\text{Pf}(B)$ in $\mathbb{P}^{b-1}(\mathbb{F}_q)$ giving rise to a point ‘of rank $2i$’.

We will now proceed with some examples. In each case it turns out that the matrices $B(Y)$ have the form

$$B(Y) = \begin{pmatrix}
0 & U(Y) \\
-U(Y)^{tr} & 0
\end{pmatrix}$$

where $U(Y)$ is a matrix.

**Example 4.1** (Heisenberg group, $H(\mathbb{F}_q)$). Suppose that $G$ is the Heisenberg group $H(\mathbb{F}_q)$. The matrix $U(Y)$, where $Y = (Y_1)$ has a single variable, is simply the $1 \times 1$ matrix with entry $Y_1$. There are two cases, $i = 0$ and $i = 1$, for the rank of the matrix $U(Y)$. The number of vectors $y$ in each case is $1$ and $q - 1$ respectively. When $g = 1$ is the identity, we have $K^1_G(1) = 1$ and $V^0_G(1) = 0$ so that $\zeta_G^1(s, 1) = q^2$. We also have $K^1_G(1) = q - 1$ and $V^1_G(1) = 0$ so that $\zeta_G^1(s, 1) = q^{1-s}(q - 1)$. Together, this gives us

$$\zeta_G(s, 1) = q^2 + q^{-s+1}(q - 1)$$

and when $s = 1$ this is simply $k(G)$, the class number.
Suppose now that $1 \neq g \in G'$. This occurs with multiplicity $(q - 1)$. It is not hard to see that $c_G^0(s, g) = q^2$ since $K_G^0(g) = 1$ and $V_G^0(g) = 0$. Also, $K_G^1(g) = 0$ and $V_G^1(g) = q - 1$ so that

$$\zeta_G(s, g) = q^2 - q^{-s+1}.$$  

**Example 4.2** (A quadric surface in $\mathbb{P}^2(\mathbb{F}_q)$). Let $g$ be the 7-dimensional nilpotent $\mathbb{F}_q$-Lie algebra of class 2 with $\mathbb{F}_q$-basis $(x_1, \ldots, x_4, y_1, y_2, y_3)$ subject to the relations $[x_1, x_3] = y_1$, $[x_1, x_4] = y_2$, $[x_2, x_3] = y_3$, $[x_2, x_4] = y_1$. With respect to this basis we have

$$U(Y) = \begin{pmatrix} Y_1 & Y_2 \\ Y_3 & Y_4 \end{pmatrix}.$$  

The determinant of this matrix is defines the quadric surface $Y_1^2 - Y_2Y_3$ in $\mathbb{P}^2(\mathbb{F}_q)$. There are three cases, $i = 0, 1$ and 2, for the rank of the matrix $U(Y)$. The number of such vectors $y$ in each case is $1$, $(q + 1)(q - 1)$ and $q^2(q - 1)$ respectively. As usual, the $i = 0$ case corresponds to when $y$ is zero, $i = 1$ when $\tilde{y}$ lies on the curve and $i = 2$ otherwise. When $g$ is the identity we can compute

$$K_G(1) = (1, (q + 1)(q - 1), q^2(q - 1))$$  

and $V_G(1) = (0, 0, 0)$ so that $k(G) = q^4 + q^2(q + 1)(q - 1) + q^2(q - 1)$.

Now suppose that $g \neq 1$. We have two cases. The first case is when $H_g$ corresponds to a tangent of the surface $Y_1^2 = Y_2Y_3$. This occurs with multiplicity $(q + 1)(q - 1)$. In this case

$$K_G(g) = (1, (q - 1), q(q - 1))$$  

and

$$V_G(g) = (0, q(q - 1), (q^2 - q)(q - 1)).$$  

The second case is when $H_g$ corresponds to a line which intersects the surface $Y_1^2 = Y_2Y_3$ at two distinct points. This occurs with multiplicity $q^2(q - 1)$. In this case

