COMPOSITIO MATHEMATICA

Kirillov's orbit method and polynomiality of the faithful dimension of p-groups

Mohammad Bardestani, Keivan Mallahi-Karai and Hadi Salmasian

Compositio Math. **155** (2019), 1618–1654.

doi:10.1112/S0010437X19007462

Compositio Math. 155 (2019) 1618–1654
doi:10.1112/S0010437X19007462

Kirillov's orbit method and polynomiality of the faithful dimension of *p*-groups

Mohammad Bardestani, Keivan Mallahi-Karai and Hadi Salmasian

Dedicated to Mehrdad Shahshahani

Abstract

Given a finite group G and a field K, the *faithful dimension* of G over K is defined to be the smallest integer n such that G embeds into $\mathrm{GL}_n(K)$. We address the problem of determining the faithful dimension of a p-group of the form $\mathscr{G}_q := \exp(\mathfrak{g} \otimes_{\mathbb{Z}} \mathbb{F}_q)$ associated to $\mathfrak{g}_q := \mathfrak{g} \otimes_{\mathbb{Z}} \mathbb{F}_q$ in the Lazard correspondence, where $\mathfrak{g}$ is a nilpotent $\mathbb{Z}$-Lie algebra which is finitely generated as an abelian group. We show that in general the faithful dimension of $\mathscr{G}_p$ is a piecewise polynomial function of p on a partition of primes into Frobenius sets. Furthermore, we prove that for p sufficiently large, there exists a partition of $\mathbb{N}$ by sets from the Boolean algebra generated by arithmetic progressions, such that on each part the faithful dimension of $\mathscr{G}_q$ for $q := p^f$ is equal to $fg(p^f)$ for a polynomial $g(T)$. We show that for many naturally arising p-groups, including a vast class of groups defined by partial orders, the faithful dimension is given by a single formula of the latter form. The arguments rely on various tools from number theory, model theory, combinatorics and Lie theory.

1. Introduction

Let G be a finite group and let K be a field. The *faithful dimension* of G over K, denoted by $m_{\mathrm{faithful},K}(\mathrm{G})$, is defined to be the smallest possible dimension of a faithful K-representation of G. The question of computing or estimating $m_{\mathrm{faithful},K}(\mathrm{G})$ has found many applications. For instance, it is intimately connected to computing the essential dimension $\mathrm{ed}_K(\mathrm{G})$ of G, defined by Buhler and Reichstein [BR97], which is the smallest dimension of a linearizable G-variety with a faithful G-action. It is known [BF13, Proposition 4.15] that $\mathrm{ed}_K(\mathrm{G}) \leqslant m_{\mathrm{faithful},K}(\mathrm{G})$ for every finite group G. Karpenko and Merkurjev [KM08] proved that if G is a p-group and K contains a primitive pth root of unity, then $\mathrm{ed}_K(\mathrm{G}) = m_{\mathrm{faithful},K}(\mathrm{G})$. For further details the reader may wish to consult [Mer17].

Note that by a result of Brauer, every complex representation of a p-group G is defined over $\mathbb{Q}(\zeta)$, where ζ is a primitive $|\mathrm{G}|$th root of unity. This implies that $m_{\mathrm{faithful},K}(\mathrm{G}) = m_{\mathrm{faithful},\mathbb{C}}(\mathrm{G})$ whenever $K \supseteq \mathbb{Q}(\zeta)$. Therefore we will only consider complex representations and use the shorthand $m_{\mathrm{faithful}}(\mathrm{G})$ instead of $m_{\mathrm{faithful},\mathbb{C}}(\mathrm{G})$.

Received 21 December 2017, accepted in final form 10 April 2019.
2010 Mathematics Subject Classification 20G05 (primary), 20C15, 14G05 (secondary).
Keywords: faithful dimension of finite groups, Kirillov's orbit method, Lazard correspondence, Frobenius sets, free nilpotent Lie algebras.

Throughout the preparation of this paper, M.B. was supported by Emmanuel Breuillard's ERC grant 'GeTeMo', K.M.-K. was partially supported by the DFG grant DI506/14-1, and H.S. was supported by NSERC Discovery Grants RGPIN-2013-355464 and RGPIN-2018-04044.

This work is a continuation of [BMS16] in which the faithful dimension of a large class of p-groups was studied. Let us start by recalling some of the results from [BMS16]. Let F be a non-Archimedean local field with a discrete valuation ν. We will denote the ring of integers of F by $\mathcal{O}$, the unique maximal ideal of $\mathcal{O}$ by $\mathfrak{p}$, and the residue field $\mathcal{O}/\mathfrak{p}$ by $\mathbb{F}_q$, the finite field of order $q := p^f$, where f is the *absolute inertia degree* of F. The number $e = \nu(p)$ is called the *absolute ramification index* of F.

For a (commutative and unital) ring R and an integer $k \geqslant 1$, the kth *Heisenberg group* with entries in R, denoted by $\mathrm{Heis}_{2k+1}(\mathrm{R})$, consists of $(k+2) \times (k+2)$ matrices of the form $I_{k+2} + A$, where A is strictly upper triangular and all of its entries other than those on the first row and the last column are zero. Similarly, $\mathrm{U}_k(\mathrm{R})$ denotes the subgroup of unitriangular matrices in $\mathrm{GL}_k(\mathrm{R})$, so that $H_{2k+1}(\mathrm{R}) \subseteq U_{k+2}(\mathrm{R})$. In [BMS16, Theorem 1.1] we proved that

$$m_{\mathrm{faithful}}(\mathrm{Heis}_{2k+1}(\mathcal{O}/\mathfrak{p}^n)) = \sum_{i=0}^{\xi-1} f q^{k(n-i)}, \tag{1}$$

where $\xi = \min\{e, n\}$. Also, when $\mathrm{char}(\mathcal{O}/\mathfrak{p}) \neq 2$, in [BMS16, Theorem 1.2] we showed that

$$m_{\mathrm{faithful}}(\mathrm{G}) = m_{\mathrm{faithful}}(\mathrm{Heis}_{2k+1}(\mathcal{O}/\mathfrak{p}^n)),$$

for any subgroup G of $\mathrm{U}_{k+2}(\mathcal{O}/\mathfrak{p}^n)$ that contains $\mathrm{Heis}_{2k+1}(\mathcal{O}/\mathfrak{p}^n)$. In particular for $F = \mathbb{F}_p((T))$, where $p \geqslant 3$, we obtained

$$m_{\mathrm{faithful}}(\mathrm{U}_k(\mathbb{F}_p[[T]]/(T^n))) = \sum_{i=0}^{n-1} p^{(k-2)(n-i)} \quad \text{for all } k \geqslant 3.$$

The latter statement implies that if $p \geqslant 3$ then

$$m_{\mathrm{faithful}}(\mathrm{U}_k(\mathbb{F}_p)) = p^{k-2} \quad \text{for all } k \geqslant 3. \tag{2}$$

The right-hand side of (2) is a polynomial in p. Note that $\mathrm{U}_k(\mathbb{F}_p) = \exp(\mathfrak{u}_k \otimes \mathbb{F}_p)$, where $\mathfrak{u}_k$ is the Lie algebra of strictly upper triangular matrices with entries in $\mathbb{Z}$ (for the definition of the exponential map in this context, see § 2). Equation (2) suggests the following problem.

Problem 1.1 (Polynomiality problem). Among all nilpotent $\mathbb{Z}$-Lie algebras $\mathfrak{g}$ which are finitely generated as abelian groups, characterize those for which there exists a polynomial $g(T)$, only depending on $\mathfrak{g}$, such that

$$m_{\mathrm{faithful}}(\exp(\mathfrak{g} \otimes_{\mathbb{Z}} \mathbb{F}_p)) = g(p),$$

for all sufficiently large primes p.

This problem is the central guiding principle of this work. Before stating our results, let us mention that the methods applied in [BMS16] were based on a suitably adapted version of the Stone–von Neumann theory, whose application is mostly limited to groups of nilpotency class 2. In this paper, we will replace the Stone–von Neumann theory by *Kirillov's orbit method* for finite p-groups. The orbit method was initially introduced by Kirillov [Kir62] to study unitary representations of nilpotent Lie groups. This machinery was later adapted to other classes of groups, such as p-adic analytic groups, finitely generated nilpotent groups, and finite p-groups (see [How77b, How77a] and [Kaz77, Proposition 1]). Jaikin-Zapirain [Jai06] used this machinery to study the representation zeta functions of compact p-adic analytic groups. These zeta functions

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

have also been studied by Avni *et al.* [AKOV13]. We refer the reader to these papers and references therein for more details.

Our approach to Problem 1.1 relies heavily on the notion of the *commutator matrix* associated to a nilpotent $\mathbb{Z}$-Lie algebra. Since its introduction in the work of Grunewald and Segal [GS84] as a tool for classification of torsion-free finitely generated nilpotent groups, the notion of the commutator matrix has been used in studying a large variety of problems related to finite and infinite groups. Voll [Vol05, Vol04] has used commutator matrices in his works on normal subgroup lattices of nilpotent groups. Stasinski and Voll [SV14] also employed them to study the representation growth of infinite groups. In addition, O'Brien and Voll [O'BV15] used commutator matrices for counting conjugacy classes and characters of certain finite p-groups. In our work, we relate the faithful dimension of finite p-groups to the question of existence of sufficiently many points in general position on rank varieties associated with the commutator matrices that were considered by O'Brien and Voll.

2. Main results

Before we state our results we will need to set some notation. Let $\mathfrak{g}$ be a Lie algebra over a commutative ring R. For $x \in \mathfrak{g}$, the map defined by $y \mapsto [x, y]$ is denoted by ad_x. Let $(\mathfrak{g}^l)_{l\geqslant 1}$ denote the *descending central series* of $\mathfrak{g}$. In other words we set $\mathfrak{g}^1 := \mathfrak{g}$, and we define $\mathfrak{g}^{l+1}$ for $l \geqslant 1$ inductively, as the R-submodule of $\mathfrak{g}$ generated by commutators of the form $[x, y]$, where $x \in \mathfrak{g}$ and $y \in \mathfrak{g}^l$. The commutator subalgebra of $\mathfrak{g}$ will be denoted by $\mathfrak{g}'$. Note that $\mathfrak{g}' = \mathfrak{g}^2$. The Lie algebra $\mathfrak{g}$ is said to be *nilpotent* if $\mathfrak{g}^{c+1} = 0$ for some $c \in \mathbb{N}$. If c is the smallest integer with this property, then $\mathfrak{g}$ is said to be *c-step nilpotent* or *nilpotent of class c*.

Suppose now that $\mathfrak{g}$ is a finite $\mathbb{Z}$-Lie algebra whose cardinality is a power of p, and assume that $\mathfrak{g}$ is nilpotent of class $c < p$. One may define a group operation on $\mathfrak{g}$ by the Campbell–Baker–Hausdorff formula: for all $x, y \in \mathfrak{g}$ we define the group multiplication by

$$x * y := \sum_{n>0} \frac{(-1)^{n+1}}{n} \sum_{\substack{(a_1,b_1),\dots,(a_n,b_n)\\ a_j+b_j\geqslant 1}} \frac{\left(\sum_{1\leqslant i\leqslant n} a_i + b_i\right)^{-1}}{a_1!b_1!\cdots a_n!b_n!} (\mathrm{ad}_x)^{a_1}(\mathrm{ad}_y)^{b_1}\cdots(\mathrm{ad}_x)^{a_n}(\mathrm{ad}_y)^{b_n-1}(y),$$

where if $b_n = 0$ then the last term $(\mathrm{ad}_y)^{b_n-1}(y)$ is dropped. Plainly, if $b_n > 1$, or if $b_n = 0$ and $a_n > 1$, then the corresponding summand vanishes. Note that the above sum is finite, because $\mathfrak{g}$ is nilpotent. The group defined in this way is denoted by $\exp(\mathfrak{g})$. For instance, when $\mathfrak{g}$ is 2-step nilpotent and $p \geqslant 3$, the group multiplication of $\exp(\mathfrak{g})$ takes the simple form

$$x * y = x + y + \tfrac{1}{2}[x, y],$$

and when $\mathfrak{g}$ is 3-step nilpotent and $p \geqslant 5$ we obtain

$$x * y = x + y + \tfrac{1}{2}[x, y] + \tfrac{1}{12}[x, [x, y]] + \tfrac{1}{12}[y, [y, x]].$$

Similar formulas can be written for any given nilpotency class when p is large enough. The group $\exp(\mathfrak{g})$ defined above is a p-group of nilpotency class c. In fact Lazard proved [Khu88, ch. 9] that every p-group G of nilpotency class $c < p$ arises in this way from a unique Lie algebra $\mathfrak{g} := \mathrm{Lie}(G)$.

From now on, for a c-step nilpotent $\mathbb{Z}$-Lie algebra $\mathfrak{g}$ which is finitely generated as an abelian group, and for $q := p^f$ with $p > c$, we set

$$\mathfrak{g}_q := \mathfrak{g} \otimes_{\mathbb{Z}} \mathbb{F}_q \quad \text{and} \quad \mathscr{G}_q := \exp(\mathfrak{g}_q),$$

where $\mathbb{F}_q$ is the finite field with q elements.

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

2.1 A palette of possibilities

To illustrate the range of possibilities that can arise, we will start this section with three examples, and then state our main results. We will elaborate on these examples in § 5.

Example 2.1 (Elliptic curve). Let a be a non-zero integer. Consider the $\mathbb{Z}$-Lie algebra $\mathfrak{g}_a$, introduced by Boston and Isaacs [BI04, § 3], which is spanned as a free $\mathbb{Z}$-module by $\{v_1, \dots, v_9\}$, subject to the relations

$$[v_1, v_4] = [v_2, v_5] = [v_3, v_6] = v_7, \quad [v_1, v_5] = [v_2, v_6] = v_8, \quad [v_1, v_6] = av_9, \quad [v_2, v_4] = [v_3, v_4] = v_9.$$

All other brackets $[v_i, v_j]$ with $i < j$ vanish. It will be shown in § 5.2 that if p is a sufficiently large prime ($p > 1800$ will suffice) and p does not divide a, then

$$m_{\text{faithful}}(\exp(\mathfrak{g}_a \otimes_{\mathbb{Z}} \mathbb{F}_p)) = 3p^2.$$

As we will see in the proof, the uniformity in p is related to the fact that for such values of p the cubic curve $Y^2 = 4aX^3 + X^2 - 4X$ has a non-zero rational point over $\mathbb{F}_p$. Note that in this example, aside from a finite set of primes, the value of $m_{\text{faithful}}(\exp(\mathfrak{g}_a \otimes_{\mathbb{Z}} \mathbb{F}_p))$ is given by one polynomial in p.

Example 2.2 (Binary quadratic form). Consider the $\mathbb{Z}$-Lie algebra $\mathfrak{g}$ spanned as a free $\mathbb{Z}$-module by $\{v_1, \dots, v_6\}$ subject to the relations

$$[v_1, v_2] = [v_3, v_4] = v_5, \quad [v_1, v_4] = [v_2, v_3] = v_6,$$

where all other commutators $[v_i, v_j]$ with $i < j$ are defined to be 0. Then in § 5.3 we will show that for odd primes p, the value of $m_{\text{faithful}}(\mathscr{G}_p)$ is given by two different polynomials along two arithmetic progressions, namely,

$$m_{\text{faithful}}(\mathscr{G}_p) = \begin{cases} 2p & \text{if } p \equiv 1 \pmod 4, \\ 2p^2 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Put more formally, set

$$\mathscr{P}_1 := \{p \geqslant 3 : p \equiv 1 \pmod 4\} \quad \text{and} \quad \mathscr{P}_2 := \{p \geqslant 3 : p \equiv 3 \pmod 4\}.$$

Also, set $g_1(T) := 2T$ and $g_2(T) := 2T^2$. Then $m_{\text{faithful}}(\mathscr{G}_p) = g_i(p)$ for all $p \in \mathscr{P}_i$, $i = 1, 2$.

As the next example shows, even this is not the end of the story.

Example 2.3 (Binary cubic form). Consider the $\mathbb{Z}$-Lie algebra $\mathfrak{g}$ spanned as a free $\mathbb{Z}$-module by $\{v_1, \dots, v_8\}$ with the following relations:

$$[v_1, v_4] = [v_2, v_5] = [v_3, v_6] = v_7, \quad [v_1, v_5] = [v_2, v_6] = [v_3, v_5] = v_8, \quad [v_3, v_4] = -v_8.$$

All other commutators $[v_i, v_j]$ with $i < j$ vanish. Let p be an odd prime. In § 5.4 we will show that

$$m_{\text{faithful}}(\mathscr{G}_p) = \begin{cases} p^2 + p^3 & \text{if } \left(\dfrac{p}{23}\right) = -1, \\ 2p^3 & \text{if } p \text{ is represented by the form } 2x^2 + xy + 3y^2, \\ 2p^2 & \text{if } p \text{ is represented by the form } x^2 + xy + 6y^2 \quad \text{or} \quad p = 23, \end{cases}$$

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol. The conditions defining this function split the set of prime numbers $p \geqslant 3$ into disjoint sets $\mathscr{P}_1$, $\mathscr{P}_2$ and $\mathscr{P}_3$. On each one of these sets, one of the polynomials $g_1(T) = T^2 + T^3$, $g_2(T) = 2T^3$ and $g_3(T) = 2T^2$ is applicable. It is worth mentioning that by Gauss genus theory, the sets $\mathscr{P}_2$ and $\mathscr{P}_3$ are *not* unions of arithmetic progressions (for example see [Kus67]).