$$K_G(g) = (1, 2(q - 1), (q - 1)(q - 1))$$  

and

$$V_G(g) = (0, (q - 1)(q - 1), (q^2 - q + 1)(q - 1)).$$  

**Example 4.3** (A quadric surface in $\mathbb{P}^3(\mathbb{F}_q)$). Let $g$ be the 8-dimensional nilpotent $\mathbb{F}_q$-Lie algebra of class 2 with $\mathbb{F}_q$-basis $(x_1, \ldots, x_4, y_1, \ldots, y_4)$ subject to the relations $[x_1, x_3] = y_1$, $[x_1, x_4] = y_2$, $[x_2, x_3] = y_3$, $[x_2, x_4] = y_4$. With respect to this basis we have

$$U(Y) = \begin{pmatrix} Y_1 & Y_2 \\ Y_3 & Y_4 \end{pmatrix}.$$  

The determinant of this matrix defines the quadric surface $Y_1Y_4 - Y_2Y_3$ in $\mathbb{P}^3(\mathbb{F}_q)$. There are three cases, $i = 0, 1$ and 2, for the rank of the matrix $U(Y)$. The number of vectors $y$ in each case is $1$, $(q + 1)^2(q - 1)$ and $(q^3 - q)(q - 1)$ respectively. As usual, the $i = 0$ case corresponds to when $y$ is zero, $i = 1$ when $\tilde{y}$ lies on the curve and $i = 2$ otherwise. When $g$ is the identity we compute

$$K_G(1) = (1, (q + 1)^2(q - 1), q^4 - 1 - (q + 1)^2(q - 1))$$  

and $V_G(1) = (0, 0, 0)$ so that $k(G) = q^4 + q^2(q + 1)^2(q - 1) + q^4 - 1 - (q + 1)^2(q - 1)$. 

8
Now suppose that \( g \neq 1 \). We have two cases. The first case is when \( g \) corresponds to a tangent of the surface \( Y_1Y_4 = Y_2Y_3 \). This occurs with multiplicity \((q + 1)^2(q - 1)\). In this case

\[
K_G(g) = (1, (2q + 1)(q - 1), (q^2 - q)(q - 1))
\]

and

\[
V_G(g) = (0, q^2(q - 1), (q^3 - q^2)(q - 1)).
\]

The second case is when \( g \) corresponds to a plane which intersects the surface \( Y_1Y_4 = Y_2Y_3 \) and is non-tangent. This occurs with multiplicity \((q^3 - q)(q - 1)\). In this case

\[
K_G(g) = (1, (q + 1)(q - 1), q^2(q - 1))
\]

and

\[
V_G(g) = (0, q(q + 1)(q - 1), (q^3 - q^2 - q)(q - 1)).
\]

The following examples were studied by Boston & Isaacs [2].

**Example 4.4** (Elliptic curves in \( \mathbb{P}^2(\mathbb{F}_p) \)). Let \( p \) be a prime and \( \alpha \in \mathbb{F}_p^* \). Let \( g_\alpha \) be the 9-dimensional nilpotent \( \mathbb{F}_p \)-Lie algebra of class 2 with \( \mathbb{F}_p \)-basis \((x_1, \ldots, x_6, y_1, y_2, y_3)\) subject to the relations \([x_1, x_4] = y_1, [x_1, x_5] = y_2, [x_1, x_6] = \alpha y_3, [x_2, x_4] = y_1, [x_2, x_5] = y_1, [x_2, x_6] = y_2, [x_3, x_4] = y_3, [x_3, x_5] = y_3, [x_3, x_6] = y_1\). With respect to this basis we have

\[
U(Y) = \begin{pmatrix}
Y_1 & Y_2 & \alpha Y_3 \\
Y_3 & Y_1 & Y_2 \\
Y_3 & 0 & Y_1
\end{pmatrix}.
\]

The determinant of this matrix defines an elliptic curve \( E_\alpha \) in \( \mathbb{P}^2(\mathbb{F}_p) \) and let \( n_\alpha \) denote the number of \( \mathbb{F}_p \)-rational points of the curve \( E_\alpha \). There are three cases, \( i = 0, 1 \) and \( 2 \), for the rank of the matrix \( U(Y) \). The number of such vectors \( y \) in each case is \( 1, n_\alpha(p - 1) \) and \((p^2 + p + 1 - n_\alpha)(p - 1)\) respectively. As usual, the \( i = 0 \) case corresponds to when \( y \) is zero, \( i = 1 \) when \( y \) lies on the curve and \( i = 2 \) otherwise. When \( g \) is the identity we can compute

\[
K_G(1) = (1, n_\alpha(p - 1), (p^2 + p + 1 - n_\alpha)(p - 1))
\]

and \( V_G(1) = (0, 0, 0) \) so that \( k(G) = p^6 + p^2n_\alpha(p - 1) + (p^2 + p + 1 - n_\alpha)(p - 1) \).