Example 2.4 (Lee's Lie algebra). Consider the $\mathbb{Z}$-Lie algebra $\mathfrak{g}$ spanned as a free $\mathbb{Z}$-module by $\{v_1, \dots, v_8\}$ with the following relations:

$$[v_1, v_4] = [v_2, v_5] = v_6, \quad 2[v_1, v_5] = [v_3, v_4] = 2v_7, \quad [v_2, v_4] = [v_3, v_5] = v_8.$$

All other commutators $[v_i, v_j]$ with $i < j$ vanish. This Lie algebra was defined in [Lee16]. Let p be an odd prime. In § 5.5 we will show that

$$m_{\text{faithful}}(\mathscr{G}_p) = \begin{cases} p + 2p^2 & \text{if } p \equiv 2 \pmod 3 \text{ or } p = 3, \\ 3p & \text{if } p \equiv 1 \pmod 3 \text{ and } p \text{ is represented by the form } x^2 + 27y^2, \\ 3p^2 & \text{if } p \equiv 1 \pmod 3 \text{ and } p \text{ is not represented by the form } x^2 + 27y^2. \end{cases}$$

We remark that in [Lee16], the author computes the order of the automorphism group of the Lie algebra $\mathfrak{g}_p$. The formula obtained in [Lee16] is given by different polynomials depending on the splitting of $\lambda^3 - 2$ in $\mathbb{F}_p$, and therefore its cases are parallel to the ones that appear above.

The important point to note here is that in each one of the above examples, the set of primes can be decomposed into finitely many *arithmetically defined* sets, such that the value of $m_{\text{faithful}}(\mathscr{G}_p)$ on each one of these sets is given by a polynomial. Let us explain this in more detail. For a polynomial $g(T) \in \mathbb{Z}[T]$, denote by $\mathcal{V}_g$ the set of primes p for which the congruence $g(T) \equiv 0 \pmod p$ has a solution. We will call $\mathcal{V}_g$ an *elementary Frobenius set*. Let $\mathbb{P}$ denote the set of prime numbers. By a *Frobenius set* we mean an element of the Boolean algebra inside the power set of $\mathbb{P}$ that is generated by elementary Frobenius sets. In other words, a Frobenius set is a finite union of sets of the form

$$\mathcal{V}_{g_1} \cap \cdots \cap \mathcal{V}_{g_k} \cap \mathcal{V}_{g_{k+1}}^c \cap \cdots \cap \mathcal{V}_{g_l}^c.$$

We remark that every Frobenius set is a *Frobenian set*, as defined by Serre [Ser12, § 3.3.1], but the converse does not hold. For more details about the connection between Frobenius and Frobenian sets, see [Lag83].

For $p > 2$ the equation $x^2 + 1 = 0$ has a solution in $\mathbb{F}_p$ if and only if $p \equiv 1 \pmod 4$. This shows that the sets appearing in Example 2.2 are Frobenius sets. One can see that the sets $\mathscr{P}_i$ in Example 2.3 are Frobenius sets as follows. First, using the quadratic reciprocity law one can easily verify that the set $\mathscr{P}_1$ consists of those primes $p \geqslant 3$ for which the equation $x^2 + 23$ has no solution in $\mathbb{F}_p$. The other two parts are based on the less trivial fact that $p \geqslant 3$ can be represented by the quadratic form $a^2 + ab + 6b^2$ (respectively, $2a^2 + ab + 3b^2$) if and only if $p \notin \mathscr{P}_1$ and $x^3 - x - 1$ has a solution (respectively, no solution) in $\mathbb{F}_p$. Consequently, each $\mathscr{P}_i$ is a Frobenius set.

Let $\mathscr{P}$ be any set of primes. The *Dirichlet density* of $\mathscr{P}$ is defined by

$$d(\mathscr{P}) := \lim_{s \to 1^+} \frac{\sum_{p \in \mathscr{P}} p^{-s}}{\sum_{p \in \mathbb{P}} p^{-s}},$$

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

if the limit exists. The Chebotarev density theorem implies that any infinite Frobenius set has a positive Dirichlet density. It follows from Dirichlet's theorem on primes in arithmetic progressions that the Dirichlet density of the sets $\mathscr{P}_i$ in Example 2.2 is positive. For the sets $\mathscr{P}_i$ in Example 2.3, positivity of the Dirichlet density can be proved by class field theory. For more details we refer the reader to [Cox13, Theorem 9.12].

With this preparation, we are now ready to state our first result.

THEOREM 2.5. *Let $\mathfrak{g}$ be a nilpotent $\mathbb{Z}$-Lie algebra of nilpotency class c which is finitely generated as an abelian group. Then there exist a partition $\mathscr{P}_1, \dots, \mathscr{P}_r$ of the set of prime numbers larger than c into Frobenius sets, and polynomials $g_1(T), \dots, g_r(T)$ with non-negative integer coefficients, depending only on $\mathfrak{g}$, such that*

$$m_{\text{faithful}}(\mathscr{G}_p) = g_i(p) \quad \text{for all } p \in \mathscr{P}_i,$$

where $1 \leqslant i \leqslant r$.

The proof of this theorem relies on a theorem of Ax [Ax67] from model theory (see also van den Dries [VdDri91]), coupled with a parameterization of irreducible representations provided by the Kirillov machinery. As we shall see, studying $m_{\text{faithful}}(\mathscr{G}_p)$ leads to questions related to the existence of rational points over finite fields of certain determinantal varieties associated with the commutator matrix. We remark that our proof is effective and we can use its method to describe the associated Frobenius sets and polynomials. We will demonstrate this by a detailed analysis of the above examples after we give the proof of Theorem 2.5.

One can also consider $m_{\text{faithful}}(\mathscr{G}_q)$ for $q := p^f$ when the prime p is fixed and f varies. Let $\mathscr{P}$ be one of the Frobenius sets in Theorem 2.5 with the associated polynomial $g(T) \in \mathbb{Z}[T]$. The following example shows that it is not necessarily true that

$$m_{\text{faithful}}(\mathscr{G}_q) = fg(q) \quad \text{for all } f \geqslant 1.$$

Example 2.6. Take $\mathfrak{g}$ as in Example 2.2 and set $\mathscr{P} := \mathscr{P}_2$, where $\mathscr{P}_2$ is as in the same example. Recall that

$$m_{\text{faithful}}(\mathscr{G}_p) = 2p^2 \quad \text{for all } p \in \mathscr{P}.$$

However, in § 5.3 we shall demonstrate that

$$m_{\text{faithful}}(\mathscr{G}_q) = \begin{cases} 2fq & f \text{ is even,} \\ 2fq^2 & f \text{ is odd.} \end{cases}$$

Nevertheless, we prove the following theorem which shows that in general, the behaviour of $m_{\text{faithful}}(\mathscr{G}_q)$ for $q := p^f$ with p fixed is very similar to the above example.

THEOREM 2.7. *Let $\mathfrak{g}$ be a nilpotent $\mathbb{Z}$-Lie algebra of nilpotency class c which is finitely generated as an abelian group. Fix a prime $p > C$, where C is the constant given in (31). Then there exist a partition $\mathscr{A}_1, \dots, \mathscr{A}_r$ of the set of natural numbers, and polynomials $g_1(T), \dots, g_r(T)$ with non-negative integer coefficients, depending on p and $\mathfrak{g}$, such that:*

(1) *each $\mathscr{A}_i$, $1 \leqslant i \leqslant r$, is a union of a finite set and finitely many arithmetic progressions;*
(2) *for all $1 \leqslant i \leqslant r$, if $q = p^f$ where $f \in \mathscr{A}_i$, then $m_{\text{faithful}}(\mathscr{G}_q) = fg_i(q)$.*

The proof of Theorem 2.7 uses Dwork's theorem on rationality of zeta functions of varieties and the Skolem–Mahler–Lech theorem.

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

Remark 2.8. It would be interesting to obtain a uniform generalization of Theorems 2.5 and 2.7.

At this point two remarks are in order. On the one hand, Theorems 2.5 and 2.7 set an upper limit on how complicated the value of $m_{\text{faithful}}(\mathscr{G}_q)$ as a function of p and f can be. It would be desirable to know to what extent the collection of functions appearing in Theorem 2.5 can be realized as $m_{\text{faithful}}(\mathscr{G}_q)$ for some Lie algebra $\mathfrak{g}$. On the other hand, one may still hope that at least for a large class of naturally arising Lie algebras $\mathfrak{g}$, the function $m_{\text{faithful}}(\mathscr{G}_q)$ is given by a *single* polynomial. In the next section we address these two problems.

2.2 Pattern groups

Let us begin this section by introducing a large class of nilpotent groups which can be viewed as a generalization of the nth Heisenberg group $\text{Heis}_{2n+1}(\mathbb{F}_q)$ defined in the introduction.

Set $[n] := \{1, 2, \dots, n\}$, and let $([n], \prec)$ be a partially ordered set. Without loss of generality, we can assume that if $i \prec j$ then $i < j$. To this partial order we assign the *pattern Lie algebra*

$$\mathfrak{g}_\prec := \text{Span}_{\mathbb{Z}}\{\mathbf{e}_{ij} : i \prec j\} \subseteq \mathfrak{gl}(n, \mathbb{Z}),$$

where $\mathbf{e}_{ij}$ denotes the $n \times n$ matrix whose unique non-zero entry is a 1 in the (i, j) position.

Note that $\mathfrak{g}_\prec$ is nilpotent since the commutator relation

$$[\mathbf{e}_{ij}, \mathbf{e}_{kl}] = \delta_{jk}\mathbf{e}_{il} - \delta_{li}\mathbf{e}_{kj}$$

ensures that $\mathfrak{g}_\prec$ is a subalgebra of the Lie algebra $\mathfrak{u}_n$ of strictly upper-triangular n by n matrices. For instance, the $(2n+1)$-dimensional Heisenberg Lie algebra corresponds to the partial order

$$1 \prec 2, 3, \dots, n+1 \prec n+2. \tag{3}$$

For all $i \prec j$ define

$$\alpha(i, j) := \#\{k \in [n] : i \prec k \prec j\}.$$

Moreover, the *length* of $([n], \prec)$, denoted by $\lambda_\prec$, is defined to be the maximum value of r such that there exists a chain $i_0 \prec \cdots \prec i_r$ in $([n], \prec)$. For instance the length of the partial order given in (3) is equal to 2. We remark that $\lambda_\prec$ is equal to the nilpotency class of $\mathfrak{g}_\prec$ (see Lemma 4.1).

Definition 2.9. An ordered pair (i, j) is called an *extreme pair* if i is a minimal element in $([n], \prec)$, j is a maximal element in $([n], \prec)$, and $i \prec j$. The set of extreme pairs will be denoted by I_{ex}.

We can now state our theorem on the faithful dimension of pattern groups.

Theorem 2.10. *Let $\prec$ be a partial order of length $\lambda_\prec$ on the set $[n]$, and let $q := p^f$ where $p > \lambda_\prec$. Then*

$$m_{\text{faithful}}(\exp(\mathfrak{g}_\prec \otimes_{\mathbb{Z}} \mathbb{F}_q)) = \sum_{(i,j)\in I_{\text{ex}}} f q^{\alpha(i,j)}.$$

Theorem 2.10 generalizes (2), and its proof relies on Kirillov theory and more specifically on an explicit description of the size of coadjoint orbits in terms of combinatorial data of the partial order. Note that by Theorems 2.5 and 2.7, *a priori* there is no reason to expect the faithful dimension to be given by a *single* formula of the form $fg(p^f)$ for a polynomial $g(T)$. Theorem 2.10 is proved by a detailed analysis of the size of coadjoint orbits and a combinatorial lemma due to Rado and Horn.

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

Question 2.11. Let F be a non-Archimedean local field with the ring of integers $\mathcal{O}$, the unique maximal ideal $\mathfrak{p}$ and the associated residue field $\mathbb{F}_q$. Is it true that $m_{\text{faithful}}(\exp(\mathfrak{g}_{\prec} \otimes_{\mathbb{Z}} \mathcal{O}/\mathfrak{p}^n))$ is given by the formula

$$\sum_{\ell=0}^{\xi-1} \sum_{(i,j)\in I_{\text{ex}}} f q^{(n-\ell)\alpha(i,j)}, \quad \xi = \min\{n, e\}, \tag{4}$$

where f is the absolute inertia degree and e is the absolute ramification index of F? Formula (4) is suggested by (1) and Theorem 2.10.

An immediate consequence of Theorem 2.10 is the following corollary.

COROLLARY 2.12. *For any non-zero polynomial $g(T) \in \mathbb{Z}[T]$ with non-negative coefficients, there exists a nilpotent $\mathbb{Z}$-Lie algebra $\mathfrak{g}$ which is finitely generated as an abelian group such that*

$$m_{\text{faithful}}(\mathscr{G}_q) = f g(q),$$

when $p \geqslant \deg g(T) + 2$ and $f \geqslant 1$.

2.3 Relatively free nilpotent groups

In this section we will turn to free objects in certain categories of nilpotent Lie algebras. Let $\mathfrak{f}_{n,c} := \mathfrak{f}_{n,c}(\mathbb{Z})$ be the free nilpotent $\mathbb{Z}$-Lie algebra on n generators and of class c; it is defined to be the quotient algebra $\mathfrak{f}_n/\mathfrak{f}_n^{c+1}$, where $\mathfrak{f}_n$ is the free $\mathbb{Z}$-Lie algebra on n generators, and $\mathfrak{f}_n^{c+1}$ denotes the $(c+1)$th term in the lower central series of $\mathfrak{f}_n$ starting with $\mathfrak{f}_n^1 = \mathfrak{f}_n$. It is well known that the rank of the quotient $\mathfrak{f}_n^c/\mathfrak{f}_n^{c+1}$ (as a $\mathbb{Z}$-module) is given by Witt's formula

$$r_n(c) := \frac{1}{c} \sum_{d|c} \mu(d) n^{c/d},$$

where μ is the Möbius function. Using the orbit method one can prove that

$$m_{\text{faithful}}(\exp(\mathfrak{f}_{n,c} \otimes_{\mathbb{Z}} \mathbb{F}_q)) \geqslant r_n(c) f q.$$

This lower bound is sharp for $\mathfrak{f}_{n,2}$ and $\mathfrak{f}_{n,3}$.

THEOREM 2.13. *Let $n \geqslant 2$ and let $\mathbb{F}_q$ be the finite field with $q = p^f$ elements. Then, we have:*

(1) $m_{\text{faithful}}(\exp(\mathfrak{f}_{n,2} \otimes_{\mathbb{Z}} \mathbb{F}_q)) = ((n^2 - n)/2) f q$ *for* $p \geqslant 3$;
(2) $m_{\text{faithful}}(\exp(\mathfrak{f}_{n,3} \otimes_{\mathbb{Z}} \mathbb{F}_q)) = ((n^3 - n)/3) f q$ *for* $p \geqslant 5$.

The proofs of these results involve explicit computations with Hall bases and rely on a subtle combinatorial optimization.

Remark 2.14. For $2 \leqslant c \leqslant 6$, the value of $m_{\text{faithful}}(\exp(\mathfrak{f}_{2,c} \otimes_{\mathbb{Z}} \mathbb{F}_p))$ is given by Table 1.

In § 7.4, we outline the computations that yield the values of $m_{\text{faithful}}(\exp(\mathfrak{f}_{2,c} \otimes_{\mathbb{Z}} \mathbb{F}_p))$ in Table 1. However, we are not able to obtain any general formula for $m_{\text{faithful}}(\exp(\mathfrak{f}_{2,c} \otimes_{\mathbb{Z}} \mathbb{F}_p))$ in terms of c.

For a Lie algebra $\mathfrak{g}$, let $(D^k\mathfrak{g})_{k\geqslant 0}$ be the derived series of $\mathfrak{g}$. Thus $D^0\mathfrak{g} = \mathfrak{g}$, $D\mathfrak{g} = [\mathfrak{g}, \mathfrak{g}]$, and $D^{k+1}\mathfrak{g} = [D^k\mathfrak{g}, D^k\mathfrak{g}]$ for $k \geqslant 1$. Note that $\mathfrak{g}/D^2\mathfrak{g}$ is the largest metabelian quotient of $\mathfrak{g}$. When $\mathfrak{g} = \mathfrak{f}_{n,c}$, this quotient is called the free metabelian Lie algebra of class c on n generators and will be denoted by $\mathfrak{m}_{n,c}$.

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

Table 1. The faithful dimension for 2-generated relatively free nilpotent groups of small nilpotency.

c	Condition	$m_{\text{faithful}}(\exp(\mathfrak{f}_{2,c} \otimes_{\mathbb{Z}} \mathbb{F}_p))$
2	$p \geqslant 3$	p
3	$p \geqslant 5$	$2p$
4	$p \geqslant 5$	$3p$
5	$p \geqslant 7$	$2p^2 + 4p$
6	$p \geqslant 7$	$p^3 + 3p^2 + 5p$

Theorem 2.15. *Let $c \geqslant 2$. Then $m_{\text{faithful}}(\exp(\mathfrak{m}_{2,c} \otimes_{\mathbb{Z}} \mathbb{F}_q)) = (c-1)fq$ for $q := p^f$ with $p > c$.*

In the course of the proof of Theorem 2.15 we will see that computing the faithful dimension of $\exp(\mathfrak{m}_{2,c} \otimes_{\mathbb{Z}} \mathbb{F}_q)$ is linked to *rational normal curves*, that is, the image of the *Veronese map* given by

$$\nu_{c-2} : \mathbf{P}^1(\mathbb{F}_q) \to \mathbf{P}^{c-2}(\mathbb{F}_q), \quad [X_0 : X_1] \mapsto [X_0^{c-2} : X_0^{c-3}X_1 : \cdots : X_1^{c-2}].$$

This suggests that other tools (e.g. from the theory of determinantal varieties) might be relevant in the more general situation.

3. Preliminaries

In this section we introduce some notation and prove a number of basic facts which will be used throughout this paper. In particular, we will explain the connection between faithful representations and the central characters of their irreducible components. We will also briefly recall the orbit method.

Notation. Let G be a group with the identity element $\mathbf{1}$. The centre and the commutator subgroup of G will be denoted, respectively, by $\mathrm{Z}(\mathrm{G})$ and $\mathrm{G}' = [\mathrm{G}, \mathrm{G}]$. For an abelian p-group G, we write

$$\Omega_1(\mathrm{G}) := \{g \in \mathrm{G} : g^p = \mathbf{1}\},$$

which is a $\mathbb{Z}/p\mathbb{Z}$-vector space. The Pontryagin dual of an abelian group A, i.e. $\mathrm{Hom}(A, \mathbb{C}^*)$, will be denoted by $\widehat{A}$. Evidently, when A is an elementary abelian p-group, $\widehat{A}$ has a canonical $\mathbb{Z}/p\mathbb{Z}$-vector space structure. We denote the cardinality of a set S by $\#S$.

3.1 Central characters of faithful representations of p-groups

Let A be a finite abelian group. We denote the minimal number of generators of A by $d(A)$. For an exact sequence of finite abelian groups $0 \to A_1 \to A \to A_2 \to 0$, the numbers $d(A)$, $d(A_1)$ and $d(A_2)$ satisfy the inequalities

$$\max\{d(A_i) : i = 1, 2\} \leqslant d(A) \leqslant d(A_1) + d(A_2). \tag{5}$$

The number of invariant factors of A will be denoted by $d'(A)$. It can be easily seen from elementary divisor theory that $d'(A) = d(A)$. Evidently $m_{\text{faithful}}(A) \leqslant d'(A)$. Now for a given faithful representation $\rho : A \to \mathrm{GL}_m(\mathbb{C})$, by decomposing ρ into irreducible components and applying (5) we obtain $d(A) = d'(A) \leqslant m_{\text{faithful}}(A)$. This implies that

$$m_{\text{faithful}}(A) = d(A) = d'(A).$$

In particular, we obtain the following lemma.

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

LEMMA 3.1. *For a finite abelian p-group A,*

$$d(A) = d'(A) = m_{\text{faithful}}(A) = \dim_{\mathbb{Z}/p\mathbb{Z}}(A \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z}) = \dim_{\mathbb{Z}/p\mathbb{Z}}(\Omega_1(A)).$$

Let E be a finite elementary abelian p-group equipped with the canonical $\mathbb{Z}/p\mathbb{Z}$-vector space structure. Every one-dimensional representation $\chi : E \to \mathbb{C}^*$ factors uniquely as $\chi = \epsilon \circ \chi_\circ$, where $\chi_\circ \in \mathrm{Hom}(E, \mathbb{Z}/p\mathbb{Z})$ and the embedding $\epsilon : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}^*$ is defined by

$$\epsilon(x + p\mathbb{Z}) = \exp((2\pi i x)/p).$$

Hence the $\mathbb{Z}/p\mathbb{Z}$-linear map

$$\widehat{E} \to \mathrm{Hom}(E, \mathbb{Z}/p\mathbb{Z}), \quad \chi \mapsto \chi_\circ, \tag{6}$$

provides an isomorphism of $\mathbb{Z}/p\mathbb{Z}$-vector spaces between $\widehat{E}$ and $\mathrm{Hom}(E, \mathbb{Z}/p\mathbb{Z})$. Now, let G be a finite p-group. Applying (6) to $\Omega_1(\mathrm{Z}(G))$, we obtain the $\mathbb{Z}/p\mathbb{Z}$-isomorphism

$$\mathrm{Hom}(\Omega_1(\mathrm{Z}(\mathrm{G})), \mathbb{C}^*) \to \mathrm{Hom}(\Omega_1(\mathrm{Z}(\mathrm{G})), \mathbb{Z}/p\mathbb{Z}). \tag{7}$$

Hereafter the $\mathbb{Z}/p\mathbb{Z}$-vector space $\mathrm{Hom}(\Omega_1(\mathrm{Z}(\mathrm{G})), \mathbb{C}^*)$ will be denoted by $\widehat{\Omega}_1(\mathrm{Z}(\mathrm{G}))$.

Remark 3.2. Recall the standard fact that for a finite p-group G, every non-trivial normal subgroup of G intersects $\mathrm{Z}(\mathrm{G})$ and hence $\Omega_1(\mathrm{Z}(\mathrm{G}))$ non-trivially. Consequently, a representation of G is faithful if and only if its restriction to $\Omega_1(\mathrm{Z}(\mathrm{G}))$ is faithful.

We recall the following simple lemma.

LEMMA 3.3. *Let $L, L_1, \ldots, L_n$ be linear functionals on a vector space V with respective null spaces N, $N_1, \ldots, N_n$. Then L is a linear combination of $L_1, \ldots, L_n$ if and only if N contains the intersection $N_1 \cap \cdots \cap N_n$.*

The following observation, due to Meyer and Reichstein [MR10], will play a crucial role in computing the faithful dimension of p-groups.

LEMMA 3.4. *Let G be a finite p-group and let $(\rho_i, V_i)_{1 \leqslant i \leqslant n}$ be a family of irreducible representations of G with central characters χ_i. Assume that the set of characters*

$$\{\chi_{i|_{\Omega_1(\mathrm{Z}(\mathrm{G}))}} : 1 \leqslant i \leqslant n\}$$

spans $\widehat{\Omega}_1(\mathrm{Z}(\mathrm{G}))$. Then $\bigoplus_{1 \leqslant i \leqslant n} \rho_i$ is a faithful representation of G.

Proof. Since the set $\{\chi_{i|_{\Omega_1(\mathrm{Z}(\mathrm{G}))}} : 1 \leqslant i \leqslant n\}$ spans $\widehat{\Omega}_1(\mathrm{Z}(\mathrm{G}))$, from the $\mathbb{Z}/p\mathbb{Z}$-isomorphism (7) and Lemma 3.3 we obtain

$$\bigcap_{i=1}^{n} \ker \chi_{i|_{\Omega_1(\mathrm{Z}(\mathrm{G}))}} = \{\mathbf{1}\}.$$

Hence $\bigoplus_{1 \leqslant i \leqslant n} \rho_i$ is a faithful representation of $\Omega_1(\mathrm{Z}(\mathrm{G}))$. Remark 3.2 implies that $\bigoplus_{1 \leqslant i \leqslant n} \rho_i$ is a faithful representation of G. □

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

Lemma 3.5. *Let* G *be a finite* p*-group and let* ρ *be a faithful representation of* G *with the smallest possible dimension. Then* ρ *decomposes as a direct sum of exactly* $r := d(\mathrm{Z}(\mathrm{G}))$ *irreducible representations*

$$\rho = \rho_1 \oplus \cdots \oplus \rho_r.$$

Therefore the set of central characters $\{\chi_{i|_{\Omega_1(\mathrm{Z}(\mathrm{G}))}} : 1 \leqslant i \leqslant r\}$ *is a basis of* $\widehat{\Omega}_1(\mathrm{Z}(\mathrm{G}))$.

Proof. Let $\rho = \bigoplus_{1\leqslant i\leqslant n} \rho_i$ be the decomposition of ρ, and let χ_i, $1 \leqslant i \leqslant n$, denote the central character of ρ_i. Since ρ is faithful and $r = d(\mathrm{Z}(\mathrm{G}))$, it follows that $n \geqslant r$. Furthermore, faithfulness of ρ also implies $\bigcap_{i=1}^{n} \ker \chi_i = \{\mathbf{1}\}$. Hence, from Lemma 3.3, Lemma 3.4, and the minimality of $\dim(\rho)$ it follows that $n = r$ and also that the set

$$\{\chi_{i|_{\Omega_1(\mathrm{Z}(\mathrm{G}))}} : 1 \leqslant i \leqslant r\}$$

is a basis of $\widehat{\Omega}_1(\mathrm{Z}(\mathrm{G}))$. □

3.2 Kirillov's orbit method

The orbit method was introduced by Kirillov [Kir62] to study unitary representations of simply connected nilpotent Lie groups. For such a group G with Lie algebra $\mathfrak{g}$, this method provides an explicit bijection between the unitary dual $\widehat{\mathrm{G}}$ of G, and the set $\mathrm{Hom}^{\mathrm{cont}}(\mathfrak{g}, \mathbb{C}^*)/\mathrm{G}$ of orbits of the induced action of G on $\mathrm{Hom}^{\mathrm{cont}}(\mathfrak{g}, \mathbb{C}^*)$, called the coadjoint orbits. Since Kirillov's work, this method has been extended to study representations of nilpotent groups in other contexts. Relevant to this work is the version applicable to finite p-groups, which we now briefly explain. For more details we refer the reader to [BS08]. Let G be a p-group of nilpotency class $c < p$. By the Lazard correspondence, there exists a unique finite $\mathbb{Z}$-Lie algebra $\mathfrak{g} := \mathrm{Lie}(\mathrm{G})$ of cardinality $|\mathrm{G}|$ and nilpotency class c such that $\mathrm{G} \cong \exp(\mathfrak{g})$. Note that in the definition of $\exp(\mathfrak{g})$ the underlying set of the group is $\mathfrak{g}$ and the multiplication law is defined by the Campbell–Baker–Hausdorff formula. Usually we identify the underlying sets of the group G and the Lie algebra $\mathfrak{g}$. A simple application of the Campbell–Baker–Hausdorff formula shows that in this identification the centre of $\mathfrak{g}$ (as a Lie algebra) will be mapped onto the centre of G as a group.

Consider now the coadjoint action of G on $\widehat{\mathfrak{g}} := \mathrm{Hom}_{\mathbb{Z}}(\mathfrak{g}, \mathbb{C}^*)$, defined by

$$\theta^x(y) := \theta\left(\sum_{n=0}^{c} \frac{\mathrm{ad}_x^n(y)}{n!}\right),$$

where $x, y \in \mathfrak{g}$ and $\theta \in \widehat{\mathfrak{g}}$. Note that since $p > c$, the sum is well defined.

Theorem 3.6. *Assume that* $p \geqslant 3$ *and let* G *be a* p*-group of nilpotency class* $c < p$*. Furthermore, assume that* $\mathfrak{g} = \mathrm{Lie}(\mathrm{G})$*. Then there exists a bijection between* G*-orbits* $\Theta \subseteq \widehat{\mathfrak{g}}$ *and irreducible representations* $\rho_\Theta \in \widehat{\mathrm{G}}$ *such that Kirillov's character formula holds:*

$$\chi_\Theta(x) := \chi_{\rho_\Theta}(x) = |\Theta|^{-1/2} \sum_{\theta\in\Theta} \theta(x).$$

Proof. See [BS08, Theorem 2.6]. □

Remark 3.7. For an extension of Kirillov's orbit method to the case $p = 2$, see [SV14, Theorem 2.6].

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

Let $\Theta \subset \widehat{\mathfrak{g}}$ be the orbit of $\theta_0 \in \widehat{\mathfrak{g}}$. Then from Kirillov's character formula we see that the central character of ρ_Θ is $\theta_{0|_{\mathrm{Z}(\mathfrak{g})}}$ and

$$\dim(\rho_\Theta) = |\Theta|^{1/2} = [\mathfrak{g} : \mathrm{Stab}_{\mathrm{G}}(\theta_0)]^{1/2}. \tag{8}$$

PROPOSITION 3.8. *The stabilizer of θ_0 is given by*

$$\mathrm{Stab}_{\mathrm{G}}(\theta_0) = \{x \in \mathfrak{g} : \theta_0([x,y]) = 1 \ \forall y \in \mathfrak{g}\}. \tag{9}$$

Proof. One inclusion is obvious. For the inclusion $\subseteq$ note that

$$\mathrm{Stab}_{\mathrm{G}}(\theta_0) = \{x \in \mathfrak{g} : \theta_0^x(y) = \theta_0(y), \forall y \in \mathfrak{g}\} = \left\{x \in \mathfrak{g} : \theta_0\left(\sum_{n=0}^{c} \frac{\mathrm{ad}_x^n(y)}{n!}\right) = \theta_0(y), \forall y \in \mathfrak{g}\right\}.$$

Fix $x \in \mathrm{Stab}_{\mathrm{G}}(\theta_0)$. Then

$$\theta_0\left(\sum_{n=1}^{c} \frac{\mathrm{ad}_x^n(y)}{n!}\right) = 0 \quad \text{for all } y \in \mathfrak{g}. \tag{10}$$

Choose an arbitrary element $y \in \mathfrak{g}^{c-1}$. Since $\mathfrak{g}^{c+1} = 0$, it follows from (10) that $\theta_0(\mathrm{ad}_x(y)) = 0$. Next choose an arbitrary $y \in \mathfrak{g}^{c-2}$, and note that

$$\sum_{n=1}^{c} \frac{\mathrm{ad}_x^n(y)}{n!} = \mathrm{ad}_x(y) + \frac{\mathrm{ad}_x^2(y)}{2}.$$

In light of the previous step, $\theta_0(\mathrm{ad}_x(y)) = 0$. Continuing this process, the claim follows for all $y \in \mathfrak{g}$. □

Let us now illustrate the power of the orbit method by showing how it can be used to compute the faithful dimension of certain 2-step nilpotent groups.

PROPOSITION 3.9. *Let* G *be a 2-step nilpotent p-group, where $p \geqslant 3$. Assume that* $\mathrm{Z}(G)$ *is cyclic. Then* $m_{\mathrm{faithful}}(\mathrm{G}) = \sqrt{[\mathrm{G} : \mathrm{Z}(\mathrm{G})]}$.

Proof. Let ρ be a faithful representation of G of minimal dimension. Since the centre of G is cyclic, it follows from Lemma 3.5 that ρ is irreducible. By the Lazard correspondence $\mathrm{G} = \exp(\mathfrak{g})$, where $\mathfrak{g}$ is a finite Lie algebra of class 2. It suffices to show that $\dim \rho = \sqrt{[\mathfrak{g} : \mathrm{Z}(\mathfrak{g})]}$. Thanks to the orbit method, there exists $\theta_0 \in \widehat{\mathfrak{g}}$ such that

$$\chi_\rho(x) = \frac{1}{\sqrt{|\Theta|}} \sum_{\theta \in \Theta} \theta(x),$$

where Θ is the G-orbit of θ_0. Therefore

$$\dim \rho = \sqrt{|\Theta|} = \sqrt{[\mathfrak{g} : \mathrm{Stab}_{\mathrm{G}}(\theta_0)]}.$$

Recall that we identify $\mathrm{Z}(\mathrm{G})$ with $\mathrm{Z}(\mathfrak{g})$. The restriction to $\mathrm{Z}(\mathfrak{g})$ of the central character of ρ is θ_0, and so $\theta_0 : \mathrm{Z}(\mathfrak{g}) \to \mathbb{C}^*$ is faithful. Now let $x \in \mathrm{Stab}_{\mathrm{G}}(\theta_0)$. Then $\theta_0([x,y]) = 1$ for all $y \in \mathfrak{g}$, so that $[x,y] = 0$. Consequently, $\mathrm{Stab}_{\mathrm{G}}(\theta_0) = \mathrm{Z}(\mathfrak{g})$. This completes the proof. □

The class of p-groups covered by Proposition 3.9 includes all the extra special p-groups for $p \geqslant 3$; a p-group G is called extra special when its centre $\mathrm{Z}(\mathrm{G})$ has p elements and $\mathrm{G}/\mathrm{Z}(\mathrm{G})$ is an elementary abelian p-group. It is well known that an extra special p-group has order p^{2n+1} for some positive integer n. Thus the faithful dimension of G is p^n.