Now suppose that \( g \neq 1 \). Let \( k_\alpha \) denote the number of inflection points of \( E_\alpha \). We have four cases depending on how many times the line \( H_g \) corresponding to \( g \) intersects the elliptic curve \( E_\alpha \) at rational points, this can be zero, once, twice or three times occurring with multiplicities \( p^2 + p + 1 - n_\alpha(p + 1) + \frac{(n_\alpha - k)(n_\alpha - k)(n_\alpha - k)(n_\alpha - k)(n_\alpha - k)(n_\alpha - k)(n_\alpha - k)(n_\alpha - k)(n_\alpha - k)(n_\alpha - k)(n_\alpha - k)}{2} \), \( n_\alpha(p + 1) - (n_\alpha - k)(n_\alpha - k)(n_\alpha - k)(n_\alpha - k)(n_\alpha - k)(n_\alpha - k)(n_\alpha - k)(n_\alpha - k)(n_\alpha - k)(n_\alpha - k)(n_\alpha - k) \) and \((n_\alpha - k)(n_\alpha - k)(n_\alpha - k)(n_\alpha - k)(n_\alpha - k)(n_\alpha - k)(n_\alpha - k)(n_\alpha - k)(n_\alpha - k)(n_\alpha - k)(n_\alpha - k)) \) respectively.

Suppose that \( 1 \neq g \) defines a line which intersects the curve at \( m \) rational points where \( m = 0, 1, 2, 3 \). We have

\[
K_G(g) = (1, m(p - 1), (p + 1 - m)(p - 1))
\]

and

\[
V_G(g) = (0, (n_\alpha - m)(p - 1), (p^2 + m - n_\alpha)(p - 1)).
\]
5 Acknowledgements

I would like to thank Christopher Voll for his support, guidance and insight throughout this project and for numerous helpful discussions.

References

[1] M. Abért. On the probability of satisfying a word in a group. *J. Group Theory*, 9(5):685–694, 2006.

[2] N. Boston and I. M. Isaacs. Class numbers of $p$-groups of a given order. *J. Algebra*, 279(2):810–819, 2004.

[3] M. Boyarchenko and M. Sabitova. The orbit method for profinite groups and a $p$-adic analogue of brown’s theorem. *Israel J. Math.*, 165:67–91, 2008.

[4] J. D. Dixon, L. Pyber, Á. Seress, and A. Shalev. Residual properties of free groups and probabilistic methods. *J. reine angew. Math. (Crelle’s)*, 556:159–172, 2003.

[5] S. Garion and A. Shalev. Commutator maps, measure preservation and T-systems. *Trans. Amer. Math. Soc.*, 361(9):4631–4351, 2009.

[6] J. González-Sánchez. Kirillov’s orbit method for $p$-groups and pro-$p$ groups. *Comm. Algebra*, 37(12):4476–4488, 2009.

[7] I. M. Isaacs. *Character Theory of Finite Groups*, volume 359. American Math. Soc., 1976.

[8] A. Jaikin-Zapirain. Zeta function of representations of compact $p$-adic analytic groups. *J. Amer. Math. Soc.*, (19):91–118, 2006.

[9] E. I. Khukhro. $p$-automorphisms of finite $p$-groups, volume 246 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1198.

[10] M. Larsen and A. Shalev. Fibres of word maps and some applications. *J. Algebra*, 354:36–48, 2012.

[11] M. Levy. On the probability of solving a word in nilpotent groups of class 2. (arxiv 1101.4286v1).

[12] E. A. O’Brien and C. Voll. Enumerating classes and characters of $p$-groups. *Trans. Amer. Math. Soc.*, 367:7775–7796, 2015.