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

4. Faithful dimension of pattern groups

This section is devoted to the proof of Theorem 2.10. We start by recalling some notation that was defined in § 2.2. Let $\prec$ be a partial order on the set $[n] := \{1, \dots, n\}$. We can associate to $\prec$ the Lie algebra defined by

$$\mathfrak{g} := \mathfrak{g}_{\prec} = \mathrm{Span}_{\mathbb{Z}}\{\mathbf{e}_{ij} : i \prec j\} \subseteq \mathfrak{gl}(n, \mathbb{Z}).$$

Recall that the length of $([n], \prec)$, denoted by $\lambda_{\prec}$, is defined to be the maximum value of r such that there exists a chain $i_0 \prec \cdots \prec i_r$ in $([n], \prec)$.

Lemma 4.1. *The nilpotency class of $\mathfrak{g}$ is equal to the length of $([n], \prec)$.*

Proof of Lemma 4.1. First note that

$$[\mathbf{e}_{ij}, \mathbf{e}_{kl}] = \delta_{jk}\mathbf{e}_{il} - \delta_{li}\mathbf{e}_{kj} \quad \text{for } i \prec j \text{ and } k \prec l. \tag{11}$$

From (11) it follows that $[\mathbf{e}_{ij}, \mathbf{e}_{kl}] = \mathbf{e}_{il}$ when $i \prec j = k \prec l$ and $[\mathbf{e}_{ij}, \mathbf{e}_{kl}] = -\mathbf{e}_{kj}$ when $k \prec l = i \prec j$. In other cases $[\mathbf{e}_{ij}, \mathbf{e}_{kl}] = 0$. Given a chain $i_0 \prec \cdots \prec i_r$ in $([n], \prec)$, one can see that

$$\mathbf{e}_{i_0, i_r} = [\mathbf{e}_{i_0, i_1}, [\mathbf{e}_{i_1, i_2}, [\cdots, \mathbf{e}_{i_{r-1}, i_r}]] \cdots] \neq 0,$$

and hence the nilpotency class of $\mathfrak{g}$ is at least r. Similarly, one can see that a non-zero commutator of length $r+1$ leads to a chain of length $r+1$, proving the claim. □

Recall that I_{ex} is the set of extreme pairs (see Definition 2.9).

Lemma 4.2. *The centre $\mathrm{Z}(\mathfrak{g})$ of $\mathfrak{g}$ is spanned by $\{\mathbf{e}_{ij} : (i, j) \in I_{\mathrm{ex}}\}$.*

Proof. We first show that $\mathbf{e}_{ij}$ with $(i, j) \in I_{\mathrm{ex}}$ is in the centre of $\mathfrak{g}$. From (11) it follows that

$$[\mathbf{e}_{ij}, \mathbf{e}_{kl}] = 0 \quad \text{for all } k \prec l,$$

since i is minimal and j is maximal. Conversely, suppose $z = \sum_{i \prec j} x_{ij}\mathbf{e}_{ij} \in \mathrm{Z}(\mathfrak{g})$. We show that for each $i_1 \prec j_1$, if $x_{i_1 j_1} \neq 0$ then $(i_1, j_1) \in I_{\mathrm{ex}}$. Assume i_1 is not minimal, and pick a minimal element $k \prec i_1$. Then (11) implies that

$$0 = [z, \mathbf{e}_{ki_1}] = -\sum_{i_1 \prec j} x_{i_1 j}\mathbf{e}_{kj},$$

and thus $x_{i_1 j_1} = 0$, which is a contradiction. A similar argument shows that j_1 is maximal. □

An additive character $\psi : \mathbb{F}_q \to \mathbb{C}^*$ is called *primitive* if the pairing

$$\mathbb{F}_q \times \mathbb{F}_q \to \mathbb{C}^*, \quad (x, y) \mapsto \psi(xy)$$

is non-degenerate. We fix a primitive character ψ by choosing $\iota : \mathbb{F}_p \to \mathbb{C}^*$ to be a faithful character and defining $\psi(x) := \iota(\mathbf{Tr}(x))$, where $\mathbf{Tr} := \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} : \mathbb{F}_q \to \mathbb{F}_p$ is the trace map. Using ψ we can identify the Pontryagin dual of the additive group of $\mathbb{F}_q$ with $\mathbb{F}_q$. It follows that all characters of $\mathfrak{g}_q$ are obtained by vectors $\mathbf{b} = (b_{ij}) \in \bigoplus_{i \prec j} \mathbb{F}_q$, via

$$\psi_{\mathbf{b}}\Big(\sum_{i \prec j} x_{ij}\mathbf{e}_{ij}\Big) := \psi\Big(\sum_{i \prec j} b_{ij}x_{ij}\Big).$$

By Lemma 4.1, the Lie algebra $\mathfrak{g}_q$ has nilpotency class $\lambda_{\prec}$. In the rest of this section we assume that $p > \lambda_{\prec}$. By the orbit method every irreducible representation of $\mathscr{G}_q$ is constructed from the orbit of a character $\psi_{\mathbf{b}} \in \widehat{\mathfrak{g}}_q$ in the coadjoint action. We denote the irreducible representation obtained from $\psi_{\mathbf{b}}$ by $\rho_{\mathbf{b}}$.

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

PROPOSITION 4.3. *Let* $\mathbf{b} = (b_{ij})$ *be an element of* $\bigoplus_{i\prec j}\mathbb{F}_q$ *and let* $\rho_{\mathbf{b}}$ *be the irreducible representation of* $\mathscr{G}_q$ *associated to the orbit of* $\psi_{\mathbf{b}}$. *For all* $(i_1, j_1) \in I_{\mathrm{ex}}$, *if* $b_{i_1j_1} \neq 0$ *then*

$$\dim \rho_{\mathbf{b}} \geqslant q^{\alpha(i_1,j_1)}.$$

Proof. Set $I := \{(i,j) : i \prec j\}$. For $x = \sum_{i\prec j} x_{ij}\mathbf{e}_{ij} \in \mathrm{Stab}_{\mathscr{G}_q}(\psi_{\mathbf{b}})$ and $y = \sum_{i\prec j} y_{ij}\mathbf{e}_{ij} \in \mathfrak{g}_q$, it follows from (11) that

$$\begin{aligned} 1 = \psi_{\mathbf{b}}([x,y]) &= \psi_{\mathbf{b}}\Bigg(\sum_{i\prec j,k\prec l} x_{ij}y_{kl}[\mathbf{e}_{ij},\mathbf{e}_{kl}]\Bigg) = \psi\Bigg(\sum_{i\prec j}\sum_{i\prec k\prec j} b_{ij}(x_{ik}y_{kj} - x_{kj}y_{ik})\Bigg) \\ &= \psi\Bigg(\sum_{i\prec j}\Bigg(\sum_{k\prec i} b_{kj}x_{ki} - \sum_{j\prec l} b_{il}x_{jl}\Bigg)y_{ij}\Bigg). \end{aligned}$$

Since $y_{ij} \in \mathbb{F}_q$ is arbitrary and ψ is a primitive character, we obtain a system of linear equations

$$L_{ij}(x_{st}) := \sum_{k\prec i} b_{kj}x_{ki} - \sum_{j\prec l} b_{il}x_{jl} = 0, \tag{12}$$

which describes the stabilizer of $\psi_{\mathbf{b}}$. The equations in (12) have coefficients in $\mathbb{F}_q$ and are indexed by pairs i, j such that $i \prec j$. We now consider only the linear forms $L_{i_1i}(x_{st})$ and $L_{jj_1}(x_{st})$, for $i_1 \prec i \prec j_1$ and $i_1 \prec j \prec j_1$. From these i and j, we obtain $2\alpha(i_1, j_1)$ linear equations with coefficients in $\mathbb{F}_q$, as follows:

$$\begin{aligned} b_{i_1j_1}x_{ij_1} &= -\sum_{i\prec k\neq j_1} b_{i_1k}x_{ik}, \quad i_1 \prec i \prec j_1, \\ b_{i_1j_1}x_{i_1j} &= -\sum_{i_1\neq l\prec j} b_{lj_1}x_{lj}, \quad i_1 \prec j \prec j_1. \end{aligned} \tag{13}$$

From $b_{i_1j_1} \neq 0$ it follows that x_{ij_1} $(i_1 \prec i \prec j_1)$ and x_{i_1j} $(i_1 \prec j \prec j_1)$ are dependent variables and thus, by noticing that each linear form has $\#I$ variables, the number of solutions of (13) is at most

$$q^{\#I-2\alpha(i_1,j_1)}. \tag{14}$$

Thus the size of the stabilizer (12) is at most (14) and this gives the lower bound by (8). □

LEMMA 4.4. *Let* b *be a non-zero element of* $\mathbb{F}_q$. *Fix* $(i,j) \in I_{\mathrm{ex}}$ *and define* $\mathbf{b} = (b_{kl})_{k\prec l}$, *where* $b_{ij} = b$ *and the other components are zero. Then the dimension of the irreducible representation* $\rho_{\mathbf{b}}$ *is* $q^{\alpha(i,j)}$.

Proof. Set $I := \{(i,j) : i \prec j\}$. The proof of Proposition 4.3, namely (12), shows that the stabilizer of $\rho_{\mathbf{b}}$ is defined by the equations $bx_{ik} = 0$ and $bx_{kj} = 0$, where $i \prec k \prec j$. These show that the stabilizer has cardinality $q^{\#I-2\alpha(i,j)}$, and therefore the dimension of $\rho_{\mathbf{b}}$ is $q^{\alpha(i,j)}$ by (8). □

Using this we now construct a faithful representation of $\mathscr{G}_q$.

LEMMA 4.5. *The group* $\mathscr{G}_q$ *has a faithful representation of dimension*

$$\sum_{(i,j)\in I_{\mathrm{ex}}} fq^{\alpha(i,j)}.$$

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

Proof. First note that $\mathrm{Z}(\mathscr{G}_q) \cong \mathrm{Z}(\mathfrak{g}_q)$ and so

$$\widehat{\Omega}_1(\mathrm{Z}(\mathscr{G}_q)) \cong \widehat{\Omega}_1(\mathrm{Z}(\mathfrak{g}_q)) = \bigoplus_{(i,j)\in I_{\mathrm{ex}}} \widehat{\Omega}_1(\mathbb{F}_q) \cong \bigoplus_{(i,j)\in I_{\mathrm{ex}}} \mathbb{F}_q. \tag{15}$$

Let $\omega_1, \dots, \omega_f$ be a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$. For $(i,j) \in I_{\mathrm{ex}}$ and $1 \leqslant l \leqslant f$, define the vectors $\mathbf{b}_l(i,j) \in \bigoplus_{s\prec t} \mathbb{F}_q$, with the (i,j) coordinate equal to ω_l and the other coordinates equal to 0. Then the set

$$\{\mathbf{b}_l(i,j) : 1 \leqslant l \leqslant f, (i,j) \in I_{\mathrm{ex}}\}$$

is a basis of $\mathrm{Z}(\mathfrak{g}_q)$ as an $\mathbb{F}_p$-vector space. It follows that the set

$$\{\psi_{\mathbf{b}_l(i,j)} : 1 \leqslant l \leqslant f, (i,j) \in I_{\mathrm{ex}}\}$$

is a basis of $\widehat{\Omega}_1(\mathrm{Z}(\mathfrak{g}_q))$ and thus of $\widehat{\Omega}_1(\mathrm{Z}(\mathscr{G}_q))$ by (15). Since $\psi_{\mathbf{b}_l(i,j)}$ is the central character of $\rho_{\mathbf{b}_l(i,j)}$, it follows from Lemma 3.4 that the representation

$$\rho := \bigoplus_{1\leqslant l\leqslant f} \bigoplus_{(i,j)\in I_{\mathrm{ex}}} \rho_{\mathbf{b}_l(i,j)}$$

is faithful. By Lemma 4.4 the dimension of $\rho_{\mathbf{b}_l(i,j)}$ is equal to $q^{\alpha(i,j)}$ and hence

$$\dim \rho = \sum_{(i,j)\in I_{\mathrm{ex}}} f q^{\alpha(i,j)}. \tag{16}$$

This finishes the proof. □

We are now ready to prove Theorem 2.10.

4.1 Proof of Theorem 2.10

Write $m := \#I_{\mathrm{ex}}$ and $n := fm$. As before, we identify $\widehat{\Omega}_1(\mathrm{Z}(\mathfrak{g}_q))$ with $\bigoplus_{(i,j)\in I_{\mathrm{ex}}} \mathbb{F}_q$ which has dimension n as an $\mathbb{F}_p$-vector space. Let ρ be a faithful representation of $\mathscr{G}_q$ with the smallest possible dimension. We will show that the dimension of ρ is bounded from below by the right-hand side of (16). Using Lemma 3.5 we can decompose ρ as a direct sum of n irreducible representations, each of which obtained via the orbit method as described above. Hence, we can write

$$\rho = \bigoplus_{k=1}^{n} \rho_{\mathbf{a}_k},$$

with vectors $\mathbf{a}_k$ given by

$$\mathbf{a}_k = (a_{st}(k))_{s\prec t} \in \bigoplus_{s\prec t} \mathbb{F}_q.$$

Since the central character of $\rho_{\mathbf{a}_k}$ is the restriction of $\psi_{\mathbf{a}_k}$, Lemma 3.5 implies that the set $\{\psi_{\mathbf{a}_k} : 1 \leqslant k \leqslant n\}$ is a basis of $\widehat{\Omega}_1(\mathrm{Z}(\mathscr{G}_q))$ and therefore the set

$$\{(a_{ij}(k))_{(i,j)\in I_{\mathrm{ex}}} : 1 \leqslant k \leqslant n\}$$

is a basis of the $\mathbb{F}_p$-vector space $\bigoplus_{(i,j)\in I_{\mathrm{ex}}} \mathbb{F}_q$. At this point we need a combinatorial lemma whose proof relies on a theorem of Rado and Horn.

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

LEMMA 4.6. *Let V be an m-dimensional $\mathbb{F}_q$-vector space. Suppose that $S = \{v_1, \dots, v_{fm}\}$ is a basis of V viewed as a vector space over the subfield $\mathbb{F}_p$. Then there exists a partition $S_1, \dots, S_f$ of S into f sets of size m such that each S_i is a basis of V as an $\mathbb{F}_q$-vector space.*

We will use the following theorem of Rado and Horn [Hor55]. The proof of this theorem itself is based on Hall's marriage theorem and ideas from matroid theory. We refer the reader to [Bol86, § 18] for more details.

THEOREM 4.7 (Rado–Horn). *Let V be a vector space over a field E and let $\{v_i : 1 \leqslant i \leqslant M\}$ be a set of non-zero vectors in V. Then the following statements are equivalent.*

(i) *The set $\{1, \dots, M\}$ can be partitioned into sets $\{\mathcal{A}_j\}_{j=1}^{k}$ such that $\{v_i : i \in \mathcal{A}_j\}$ is a linearly independent set for all $j = 1, 2, \dots, k$.*

(ii) *For all non-empty subsets $J \subseteq \{1, \dots, M\}$,*

$$\#J \leqslant k \dim_E \operatorname{Span}_E\{v_j : j \in J\}.$$

Proof of Lemma 4.6. We apply Theorem 4.7 with $k = f$ to the set of vectors S. Consider an arbitrary set $J \subseteq \{1, \dots, mf\}$ and let $d = \dim_{\mathbb{F}_q} \operatorname{Span}_{\mathbb{F}_q}\{v_j : j \in J\}$. Then

$$\#\operatorname{Span}_{\mathbb{F}_q}\{v_j : j \in J\} = q^d = p^{fd}.$$

Clearly $\operatorname{Span}_{\mathbb{F}_p}\{v_j : j \in J\} \subseteq \operatorname{Span}_{\mathbb{F}_q}\{v_j : j \in J\}$, and since $\{v_j : j \in J\}$ is linearly independent over $\mathbb{F}_p$ we obtain

$$p^{\#J} = \#\operatorname{Span}_{\mathbb{F}_p}\{v_j : j \in J\} \leqslant \#\operatorname{Span}_{\mathbb{F}_q}\{v_j : j \in J\} = p^{fd}.$$

It follows from the above inequality that

$$\#J \leqslant f \dim_{\mathbb{F}_q} \operatorname{Span}_{\mathbb{F}_q}\{v_j : j \in J\}.$$

Thus by the Rado–Horn theorem, the set $\{1, \dots, fm\}$ can be partitioned into $\mathcal{A}_1, \dots, \mathcal{A}_f$ such that each of the sets $\{v_\ell : \ell \in \mathcal{A}_i\}$ is linearly independent over $\mathbb{F}_q$. Note that $\#\mathcal{A}_i \leqslant m$ since $\dim_{\mathbb{F}_q} V = m$. But the $\mathcal{A}_i$ partition $\{1, \dots, mf\}$ and so $\mathcal{A}_i$ has the size m which implies that $\{v_\ell : \ell \in \mathcal{A}_i\}$ is a basis of V over $\mathbb{F}_q$. □

We return to the proof of Theorem 2.10. Set $V = \bigoplus_{(i,j)\in I_{\mathrm{ex}}} \mathbb{F}_q$, which is an $\mathbb{F}_p$-vector space of dimension $n = mf$. Also set $v_k = (a_{ij}(k))_{(i,j)\in I_{\mathrm{ex}}} \in V$. Recall that $S = \{v_k : 1 \leqslant k \leqslant n\}$ is a basis of V as an $\mathbb{F}_p$-vector space and so by Lemma 4.6 there exist f disjoint sets $S_1, \dots, S_f$, each of size m, such that each S_ℓ is a basis of V as an $\mathbb{F}_q$-vector space. For $1 \leqslant \ell \leqslant f$, let A_ℓ denote an $m \times m$ matrix whose rows are elements of S_ℓ. Note that A_ℓ is invertible, since S_ℓ is a basis of V as an $\mathbb{F}_q$-vector space. Using the Leibniz expansion of the determinant of A, we can assume that up to a permutation of the rows, all of the diagonal entries of A_ℓ are non-zero. Thus Proposition 4.3 implies that

$$\sum_{(i,j)\in I_{\mathrm{ex}}} q^{\alpha(i,j)} \leqslant \sum_{\mathbf{a}_k \in S_\ell} \dim \rho_{\mathbf{a}_k} \quad \text{for } 1 \leqslant \ell \leqslant f.$$

Summing over all ℓ, we obtain

$$f \sum_{(i,j)\in I_{\mathrm{ex}}} q^{\alpha(i,j)} \leqslant \dim \rho,$$

which finishes the proof.

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

5. The commutator matrix of nilpotent Lie algebras

We now consider general nilpotent Lie algebras by rebuilding the argument presented in § 4. Let $\mathfrak{g}$ be a nilpotent $\mathbb{Z}$-Lie algebra of nilpotency class c which is finitely generated as an abelian group, and let $\mathbb{F}_q$ be a finite field with $q = p^f$ elements. We set $\mathfrak{g}_q := \mathfrak{g} \otimes_{\mathbb{Z}} \mathbb{F}_q$ throughout this section. In order to apply the orbit method, we will also assume that $p > c$. Existence of torsion elements in $\mathfrak{g}$ and some of its quotients results in some technical difficulties which are addressed in what follows.

We call a subset S of a finitely generated abelian group Γ a *semibasis* if it represents a basis over $\mathbb{Z}$ of the free abelian group $\Gamma/\Gamma_{\mathrm{tor}}$, where Γ_{tor} denotes the subgroup of torsion elements of Γ. Clearly $\#S = \mathrm{rk}_{\mathbb{Z}}\Gamma$. We define $\mathsf{e}(\Gamma)$ to be the largest prime divisor of the exponent of Γ_{tor}.

Remark 5.1. Let $v_1, \dots, v_d$ be $\mathbb{Z}$-linearly independent vectors in a finitely generated abelian group Γ such that $\mathrm{rk}_{\mathbb{Z}}(\Gamma) = d$, and let M be the subgroup of Γ generated by the v_i. Set $q := p^f$, where f is a positive integer and p is a prime such that $p > \mathsf{e}(\Gamma/M)$. Then the elements $v_1 \otimes_{\mathbb{Z}} 1$, $\dots, v_d \otimes_{\mathbb{Z}} 1$ form a basis of the $\mathbb{F}_q$-vector space $\Gamma_q := \Gamma \otimes_{\mathbb{Z}} \mathbb{F}_q$.

Remark 5.2. For every prime p we have $[\mathfrak{g},\mathfrak{g}]_q = [\mathfrak{g}_q, \mathfrak{g}_q]$. The equality $\mathrm{Z}(\mathfrak{g}_q) = \mathrm{Z}(\mathfrak{g})_q$ also holds for p sufficiently large. An explicit lower bound for p can be obtained as follows. Let $\mathbf{v}_1, \dots, \mathbf{v}_n$ be a semibasis of $\mathfrak{g}/\mathrm{Z}(\mathfrak{g})$, and let $\mathbf{w}_1, \dots, \mathbf{w}_m$ be a semibasis of $[\mathfrak{g},\mathfrak{g}]$. Then for $1 \leqslant i < j \leqslant n$ we can write $[\mathbf{v}_i, \mathbf{v}_j] = \sum_{k=1}^{m} \lambda_{ij}^k \mathbf{w}_k + \mathbf{y}_{ij}$, where $\lambda_{ij}^k \in \mathbb{Z}$ and $\mathbf{y}_{ij} \in [\mathfrak{g},\mathfrak{g}]_{\mathrm{tor}}$. Setting $x_{j+n(k-1),i} := \lambda_{ij}^k$, we obtain an $mn \times n$ matrix $X := [x_{a,b}]$. Now for every $n \times n$ submatrix X' of X we define $\mathsf{m}(X') := \max\{p : p \mid \det(X')\}$, where $\mathsf{m}(X') := 1$ whenever $\det(X') = \pm 1$. Further, set $\mathsf{m}(X) := \min_{X'}\{\mathsf{m}(X')\}$, where the minimum is taken over $n \times n$ submatrices of X. For the equality $\mathrm{Z}(\mathfrak{g}_q) = \mathrm{Z}(\mathfrak{g})_q$ it is enough to assume that $p > C_1$, where

$$C_1 := \max\{\mathsf{m}(X), \mathsf{e}([\mathfrak{g},\mathfrak{g}]), \mathsf{e}(\mathfrak{g}/[\mathfrak{g},\mathfrak{g}])\}.$$

Now let $\mathbf{w}_1, \dots, \mathbf{w}_{l_1}$ be a semibasis of $\mathrm{Z}(\mathfrak{g}) \cap [\mathfrak{g},\mathfrak{g}]$. Let $\mathbf{w}_{l_1+1}, \dots, \mathbf{w}_m$ be elements of $\mathfrak{g}$ which represent a semibasis of $[\mathfrak{g},\mathfrak{g}]/(\mathrm{Z}(\mathfrak{g}) \cap [\mathfrak{g},\mathfrak{g}])$. Finally, let $\mathbf{z}_1, \dots, \mathbf{z}_{l_2}$ be elements of $\mathfrak{g}$ which represent a semibasis of $\mathrm{Z}(\mathfrak{g})/(\mathrm{Z}(\mathfrak{g}) \cap [\mathfrak{g},\mathfrak{g}])$. It is straightforward to verify that the vectors $\{\mathbf{w}_1, \dots, \mathbf{w}_m, \mathbf{z}_1, \dots, \mathbf{z}_{l_2}\}$ are $\mathbb{Z}$-linearly independent. Clearly the choice of these vectors implies that $\mathrm{rk}_{\mathbb{Z}}(\mathrm{Z}(\mathfrak{g}) + [\mathfrak{g},\mathfrak{g}]) = l_2 + m$. Let M be the $\mathbb{Z}$-submodule of $\mathfrak{g}$ generated by the $\mathbf{w}_i$, $1 \leqslant i \leqslant m$, and the $\mathbf{z}_j$, $1 \leqslant j \leqslant l_2$, and set

$$C_2 := \mathsf{e}(\mathfrak{g}/M).$$

From Remark 5.1 it follows that if $p > \max\{C_1, C_2\}$, where C_1 is defined in Remark 5.2, then after tensoring with $\mathbb{F}_q$, these vectors form a basis of the $\mathbb{F}_q$-vector space $[\mathfrak{g}_q, \mathfrak{g}_q] + \mathrm{Z}(\mathfrak{g}_q)$.

Now let $\mathbf{v}'_1, \dots, \mathbf{v}'_n$ be elements of $\mathfrak{g}$ which represent a semibasis of $\mathfrak{g}/\mathrm{Z}(\mathfrak{g})$. For $1 \leqslant i < j \leqslant n$, there exist integers η_{ij}^k, $1 \leqslant k \leqslant m$, such that the elements

$$\mathbf{v}'_{i,j} := \left([\mathbf{v}'_i, \mathbf{v}'_j] - \sum_{k=l_1+1}^{m} \eta_{ij}^k \mathbf{w}_k \right) \in [\mathfrak{g},\mathfrak{g}]$$

are torsion modulo $[\mathfrak{g},\mathfrak{g}] \cap \mathrm{Z}(\mathfrak{g})$. Set K equal to the exponent of $([\mathfrak{g},\mathfrak{g}]/[\mathfrak{g},\mathfrak{g}] \cap \mathrm{Z}(\mathfrak{g}))_{\mathrm{tor}}$. It follows that $K\mathbf{v}'_{i,j} \in [\mathfrak{g},\mathfrak{g}] \cap \mathrm{Z}(\mathfrak{g})$ for every $1 \leqslant i < j \leqslant n$. Now set $\mathbf{v}_i := K\mathbf{v}'_i$ for $1 \leqslant i \leqslant n$. Then there exist integers λ_{ij}^k such that

$$[\mathbf{v}_i, \mathbf{v}_j] = \sum_{k=1}^{m} \lambda_{ij}^k \mathbf{w}_k + \mathbf{x}_{ij} \quad \text{for every } 1 \leqslant i < j \leqslant n, \tag{17}$$

where $\mathbf{x}_{ij} \in ([\mathfrak{g},\mathfrak{g}] \cap \mathrm{Z}(\mathfrak{g}))_{\mathrm{tor}}$. We remark that $\lambda_{ij}^k = K^2 \eta_{ij}^k$ for $l_1 + 1 \leqslant k \leqslant m$.

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

For each $1 \leqslant i, j \leqslant n$, we define the linear forms

$$\Lambda_{ij}(T_1, \ldots, T_m) := \sum_{k=1}^{m} \lambda_{ij}^k T_k \in \mathbb{Z}[T_1, \ldots, T_m].$$

It is clear that $\Lambda_{ii} = 0$ and $\Lambda_{ij} = -\Lambda_{ji}$ for $1 \leqslant i, j \leqslant n$. The *commutator matrix of* $\mathfrak{g}$ (relative to the chosen ordered basis) is the skew-symmetric matrix of linear forms defined by

$$F_{\mathfrak{g}}(T_1, \ldots, T_m) := [\Lambda_{ij}(T_1, \ldots, T_m)]_{1 \leqslant i,j \leqslant n} \in \mathrm{M}_n(\mathbb{Z}[T_1, \ldots, T_m]). \tag{18}$$

This matrix has previously been used in several papers, such as those by Grunewald and Segal [GS84], Voll [Vol05, Vol04], O'Brien and Voll [O'BV15], Avni, Klopsch, Onn and Voll [AKOV13], and Stasinski and Voll [SV14].

The following theorem expresses the faithful dimension of $\mathscr{G}_q$ as the solution to a rank minimization problem. For the next theorem, we set

$$C_3 := \mathsf{e}((\mathfrak{g}/\mathrm{Z}(\mathfrak{g}))_{\mathrm{tor}}).$$

THEOREM 5.3. *Let $\mathfrak{g}$ be a nilpotent $\mathbb{Z}$-Lie algebra of nilpotency class c which is finitely generated as an abelian group. If $p > \max\{c, C_1, C_2, C_3\}$, then*

$$m_{\mathrm{faithful}}(\mathscr{G}_q) = \min\left\{ \sum_{\ell=1}^{l_1} f q^{\mathrm{rk}_{\mathbb{F}_q}(F_{\mathfrak{g}}(x_{\ell 1}, \ldots, x_{\ell m}))/2} : \begin{pmatrix} x_{11} & \cdots & x_{1l_1} \\ \vdots & \ddots & \vdots \\ x_{l_1 1} & \cdots & x_{l_1 l_1} \end{pmatrix} \in \mathrm{GL}_{l_1}(\mathbb{F}_q) \right\} + f l_2,$$

where $m := \mathrm{rk}_{\mathbb{Z}}([\mathfrak{g}, \mathfrak{g}])$, $l_1 := \mathrm{rk}_{\mathbb{Z}}([\mathfrak{g}, \mathfrak{g}] \cap \mathrm{Z}(\mathfrak{g}))$ and $l_2 := \mathrm{rk}_{\mathbb{Z}}(\mathrm{Z}(\mathfrak{g})/\mathrm{Z}(\mathfrak{g}) \cap [\mathfrak{g}, \mathfrak{g}])$.

Remark 5.4. We note that when $n = 0$, the commutator matrix is the zero matrix and thus from Theorem 5.3 we obtain $m_{\mathrm{faithful}}(\mathscr{G}_q) = (l_1 + l_2)f$. This formula can also be obtained from Lemma 3.1 since in this case for p as in Theorem 5.3 the group $\mathscr{G}_q$ is abelian.

5.1 Proof of Theorem 5.3

In this section we assume that p is chosen as in Theorem 5.3. By abuse of notation, we denote the images in $\mathfrak{g}_q$ of the $\mathbf{v}_i$, the $\mathbf{w}_i$ and the $\mathbf{z}_i$ that are chosen above by the same letters. Let $\psi : \mathbb{F}_q \to \mathbb{C}^*$ be the primitive additive character defined in § 4. Choose a basis

$$\{\mathbf{u}_1 + (\mathrm{Z}(\mathfrak{g}_q) + \mathfrak{g}_q'), \ldots, \mathbf{u}_{l_3} + (\mathrm{Z}(\mathfrak{g}_q) + \mathfrak{g}_q')\}$$

of $\mathfrak{g}_q/(\mathrm{Z}(\mathfrak{g}_q) + \mathfrak{g}_q')$. Since $p > C_2$, the set

$$\{\mathbf{w}_1, \ldots, \mathbf{w}_{l_1}, \mathbf{w}_{l_1+1}, \ldots, \mathbf{w}_m, \mathbf{z}_1, \ldots, \mathbf{z}_{l_2}, \mathbf{u}_1, \ldots, \mathbf{u}_{l_3}\}$$

is a basis of $\mathfrak{g}_q$. For

$$\mathbf{a} = (a_1, \ldots, a_{l_1}, a_{l_1+1}, \ldots, a_m, b_1, \ldots, b_{l_2}, c_1, \ldots, c_{l_3}) \in \mathbb{F}_q^{m+l_2+l_3}, \tag{19}$$

let $\psi_{\mathbf{a}} \in \widehat{\mathfrak{g}}_q$ be defined by

$$\begin{aligned} &\psi_{\mathbf{a}}\Big(\sum_{i=1}^{l_1} w_i \mathbf{w}_i + \sum_{i=l_1+1}^{m} w_i \mathbf{w}_i + \sum_{i=1}^{l_2} z_i \mathbf{z}_i + \sum_{i=1}^{l_3} u_i \mathbf{u}_i\Big) \\ &\quad := \psi\Big(\sum_{i=1}^{l_1} a_i w_i + \sum_{i=l_1+1}^{m} a_i w_i + \sum_{i=1}^{l_2} b_i z_i + \sum_{i=1}^{l_3} c_i u_i\Big). \end{aligned}$$

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

The assignment $\mathbf{a} \mapsto \psi_{\mathbf{a}}$ identifies $\widehat{\mathfrak{g}}_q$ with $\mathbb{F}_q^{m+l_2+l_3}$. For $\mathbf{a}$ as in (19), we write $\mathbf{a} = (\mathbf{a}', \mathbf{a}'', \mathbf{b}, \mathbf{c})$, where $\mathbf{a}' \in \mathbb{F}_q^{l_1}$, $\mathbf{a}'' \in \mathbb{F}_q^{m-\ell_1}$, $\mathbf{b} \in \mathbb{F}_q^{l_2}$ and $\mathbf{c} \in \mathbb{F}_q^{l_3}$, and define the projection maps

$$\mathsf{proj}_1 : \mathbb{F}_q^{m+l_2+l_3} \longrightarrow \mathbb{F}_q^{m+l_2}, \quad \mathsf{proj}_2 : \mathbb{F}_q^{m+l_2+l_3} \longrightarrow \mathbb{F}_q^{l_1+l_2}, \quad \mathsf{proj}_3 : \mathbb{F}_q^{m+l_2+l_3} \longrightarrow \mathbb{F}_q^{m},$$

by $\mathsf{proj}_1(\mathbf{a}) = (\mathbf{a}', \mathbf{a}'', \mathbf{b})$, $\mathsf{proj}_2(\mathbf{a}) = (\mathbf{a}', \mathbf{b})$, and $\mathsf{proj}_3(\mathbf{a}) = (\mathbf{a}', \mathbf{a}'')$.

In the rest of this section, we identify $\mathrm{Z}(\mathscr{G}_q)$ with $\mathrm{Z}(\mathfrak{g}_q)$. Let ρ be an irreducible representation of $\mathscr{G}_q$. By the orbit method, ρ is obtained from a character $\theta \in \widehat{\mathfrak{g}}_q$, whose restriction to $\mathrm{Z}(\mathfrak{g}_q)$ coincides with the central character of ρ. Assume that $\theta = \psi_{\mathbf{a}}$ for some $\mathbf{a} \in \mathbb{F}_q^{m+l_2+l_3}$, whose entries are indexed as in (19). Our next goal is to prove that

$$\dim \rho = q^{\mathrm{rk}_{\mathbb{F}_q}(F_{\mathfrak{g}}(a_1,\dots,a_m))/2} = q^{\mathrm{rk}_{\mathbb{F}_q}(F_{\mathfrak{g}}(\mathsf{proj}_3(\mathbf{a})))/2}. \tag{20}$$

The proof is similar to the argument of [O'BV15, Lemma 3.3], but for the reader's convenience we provide some details. Proposition 3.8 implies that $\mathrm{Z}(\mathfrak{g}_q) \subseteq \mathrm{Stab}_{\mathscr{G}_q}(\theta)$. Since $p > C_3$, it follows that K is invertible in $\mathbb{F}_q$, so that after tensoring by $\mathbb{F}_q$ the $\mathbf{v}_i$ form a basis of $\mathfrak{g}_q/\mathrm{Z}(\mathfrak{g}_q)$. For $x = \sum_{i=1}^n x_i \mathbf{v}_i \in \mathrm{Stab}_{\mathscr{G}_q}(\theta)$ and $y = \sum_{i=1}^n y_i \mathbf{v}_i \in \mathfrak{g}_q/\mathrm{Z}(\mathfrak{g}_q)$ we have $\theta([x,y]) = 1$. From (17) and the fact that $p > C_1$ it follows that

$$\psi\Bigg(\sum_{i=1}^n \Bigg(\sum_{1\leqslant r<i} \sum_{k=1}^m a_k \lambda_{ri}^k x_r - \sum_{i<s\leqslant n} \sum_{k=1}^m a_k \lambda_{is}^k x_s \Bigg) y_i \Bigg) = \psi_{\mathbf{a}}\Bigg(\sum_{1\leqslant i<j\leqslant n} \sum_{k=1}^m \lambda_{ij}^k (x_i y_j - x_j y_i) \mathbf{w}_k \Bigg) = 1.$$

Since ψ is a primitive character, it follows that $\mathrm{Stab}_{\mathscr{G}_q}(\theta)/\mathrm{Z}(\mathfrak{g}_q)$ is defined by the linear equations

$$\sum_{i<s\leqslant n} \sum_{k=1}^m a_k \lambda_{is}^k x_s - \sum_{1\leqslant r<i} \sum_{k=1}^m a_k \lambda_{ri}^k x_r = 0, \quad 1 \leqslant i \leqslant n.$$

Consequently, $x = \sum_{i=1}^n x_i \mathbf{v}_i \in \mathrm{Stab}_{\mathscr{G}_q}(\theta)/\mathrm{Z}(\mathfrak{g}_q)$ if and only if $(x_1, \dots, x_n) \in \ker F_{\mathfrak{g}}(a_1, \dots, a_m)$. The last statement implies that $\#\mathrm{Stab}_{\mathscr{G}_q}(\theta) = q^{\dim_{\mathbb{F}_q}(\mathfrak{g}_q) - \mathrm{rk}_{\mathbb{F}_q}(F_{\mathfrak{g}}(a_1,\dots,a_m))}$. Equality (20) now follows from (8).

Definition 5.5 (Admissible sets of vectors). A set of vectors

$$\{\mathbf{a}_\ell \in \mathbb{F}_q^{m+l_2+l_3} : 1 \leqslant \ell \leqslant (l_1+l_2)f\}$$

is called an *admissible set of vectors* if $\{\mathsf{proj}_2(\mathbf{a}_\ell) : 1 \leqslant \ell \leqslant (l_1+l_2)f\}$ is a basis of the $\mathbb{F}_p$-vector space $\mathbb{F}_q^{l_1+l_2}$.

Now let $\tilde{\rho}$ be a faithful representation of $\mathscr{G}_q$ with the smallest possible dimension. Note that the dimension of $\Omega_1(\mathrm{Z}(\mathfrak{g}_q)) = \mathrm{Z}(\mathfrak{g}_q)$ over $\mathbb{F}_p$ is $(l_1+l_2)f$ and $\mathrm{Z}(\mathscr{G}_q) \cong \mathrm{Z}(\mathfrak{g}_q)$. Therefore

$$\widehat{\Omega}_1(\mathrm{Z}(\mathscr{G}_q)) \cong \widehat{\Omega}_1(\mathrm{Z}(\mathfrak{g}_q)) \cong \bigoplus_{\ell=1}^{l_1+l_2} \mathbb{F}_q.$$

Thus by Lemma 3.5 the representation $\tilde{\rho}$ decomposes into $(l_1+l_2)f$ irreducible representations

$$\tilde{\rho} = \bigoplus_{\ell=1}^{(l_1+l_2)f} \rho_{\mathbf{a}_\ell}, \quad \mathbf{a}_\ell \in \mathbb{F}_q^{m+l_2+l_3},$$

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

where the representation $\rho_{\mathbf{a}_\ell}$ is obtained by $\psi_{\mathbf{a}_\ell} \in \widehat{\mathfrak{g}}_q$. Since the restriction of $\psi_{\mathbf{a}_\ell}$ is the central character of $\rho_{\mathbf{a}_\ell}$, it follows from Lemma 3.5 that the set

$$\{\psi_{\mathbf{a}_\ell}|_{\widehat{\Omega}_1(\mathrm{Z}(\mathfrak{g}_q))} : 1 \leqslant \ell \leqslant (l_1+l_2)f\}$$

is a basis of $\widehat{\Omega}_1(\mathrm{Z}(\mathfrak{g}_q))$ and therefore the set

$$\{\mathsf{proj}_2(\mathbf{a}_\ell) : 1 \leqslant \ell \leqslant (l_1+l_2)f\}$$

is a basis of the $\mathbb{F}_p$-vector space $\mathbb{F}_q^{l_1+l_2}$. To summarize, we have proven that for each faithful representation $\tilde{\rho}$ with the smallest possible dimension we can find an admissible set of vectors

$$\{\mathbf{a}_\ell \in \mathbb{F}_q^{m+l_2+l_3} : 1 \leqslant \ell \leqslant (l_1+l_2)f\}$$

such that

$$\dim(\tilde{\rho}) = \sum_{\ell=1}^{(l_1+l_2)f} q^{\mathrm{rk}_{\mathbb{F}_q}(F_{\mathfrak{g}}(\mathsf{proj}_3(\mathbf{a})))/2}. \tag{21}$$

Conversely, let $\{\mathbf{a}_\ell \in \mathbb{F}_q^{m+l_2+l_3} : 1 \leqslant \ell \leqslant (l_1+l_2)f\}$ be an admissible set of vectors. Then by Lemma 3.4, we can construct a faithful representation $\tilde{\rho}$, not necessarily of minimal dimension, such that its dimension is equal to (21). In the definition of admissible vectors we considered $\mathbb{F}_q^{l_1+l_2}$ as an $\mathbb{F}_p$-vector space. We now consider $\mathbb{F}_q^{l_1+l_2}$ as an $\mathbb{F}_q$-vector space and define the following notion.

DEFINITION 5.6 (Regular sets of vectors). A set of vectors

$$\{\mathbf{a}_\ell \in \mathbb{F}_q^{m+l_2+l_3} : 1 \leqslant \ell \leqslant l_1+l_2\},$$

is called a *regular set of vectors* if the set $\{\mathsf{proj}_2(\mathbf{a}_\ell) : 1 \leqslant \ell \leqslant (l_1+l_2)\}$ is a basis of the $\mathbb{F}_q$-vector space $\mathbb{F}_q^{l_1+l_2}$.

We now claim that

$$m_{\mathrm{faithful}}(\mathscr{G}_q) = \min\left\{ \sum_{\ell=1}^{l_1+l_2} f q^{\mathrm{rk}_{\mathbb{F}_q}(F_{\mathfrak{g}}(\mathsf{proj}_3(\mathbf{a}_\ell)))/2} : \{\mathbf{a}_\ell \in \mathbb{F}_q^{m+l_2+l_3}\}_{\ell=1}^{l_1+l_2} \text{ is a regular set} \right\}. \tag{22}$$

Let $\{\omega_1, \ldots, \omega_f\}$ be a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$ and let

$$\{\mathbf{a}_\ell \in \mathbb{F}_q^{m+l_2+l_3} : 1 \leqslant \ell \leqslant l_1+l_2\}$$

be a regular set of vectors that minimizes (22). Clearly $\{\omega_i \mathbf{a}_\ell : 1 \leqslant i \leqslant f, 1 \leqslant \ell \leqslant l_1+l_2\}$ is an admissible set of vectors and

$$\sum_{\ell=1}^{l_1+l_2} f q^{\mathrm{rk}_{\mathbb{F}_q}(F_{\mathfrak{g}}(\mathsf{proj}_3(\mathbf{a}_\ell)))/2} = \sum_{i=1}^{f}\sum_{\ell=1}^{l_1+l_2} q^{\mathrm{rk}_{\mathbb{F}_q}(F_{\mathfrak{g}}(\mathsf{proj}_3(\omega_i\mathbf{a}_\ell)))/2} \geqslant m_{\mathrm{faithful}}(\mathscr{G}_q).$$

Conversely, let $\tilde{\rho}$ be a faithful representation with the smallest possible dimension. From the above discussion we obtain an admissible set of vectors

$$\{\mathbf{a}_\ell \in \mathbb{F}_q^{m+l_2+l_3} : 1 \leqslant \ell \leqslant (l_1+l_2)f\}.$$

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

From Lemma 4.6 this set can be partitioned into f sets $\mathcal{B}_i$ in which each $\mathcal{B}_i$ is a regular set of vectors. Without loss of generality assume that

$$\sum_{\mathbf{a}_\ell \in \mathcal{B}_1} q^{\mathrm{rk}_{\mathbb{F}_q}(F_{\mathfrak{g}}(\mathsf{proj}_3(\mathbf{a}_\ell)))/2} \leqslant \sum_{\mathbf{a}_\ell \in \mathcal{B}_i} q^{\mathrm{rk}_{\mathbb{F}_q}(F_{\mathfrak{g}}(\mathsf{proj}_3(\mathbf{a}_\ell)))/2} \quad 2 \leqslant i \leqslant f.$$

Thus

$$\sum_{\mathbf{a}_\ell \in \mathcal{B}_1} f q^{\mathrm{rk}_{\mathbb{F}_q}(F_{\mathfrak{g}}(\mathsf{proj}_3(\mathbf{a}_\ell)))/2} \leqslant \dim(\tilde{\rho}),$$

which proves the claim.

We are now ready to finish the proof of Theorem 5.3. Let $\{\mathbf{a}_\ell \in \mathbb{F}_q^{m+l_2+l_3} : 1 \leqslant \ell \leqslant l_1+l_2\}$ be a regular set of vectors. Let $A \in \mathrm{GL}_{l_1+l_2}(\mathbb{F}_q)$ be the matrix whose rows are

$$\mathsf{proj}_2(\mathbf{a}_1), \dots, \mathsf{proj}_2(\mathbf{a}_{l_1+l_2}).$$

Therefore

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1l_1} & b_{11} & \cdots & b_{1l_2} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{l_1 1} & \cdots & a_{l_1 l_1} & b_{l_1 1} & \cdots & b_{l_1 l_2} \\ a_{(l_1+1)1} & \cdots & a_{(l_1+1)l_1} & b_{(l_1+1)1} & \cdots & b_{(l_1+1)l_2} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{(l_1+l_2)1} & \cdots & a_{(l_1+l_2)l_1} & b_{(l_1+l_2)1} & \cdots & b_{(l_1+l_2)l_2} \end{pmatrix},$$

where $\mathsf{proj}_2(\mathbf{a}_i) = (a_{i1}, \dots, a_{il_1}, b_{i1}, \dots, b_{il_2})$. The first l_1 columns of A are linearly independent over $\mathbb{F}_q$, and therefore we can find an invertible $l_1 \times l_1$ submatrix of the first l_1 columns. By possibly permuting the rows of A we can assume that this submatrix lies at the intersection of the first l_1 rows and l_1 columns of A. It is clear that

$$\sum_{\ell=1}^{l_1+l_2} q^{\mathrm{rk}_{\mathbb{F}_q}(F_{\mathfrak{g}}(a_{\ell 1}, \dots, a_{\ell m}))/2} \geqslant \sum_{\ell=1}^{l_1} q^{\mathrm{rk}_{\mathbb{F}_q}(F_{\mathfrak{g}}(a_{\ell 1}, \dots, a_{\ell m}))/2} + l_2.$$

From this and (22) we conclude that

$$m_{\mathrm{faithful}}(\mathscr{G}_q) \geqslant \min \left\{ \sum_{\ell=1}^{l_1} f q^{\mathrm{rk}_{\mathbb{F}_q}(F_{\mathfrak{g}}(a_{\ell 1}, \dots, a_{\ell m}))/2} : \begin{pmatrix} a_{11} & \cdots & a_{1l_1} \\ \vdots & \ddots & \vdots \\ a_{l_1 1} & \cdots & a_{l_1 l_1} \end{pmatrix} \in \mathrm{GL}_{l_1}(\mathbb{F}_q) \right\} + f l_2. \quad (23)$$

Conversely, let

$$\{a_{\ell(l_1+1)}, \dots, a_{\ell m}\}_{1 \leqslant \ell \leqslant l_1}$$

be an arbitrary set of elements of $\mathbb{F}_q$ and let

$$B := \begin{pmatrix} a_{11} & \cdots & a_{1l_1} \\ \vdots & \ddots & \vdots \\ a_{l_1 1} & \cdots & a_{l_1 l_1} \end{pmatrix} \in \mathrm{GL}_{l_1}(\mathbb{F}_q)$$

be an arbitrary invertible matrix. Then the rows of the matrix

$$\begin{pmatrix} B & 0 \\ 0 & I_{l_1 \times l_1} \end{pmatrix} \in \mathrm{GL}_{l_1+l_2}(\mathbb{F}_q)$$

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

are projections (under proj_2) of a regular set of vectors in $\mathbb{F}_q^{m+l_2+l_3}$. Similar to the proof of (22), using this regular set of vectors we can construct a faithful representation of $\mathscr{G}_q$ of dimension

$$\sum_{\ell=1}^{l_1} f q^{\mathrm{rk}_{\mathbb{F}_q}(F_{\mathfrak{g}}(a_{\ell 1},\ldots,a_{\ell m}))/2} + f l_2.$$

From this we conclude that

$$m_{\text{faithful}}(\mathscr{G}_q) \leqslant \min\left\{ \sum_{\ell=1}^{l_1} f q^{\mathrm{rk}_{\mathbb{F}_q}(F_{\mathfrak{g}}(a_{\ell 1},\ldots,a_{\ell m}))/2} : \begin{pmatrix} a_{11} & \cdots & a_{1l_1} \\ \vdots & \ddots & \vdots \\ a_{l_1 1} & \cdots & a_{l_1 l_1} \end{pmatrix} \in \mathrm{GL}_{l_1}(\mathbb{F}_q) \right\} + f l_2. \quad (24)$$

Therefore, by combining (23) and (24) we obtain Theorem 5.3.

We now address Examples 2.1, 2.2, 2.3, and 2.6 in detail. By a straightforward calculation, one can verify that in all of these examples $C_1 = C_2 = C_3 = 1$, and hence Theorem 5.3 is applicable for $p > 2$.

5.2 Details for Example 2.1

From the defining bracket relations we deduce that $\mathfrak{g}_a' = \mathrm{Z}(\mathfrak{g}_a) = \mathrm{Span}_{\mathbb{Z}}\{v_7, v_8, v_9\}$ and so $\mathfrak{g}_a$ is a 2-step nilpotent Lie algebra. From the relations we also obtain the following commutator matrix:

$$F_{\mathfrak{g}}(T_1,T_2,T_3) = \begin{pmatrix} 0 & M \\ -M^{\mathrm{tr}} & 0 \end{pmatrix}, \quad M := M(T_1,T_2,T_3) = \begin{pmatrix} T_1 & T_2 & aT_3 \\ T_3 & T_1 & T_2 \\ T_3 & 0 & T_1 \end{pmatrix}.$$

Observe that the determinant of M is

$$g(T_1,T_2,T_3) := T_3T_2^2 + T_1^3 - T_1T_2T_3 - aT_1T_3^2.$$

By Theorem 5.3 the faithful dimension of $\mathscr{G}_{a,p} = \exp(\mathfrak{g}_a \otimes_{\mathbb{Z}} \mathbb{F}_p)$, for $p \geqslant 3$, is the minimum value of

$$p^{\mathrm{rk}_{\mathbb{F}_p}(M(x_{11},x_{12},x_{13}))} + p^{\mathrm{rk}_{\mathbb{F}_p}(M(x_{21},x_{22},x_{23}))} + p^{\mathrm{rk}_{\mathbb{F}_p}(M(x_{31},x_{32},x_{33}))} \quad (25)$$

subject to the condition

$$\begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{pmatrix} \in \mathrm{GL}_3(\mathbb{F}_p). \quad (26)$$

Let p be a prime not dividing a. Computing all 2×2 minors of M shows that

$$2 \leqslant \mathrm{rk}_{\mathbb{F}_p}(M(x,y,z)) \leqslant 3$$

unless $x = y = z = 0$. Let us consider the question of existence of a vector $(x,y,z) \in \mathbb{F}_p^3$ such that $x \neq 0$ and

$$g(x,y,z) = y^2z + x^3 - xyz - axz^2 = 0. \quad (27)$$

Obviously we should take $z \neq 0$ Picking $x = 1$, we obtain the equation $zy^2 - zy + (1 - az^2) = 0$, whose discriminant with respect to y is equal to $4az^3 + z^2 - 4z$. Thus to solve (27) it suffices to show that for any non-zero $a \in \mathbb{Z}$ the curve $Y^2 = 4aX^3 + X^2 - 4X$ has a rational point in $\mathbb{F}_p$ with $X \neq 0$. This can be done by noticing that $Y^2 - 4aX^3 - X^2 + 4X$ is absolutely irreducible [Sch76, Corollary, p. 13] and thus by Hasse's bound on the number of $\mathbb{F}_p$-points of elliptic curves [Sch76, Theorem 2A, p. 10] one can verify that such a point exists for $p > 1800$. Let $(1,y,z)$ be a solution of (27). Then the vectors $(0,1,0)$ and $(0,0,1)$ and $(1,y,z)$ satisfy (26), and minimize (25). Thus the faithful dimension of $\mathscr{G}_{a,p}$ is equal to $3p^2$.

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

5.3 Details for Examples 2.2 and 2.6

We discuss these examples together by proving the following formula:

$$m_{\text{faithful}}(\mathscr{G}_q) = \begin{cases} 2fq & \text{if } p \equiv 1 \pmod 4, \\ 2fq & \text{if } p \equiv 3 \pmod 4 \text{ and } f \text{ is even}, \\ 2fq^2 & \text{if } p \equiv 3 \pmod 4 \text{ and } f \text{ is odd}. \end{cases}$$

The commutator relations imply that $\mathfrak{g}' = \mathrm{Z}(\mathfrak{g}) = \mathrm{Span}_{\mathbb{Z}}\{v_5, v_6\}$, and that $\mathfrak{g}$ is a 2-step nilpotent Lie algebra. The commutator matrix of $\mathfrak{g}$ can be easily seen to be

$$F_{\mathfrak{g}}(T_1, T_2) = \begin{pmatrix} 0 & T_1 & 0 & T_2 \\ -T_1 & 0 & T_2 & 0 \\ 0 & -T_2 & 0 & T_1 \\ -T_2 & 0 & -T_1 & 0 \end{pmatrix}.$$

Note that $\det F_{\mathfrak{g}}(T_1, T_2) = (T_1^2 + T_2^2)^2$. By Theorem 5.3 the faithful dimension of $\mathscr{G}_q$ is given by

$$\min\left\{ f q^{\mathrm{rk}_{\mathbb{F}_q}(F_{\mathfrak{g}}(x_{11},x_{12}))/2} + f q^{\mathrm{rk}_{\mathbb{F}_q}(F_{\mathfrak{g}}(x_{21},x_{22}))/2} : \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q) \right\}.$$

For $p \equiv 1 \pmod 4$, let α denote a square root of -1 in $\mathbb{F}_q$. Then the trivial lower bound $2fq$ can be realized by the choice of vectors $(\alpha, 1)$ and $(-\alpha, 1)$. We now consider the case $p \equiv 3 \pmod 4$. For these primes, observe that -1 is a square in $\mathbb{F}_q$ if and only if f is even. By the above argument the faithful dimension of $\mathscr{G}_q$ is $2fq$ when f is even. Now suppose that f is odd. Then -1 is not a square in $\mathbb{F}_q$, and therefore $\det F_{\mathfrak{g}}(a_1, a_2) \neq 0$ for all non-zero vectors $(a_1, a_2) \in \mathbb{F}_q^2$. This implies that

$$\mathrm{rk}_{\mathbb{F}_q}(F_{\mathfrak{g}}(a_1, a_2)) = 4 \quad \text{for all } 0 \neq (a_1, a_2) \in \mathbb{F}_q^2.$$

Therefore the faithful dimension of $\mathscr{G}_q$ is at least $2fq^2$, which can be realized by the standard basis.

5.4 Details for Example 2.3

The commutator relations imply that $\mathfrak{g}' = \mathrm{Z}(\mathfrak{g}) = \mathrm{Span}_{\mathbb{Z}}\{v_7, v_8\}$, implying that $\mathfrak{g}$ is a 2-step nilpotent Lie algebra with the commutator matrix given by

$$F_{\mathfrak{g}}(T_1, T_2) = \begin{pmatrix} 0 & M \\ -M^{\mathrm{tr}} & 0 \end{pmatrix} \quad \text{where } M := M(T_1, T_2) = \begin{pmatrix} T_1 & T_2 & 0 \\ 0 & T_1 & T_2 \\ -T_2 & T_2 & T_1 \end{pmatrix}. \tag{28}$$

By Theorem 5.3 the faithful dimension of $\mathscr{G}_p$ is given by

$$\min\left\{ p^{\mathrm{rk}_{\mathbb{F}_p}(M(x_{11},x_{12}))} + p^{\mathrm{rk}_{\mathbb{F}_p}(M(x_{21},x_{22}))} : \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p) \right\}.$$

A simple inspection of 2×2 minors of M shows that for a non-zero vector (T_1, T_2), the matrix $M(T_1, T_2)$ has rank at least 2, implying $m_{\text{faithful}}(\mathscr{G}_p) \geqslant 2p^2$. Note that $\det M = T_1^3 - T_1 T_2^2 - T_2^3$ is the homogenization of the polynomial $T_1^3 - T_1 - 1$. This leads us to consider the number of roots of $f(T) = T^3 - T - 1$ over $\mathbb{F}_p$.

At this point we will make a digression and consider the more general question of determining the number of roots of a given integer polynomial over finite fields. Let C_f be the companion matrix of a given polynomial $f(T) \in \mathrm{Z}[T]$, and set $M(T_1, T_2) = T_1 I_{d\times d} - T_2 C_f$, where

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

$d := \deg f(T)$. The determinant of $M(T_1, T_2)$ is the homogenization of $f(T)$. This construction leads to a general collection of interesting examples of 2-step nilpotent Lie algebras with commutator matrix as in (28). We refer the reader to Serre's book [Ser12, § 2.1.2] or his beautiful paper [Ser03] for more details on what follows.

Let $f(T) \in \mathbb{Z}[T]$ be a monic integer polynomial. The discriminant of $f(T)$ is defined to be

$$\mathrm{Disc}_f = \Delta_f^2, \quad \Delta_f = \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j),$$

where $\alpha_1, \ldots, \alpha_n$ are the roots of $f(T)$ in an algebraic closure of $\mathbb{Q}$. Note that since $f(T)$ is a monic polynomial, the discriminant Disc_f is in $\mathbb{Z}$. Henceforth, p will denote an odd prime which does not divide Disc_f. Denote the reduction of $f(T)$ modulo p by $\bar{f}$. Then the roots of $\bar{f}(T)$ are also simple. Define $\mathcal{O}_f = \mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_f$ such that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Such an ideal exists since $\mathcal{O}_f$ is integral over $\mathbb{Z}$. For such a prime we can define a unique element in the Galois group of f, which is called the Frobenius automorphism.

THEOREM 5.7 (Dedekind). *Let $E = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ be the splitting field of $f(T)$. There exists a unique element $\sigma_\mathfrak{p} \in \mathrm{Gal}(E/\mathbb{Q})$ such that $\sigma_\mathfrak{p}(\alpha) \equiv \alpha^p \bmod \mathfrak{p}$, for all $\alpha \in \mathcal{O}_f$. Moreover, if $\bar{f}(T) = f_1(T) \cdots f_g(T)$ with f_i irreducible over $\mathbb{F}_p$ of degree n_i, then $\sigma_\mathfrak{p}$, when viewed as a permutation of the roots of f, has the cyclic decomposition $\sigma_1 \cdots \sigma_g$ with σ_i a cycle of length n_i.*

Proof. See [Jac85, Theorems 4.37 and 4.38]. □

For a monic integer polynomial $f(T) \in \mathbb{Z}[T]$ define

$$N_f(p) := \#\{a \in \mathbb{F}_p : f(a) = 0\}.$$

Theorem 5.7 shows that $N_f(p)$ also counts the number of fixed points of $\sigma_\mathfrak{p}$ permuting the roots of f.

Let $\mathcal{O}_E$ be the ring of integers of E and $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_E$ such that $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$, where p does not divide the discriminant of E. Then, as above, one can prove the existence of a unique automorphism $\sigma_\mathfrak{P} \in \mathrm{Gal}(E/\mathbb{Q})$ such that $\sigma_\mathfrak{P}(\alpha) \equiv \alpha^p \pmod{\mathfrak{P}}$ for all $\alpha \in \mathcal{O}_E$. Let $\mathfrak{P} \cap \mathcal{O}_f = \mathfrak{p}$. Since the elements of $\mathrm{Gal}(E/\mathbb{Q})$ are uniquely determined by their restrictions to $\mathcal{O}_f$, we have $\sigma_\mathfrak{P} = \sigma_\mathfrak{p}$. The automorphism $\sigma_\mathfrak{p}$ is called the *Frobenius automorphism* and it describes the splitting behaviour of the prime p. It is well known that p splits completely in E if and only if $\sigma_\mathfrak{p}$ is the identity element. Now let $\mathfrak{P}$ and $\mathfrak{P}'$ be two primes in $\mathcal{O}_E$ lying above the rational prime p. One can show (see [Neu99, § 9] for more details) that there exists $\tau \in \mathrm{Gal}(E/\mathbb{Q})$ such that $\tau \sigma_\mathfrak{P} \tau^{-1} = \sigma_{\mathfrak{P}'}$. This implies that the conjugacy class of $\sigma_\mathfrak{P}$ is independent of the choice of $\mathfrak{P}$. Let us now turn to the question of computing $N_f(p)$ when $f(T)$ is a cubic polynomial. The following proposition relates the Legendre symbol of the discriminant of f to the number of the irreducible factors of $\bar{f}$.

PROPOSITION 5.8. *Let $f(T) \in \mathbb{Z}[T]$ be a monic irreducible polynomial of degree n with the discriminant D, and suppose p is an odd prime which does not divide the discriminant of f. If $\bar{f} = f_1 \cdots f_g$ with f_i irreducible over $\mathbb{F}_p$ then $\left(\frac{D}{p}\right) = (-1)^{n-g}$, where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol.*

Proof. Continuing to use the same notation as before, we denote the splitting field of f by E and its ring of integers by $\mathcal{O}_E$. Set $D = \mathrm{Disc}_f$ and set $K = \mathbb{Q}(\sqrt{D})$ which is a subfield of E. Let $\mathfrak{p}$ be a prime in $\mathcal{O}_E$ lying over p and write $\wp = \mathfrak{p} \cap K$. Then $\sigma_\wp := \sigma_{\mathfrak{p}|_K}$ is the Frobenius

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

automorphism assigned to $\wp$ in $K/\mathbb{Q}$. Suppose $\sigma_{\mathfrak{p}}$ is an even permutation. Then $\sigma_{\mathfrak{p}}(\Delta_f) = \Delta_f$ and so $\sigma_\wp$ is trivial over K, which implies that $\left(\frac{D}{p}\right) = 1$. If, on the other hand, $\sigma_{\mathfrak{p}}$ is an odd permutation, then $\sigma_{\mathfrak{p}}(\Delta_f) = -\Delta_f$, and $\sigma_\wp$ is not-trivial, implying that $\left(\frac{D}{p}\right) = -1$. We have thus shown that $\operatorname{sgn}(\sigma_{\mathfrak{p}}) = \left(\frac{D}{p}\right)$. Let $n_i = \deg f_i$. Viewing $\sigma_{\mathfrak{p}}$ as a permutation of the roots of f, from Theorem 5.7, we obtain

$$\operatorname{sgn}(\sigma_{\mathfrak{p}}) = (-1)^{\sum_{i=1}^{g}(n_i-1)} = (-1)^{n-g},$$

since $\sum_{i=1}^{g} n_i = n$. This finishes the proof. □

As an application we obtain the following result.

Corollary 5.9. *Let $f(T) \in \mathbb{Z}[T]$ be an irreducible monic cubic polynomial with discriminant D, and suppose p is an odd prime which does not divide D. Then*

$$N_f(p) = \begin{cases} 0 \text{ or } 3 & \text{if } \left(\dfrac{D}{p}\right) = 1, \\ 1 & \text{if } \left(\dfrac{D}{p}\right) = -1. \end{cases}$$

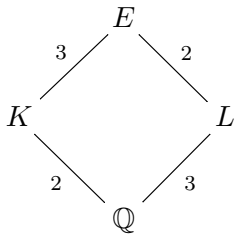
We now turn to the special case $f(T) = T^3 - T - 1$. The discriminant of f is -23 and then by the quadratic reciprocity we deduce that for $p \neq 23$

$$N_f(p) = \begin{cases} 0 \text{ or } 3 & \text{if } \left(\dfrac{p}{23}\right) = 1, \\ 1 & \text{if } \left(\dfrac{p}{23}\right) = -1. \end{cases}$$

When $\left(\frac{p}{23}\right) = 1$, we will need the reduction theory of binary quadratic forms to determine $N_f(p)$. We refer the reader to [Fla89, ch. 2, § 8] for more details. Let $\Delta < 0$ be an integer and assume that $\Delta \equiv 0, 1 \pmod 4$. The modular group $\mathrm{SL}_2(\mathbb{Z})$ acts on

$$\Sigma_\Delta := \{g(x,y) = ax^2 + bxy + cy^2 : a, b, c \in \mathbb{Z}, a > 0, \gcd(a,b,c) = 1, b^2 - 4ac = \Delta\},$$

by linear change of variables. By the reduction theory of positive definite integral binary quadratic forms (for example see [Cox13, Theorem 3.9]), the number $h(\Delta)$ of $\mathrm{SL}_2(\mathbb{Z})$-orbits is finite. This number is called the *class number* of Δ. In the case at hand, we have $h(-23) = 3$, and $\mathrm{SL}_2(\mathbb{Z})$-orbits of Σ_{-23} are represented by the forms $x^2 + xy + 6y^2$ and $2x^2 \pm xy + 3y^2$. Note that $2x^2 + xy + 3y^2$ and $2x^2 - xy + 3y^2$ are $\mathrm{GL}_2(\mathbb{Z})$-equivalent and thus represent the same set of integers. It is easy to show that $\left(\frac{p}{23}\right) = 1$, if and only if p is represented by exactly one of the form $x^2+xy+6y^2$ or $2x^2+xy+3y^2$ (see [Fla89, Proposition 10.2]). Let L be the cubic extension of $\mathbb{Q}$ obtained by adding a root of $f(T)$ and set $K = \mathbb{Q}(\sqrt{-23})$.



https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

Note that $\mathrm{Gal}(E/\mathbb{Q}) = S_3$. For $p \neq 23$, set $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$. Since the class number of K is 3 and E is unramified over K, E is the Hilbert class field of K, i.e. the maximal unramified abelian extension of K. From this we can conclude that $\mathfrak{p}$ splits completely in E if and only if $\mathfrak{p}$ is a principal ideal [Cox13, Corollary 5.25]. Moreover, note that the ring of integers of the quadratic extension K is $\mathbb{Z}[(1+\sqrt{-23})/2]$ and so $\mathfrak{p}$ is a principal ideal if and only if $p = x^2 + xy + 6y^2$. Putting all these together, we conclude that $p = x^2 + xy + 6y^2$ if and only if p splits completely in E. This means that $T^3 - T - 1$ has three roots in $\mathbb{F}_p$ if and only if $p = x^2 + xy + 6y^2$. This also shows that $p = 2x^2 + xy + 3y^2$ if and only if $T^3 - T - 1$ has no root in $\mathbb{F}_p$. Consequently,

$$N_f(p) = \begin{cases} 1 & \text{if } \left(\frac{p}{23}\right) = -1, \\ 0 & \text{if } p \text{ is of the form } 2x^2 + xy + 3y^2, \\ 3 & \text{if } p \text{ is of the form } x^2 + xy + 6y^2. \end{cases} \tag{29}$$

Let $N_{\mathbf{X}}(p)$ denote the number of rational points of the projective variety $\mathbf{X} := T_1^3 - T_1T_2^2 - T_2^3 = 0$ in $\mathbf{P}^1(\mathbb{F}_p)$. Then from (29), for all $p \neq 23$ we obtain

$$N_{\mathbf{X}}(p) = \begin{cases} 1 & \text{if } \left(\frac{p}{23}\right) = -1, \\ 0 & \text{if } p \text{ is of the form } 2x^2 + xy + 3y^2, \\ 3 & \text{if } p \text{ is of the form } x^2 + xy + 6y^2. \end{cases}$$

When $\left(\frac{p}{23}\right) = -1$, we have $N_{\mathbf{X}}(p) = 1$ and hence the faithful dimension of $\mathscr{G}_p$ equals $p^2 + p^3$. When p is of the form $2x^2 + xy + 3y^2$ then $N_{\mathbf{X}}(p) = 0$ and so the minimum is exactly $2p^3$. This implies that the faithful dimension is $2p^3$. In the remaining case, we can find distinct points (x_{11}, x_{12}) and (x_{21}, x_{22}) in $\mathbf{X}$. Since $M(x_{11}, x_{12})$ and $M(x_{21}, x_{22})$ have both rank 2, it follows that in this case the faithful dimension is $2p^2$. Moreover, $T_1^3 - T_1 - 1$ has a double root and a simple root in $\mathbb{F}_{23}$. Thus the same argument shows that in this case the faithful dimension is $2(23)^2$.

5.5 Details for Example 2.4

The commutator relations imply that $\mathfrak{g}' = \mathrm{Z}(\mathfrak{g}) = \mathrm{Span}_{\mathbb{Z}}\{v_6, v_7, v_8\}$, implying that $\mathfrak{g}$ is a 2-step nilpotent Lie algebra with the commutator matrix given by

$$F_{\mathfrak{g}}(T_1, T_2, T_3) = \begin{pmatrix} 0 & M \\ -M^{\mathrm{tr}} & 0 \end{pmatrix}, \quad M := M(T_1, T_2, T_3) = \begin{pmatrix} T_1 & T_2 \\ T_3 & T_1 \\ 2T_2 & T_3 \end{pmatrix}.$$

For a given odd prime p, and a non-zero vector $(T_1, T_2, T_3) \in \mathbb{F}_p^3$, the rank over $\mathbb{F}_p$ of M is equal to 1 if and only if (T_1, T_2, T_3) is proportional to $(\lambda^2/2, \lambda/2, 1)$ such that $\lambda^3 - 2 = 0$, and is equal to 2 otherwise. Set $f(\lambda) = \lambda^3 - 2$. As noted in [Lee16, Corollary 2.3],

$$N_f(p) = \begin{cases} 1 & \text{if } p \equiv 2 \pmod 3 \text{ or } p = 3, \\ 3 & \text{if } p \equiv 1 \pmod 3 \text{ and } p \text{ is represented by the form } x^2 + 27y^2, \\ 0 & \text{if } p \equiv 1 \pmod 3 \text{ and } p \text{ is not represented by the form } x^2 + 27y^2. \end{cases}$$

The rest of the argument is similar to Example 2.3.

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

6. Proofs of Theorems 2.5 and 2.7

Before we begin the proofs of Theorems 2.5 and 2.7, let us recall the setting. As before, let $\mathfrak{g}$ be a nilpotent $\mathbb{Z}$-Lie algebra of nilpotency class c which is finitely generated as an abelian group, and set $q := p^f$ for some $f \geqslant 1$. Let $F_{\mathfrak{g}}(T_1, \dots, T_m)$ denote the matrix of linear forms that is defined in (18). Since $F_{\mathfrak{g}}(T_1, \dots, T_m)$ is a skew-symmetric $n \times n$ matrix it follows that for all $x_1, \dots, x_m \in \mathbb{F}_q$, the rank of $F_{\mathfrak{g}}(x_1, \dots, x_m)$ is an even number no larger than n. Let M be the set of all integer vectors $\mu = (a_1, \dots, a_{l_1}) \in \mathbb{Z}^{l_1}$, with $0 \leqslant a_i \leqslant n/2$, and assign to each $\mu \in M$ the polynomial of degree at most $n/2$ given by

$$g_\mu(T) = T^{a_1} + \cdots + T^{a_{l_1}} + l_2.$$

Since g_μ is symmetric in $a_1, \dots, a_{l_1}$, we will only consider those integer vectors μ with

$$a_1 \leqslant \cdots \leqslant a_{l_1},$$

and order them with the *reverse lexicographical order*, i.e. $\mu \lhd \mu'$ if the rightmost non-zero component of the vector $\mu' - \mu$ is positive. If $\mu \lhd \mu'$ and $q > l_1$, then we can easily see that

$$g_\mu(q) < g_{\mu'}(q). \tag{30}$$

Since $r = \#M < \infty$, we can sort its elements as $\mu_1 \lhd \cdots \lhd \mu_r$. For a given vector μ, define the following affine variety associated to $\mu = (a_1, \dots, a_{l_1})$:

$$\mathbf{X}_\mu := \left\{ (x_{ij}) \in \mathrm{M}_{l_1,m}(\mathbb{C}) : \mathrm{rk}_{\mathbb{C}}(F_{\mathfrak{g}}(x_{i1}, \dots, x_{im})) = 2a_i, \det \begin{pmatrix} x_{11} & \cdots & x_{1l_1} \\ \vdots & \ddots & \vdots \\ x_{l_1 1} & \cdots & x_{l_1 l_1} \end{pmatrix} \neq 0 \right\}.$$

Note that the non-vanishing condition on the determinant can be turned into an equation by introducing a new variable, standing for the inverse of the determinant. We also remark that $\mathbf{X}_\mu$ is defined over $\mathbb{Z}$ because $F_{\mathfrak{g}}(T_1, \dots, T_m)$ is an integer matrix.

6.1 Proof of Theorem 2.5

For $\mu \in M$ set

$$\Sigma_\mu := \{p > \max\{l_1, c, C_1, C_2, C_3\} : \mathbf{X}_\mu(\mathbb{F}_p) \neq \emptyset\},$$

where the C_i are as in Theorem 5.3. For every integer k such that $1 \leqslant k \leqslant r$, Theorem 5.3 and (30) imply that $m_{\text{faithful}}(\mathscr{G}_p) = g_{\mu_k}(p)$ whenever

$$p \in \mathscr{P}_k := \Sigma_{\mu_k} \setminus \bigcup_{1 \leqslant i < k} \Sigma_{\mu_i}.$$

Since finite sets are Frobenius, the assertion of Theorem 2.5 now follows from the following theorem due to Ax [Ax67, Theorem 1].

Theorem 6.1 (Ax). *With the above notation, Σ_μ is a Frobenius set.*

Remark 6.2. An analogue of Theorem 2.5 holds for $m_{\text{faithful}}(\mathscr{G}_{p^f})$ when f is fixed and p varies. This statement can be established by a modification of the proof given above and applying [Ser12, § 7.2.4, Example 2].

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

6.2 Proof of Theorem 2.7

The proof of this theorem is similar to that of Theorem 2.5. Hence we will maintain the notation for the matrix $F_{\mathfrak{g}}(T_1, \ldots, T_m)$, the ordered set M, the polynomial g_μ, and the variety $\mathbf{X}_\mu$ as above. Now assume that $p > C$, where

$$C := \max\{l_1, c, C_1, C_2, C_3\}. \tag{31}$$

Consider the sets

$$\Sigma'_\mu := \{f \geqslant 1 : \mathbf{X}_\mu(\mathbb{F}_{p^f}) \neq \emptyset\}.$$

It follows from a theorem of Dwork [Ser12, p. 6 and § 4.3] that there exists a function $\nu : \mathbb{C} \to \mathbb{Z}$ with finite support such that

$$N_{\mathbf{X}_\mu}(p^f) := \#\mathbf{X}_\mu(\mathbb{F}_{p^f}) = \sum_{z \in \mathbb{C}} \nu(z) z^f. \tag{32}$$

It is easy to see that the sequence $c_f = N_{\mathbf{X}_\mu}(p^f)$ satisfies a linear recurrence relation of the form $c_n = \sum_{k=1}^{r} a_k c_{n-k}$. We will now invoke the following theorem of Skolem, Mahler and Lech.

THEOREM 6.3 (Skolem–Mahler–Lech [MVdP95]). *Let $\{u_n\}_{n \geqslant 1}$ be a sequence of complex numbers satisfying a linear recurrence equation. Then its zero set $\{n : u_n = 0\}$ is a union of a finite set and a finite number of sets of the form $n \equiv a \pmod{b}$ for integers a, b.*

One can easily verify that the sets of the form $F \cup A$, where F is finite and A is a finite union of arithmetic progressions form a Boolean algebra. To complete the proof of Theorem 2.7, note that from (30) and Theorem 5.3 it follows that if $p > C$ and $f \in \mathscr{A}_k := \Sigma'_{\mu_k} \setminus \bigcup_{1 \leqslant i < k} \Sigma'_{\mu_i}$ then $m_{\text{faithful}}(\exp(\mathscr{G}_q)) = f g_k(q)$.

7. Free nilpotent Lie algebras

In this section we will consider faithful representations of groups related to free nilpotent and free metabelian Lie algebras. Let us recall some definitions. The free nilpotent Lie algebra of class c on n generators, denoted by $\mathfrak{f}_{n,c}$, is the free object in the category of n-generated nilpotent Lie algebras (over $\mathbb{Z}$) of class c. More concretely, $\mathfrak{f}_{n,c}$ can be constructed from the free Lie algebra on n generators after quotienting out the ideal generated by commutators of length $c + 1$.

Recall that a Lie algebra $\mathfrak{l}$ is called metabelian if $[[\mathfrak{l}, \mathfrak{l}], [\mathfrak{l}, \mathfrak{l}]] = 0$. Similarly, one can define the *free metabelian Lie algebra* of class c on n generators as the free object in the category of n-generated metabelian Lie algebras of class c.

For computational purposes, it will be convenient to work with *Hall bases* of free nilpotent Lie algebras. We will briefly review their constructions, and refer the reader to [Bou98, ch. II] or [Ser06, ch. IV] for more details.

7.1 Hall bases of free nilpotent Lie algebras

Our exposition of the notion of a Hall basis follows [Bou98, ch. II] or [Ser06, ch. IV]. We will first need some basic definitions. A set M with a map $M \times M \to M$ sending $(x, y) \mapsto [x, y]$ is called a *magma*. Let X be a set and define inductively a family of sets X_n $(n \geqslant 1)$ as follows: $X_1 = X$ and $X_n = \amalg_{p+q=n}(X_p \times X_q)$. Let $M(X)$ denote the disjoint union $\amalg_{n=1}^{\infty} X_n$ and define $M(X) \times M(X) \to M(X)$ via $X_p \times X_q \to X_{p+q} \subseteq M(X)$. The magma $M(X)$ is called

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

the *free magma* on X. An element w of $M(X)$ is called a non-associative word on X. Its length, $\ell(w)$, is the unique n such that $w \in X_n$.

Definition 7.1. A *Hall set* relative to X is a totally ordered subset $\mathcal{H}$ of $M(X)$ satisfying the following conditions:

(A) if $u \in \mathcal{H}$, $v \in \mathcal{H}$ and $\ell(u) < \ell(v)$, then $u < v$ in the total order;
(B) $X \subseteq \mathcal{H}$ and $\mathcal{H} \cap X_2$ consists of the products $[x, y]$ with x, y in X and $x < y$;
(C) an element w of $M(X)$ of length $\geqslant 3$ belongs to $\mathcal{H}$ if and only if it is of the form $[a, [b, c]]$ with a, b, c in $\mathcal{H}$, $[b, c] \in \mathcal{H}$, $b \leqslant a < [b, c]$ and $b < c$.

In the rest of this section, $[x, y]$ denotes the Lie bracket of a free Lie algebra. Set $\mathcal{H}^i = \mathcal{H} \cap X_i$ and let $\#X = n$. The rank of $\mathfrak{f}_n^k/\mathfrak{f}_n^{k+1}$ is given by Witt's formula:

$$r_n(k) := \frac{1}{k} \sum_{d|k} \mu(d) n^{k/d},$$

where μ is the Möbius function. Under the natural projection $\mathfrak{f}_n^k \to \mathfrak{f}_n^k/\mathfrak{f}_n^{k+1}$, the images of elements of $\mathcal{H}^k$ form a $\mathbb{Z}$-basis of $\mathfrak{f}_n^k/\mathfrak{f}_n^{k+1}$. For a proof see [Bou98, ch. II] or [Ser06, Theorem 4.2]. Let $\mathfrak{f}_{n,c} := \mathfrak{f}_{n,c}(\mathbb{Z})$ be the free nilpotent $\mathbb{Z}$-Lie algebra on n generators and of class c; it is defined to be the quotient algebra $\mathfrak{f}_n/\mathfrak{f}_n^{c+1}$. The following facts are well known. Since we do not know a reference and their proofs are easy, we outline the arguments.

Proposition 7.2. *For $n \geqslant 2$ and $c \geqslant 2$, we have the following.*

(1) *The image of $\bigcup_{i=1}^{c} \mathcal{H}^i$ under the natural projection $\mathfrak{f}_n \to \mathfrak{f}_{n,c}$ is a basis of $\mathfrak{f}_{n,c}$.*
(2) *The image of $\bigcup_{i=2}^{c} \mathcal{H}^i$ under the natural projection $\mathfrak{f}_n \to \mathfrak{f}_{n,c}$ is a basis of $\mathfrak{f}'_{n,c}$.*
(3) *The image of $\mathcal{H}^c$ under the natural projection $\mathfrak{f}_n \to \mathfrak{f}_{n,c}$ is a basis of $\mathrm{Z}(\mathfrak{f}_{n,c})$.*

Proof. The first statement follows from the fact that $\bigcup_{i=1}^{\infty} \mathcal{H}^i$ is a basis of $\mathfrak{f}_n$, and the $\mathbb{Z}$-submodule $\mathfrak{f}_n^{c+1}$ of $\mathfrak{f}_n$ is generated by $\bigcup_{i=c+1}^{\infty} \mathcal{H}^i$. For the second statement, it is now enough to note that $\bigcup_{i=2}^{c} \mathcal{H}^i$ generates the $\mathbb{Z}$-module $\mathfrak{f}'_{n,c}$. The proof of the third statement is similar. □

Example 7.3. The image of $\bigcup_{i=1}^{3} \mathcal{H}^i$ under the natural projection $\mathfrak{f}_3 \to \mathfrak{f}_{3,3}$ is a basis of $\mathfrak{f}_{3,3}$. The elements of this union are explicitly given as follows:

$$\begin{aligned}
&\mathcal{H}^1 : x_1,\ x_2,\ x_3,\\
&\mathcal{H}^2 : \mathbf{w}_9 = [x_1, x_2], \quad \mathbf{w}_{10} = [x_1, x_3], \quad \mathbf{w}_{11} = [x_2, x_3],\\
&\mathcal{H}^3 : \mathbf{w}_1 = [x_1, [x_1, x_2]], \quad \mathbf{w}_2 = [x_1, [x_1, x_3]], \quad \mathbf{w}_3 = [x_2, [x_1, x_2]], \quad \mathbf{w}_4 = [x_2, [x_1, x_3]],\\
&\qquad \mathbf{w}_5 = [x_2, [x_2, x_3]], \quad \mathbf{w}_6 = [x_3, [x_1, x_2]], \quad \mathbf{w}_7 = [x_3, [x_1, x_3]], \quad \mathbf{w}_8 = [x_3, [x_2, x_3]].
\end{aligned}$$

Note that $\mathrm{Z}(\mathfrak{f}_{3,3}) \subseteq \mathfrak{f}'_{3,3}$ and furthermore one can check that the image of $\{\mathbf{w}_1, \ldots, \mathbf{w}_8\}$ is a basis of $\mathrm{Z}(\mathfrak{f}_{3,3})$, while the image of $\{\mathbf{w}_1, \ldots, \mathbf{w}_{11}\}$ is a basis of $\mathfrak{f}'_{3,3}$. By an explicit calculation and using the Jacobi identity, we obtain the following commutator matrix

$$F_{\mathfrak{f}_{3,3}}(T_1, \ldots, T_{11}) = \left(\begin{array}{ccc|ccc} 0 & T_9 & T_{10} & T_1 & T_2 & T_4 - T_6 \\ -T_9 & 0 & T_{11} & T_3 & T_4 & T_5 \\ -T_{10} & -T_{11} & 0 & T_6 & T_7 & T_8 \\ \hline -T_1 & -T_3 & -T_6 & 0 & 0 & 0 \\ -T_2 & -T_4 & -T_7 & 0 & 0 & 0 \\ T_6 - T_4 & -T_5 & -T_8 & 0 & 0 & 0 \end{array}\right) = \begin{pmatrix} F_{11} & F_{12} \\ -F_{12}^{\mathrm{tr}} & 0 \end{pmatrix}.$$

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

Now we consider the general case. Set

$$m := \sum_{k=2}^{c} r_n(k) \quad \text{and} \quad m_1 := \sum_{k=1}^{c-1} r_n(k).$$

By Proposition 7.2, the natural projection maps $\bigcup_{i=1}^{c-1} \mathcal{H}^i$ to a basis of $\mathfrak{f}_{n,c}/(\mathrm{Z}(\mathfrak{f}_{n,c}))$. Note that the commutator matrix $F_{\mathfrak{f}_{n,c}}(\mathbf{T}) \in M_{m_1}(\mathbb{Z}[\mathbf{T}])$ is a skew-symmetric matrix whose entries are $\mathbb{Z}$-linear forms in m variables. We label the variables as follows. For each $2 \leqslant k \leqslant c$ we write $\mathbf{T}^{(k)} = (T_1^{(k)}, \dots, T_{r_n(k)}^{(k)})$, so that $\mathbf{T} = (\mathbf{T}^{(k)})_{2 \leqslant k \leqslant c}$ and

$$F_{\mathfrak{f}_{n,c}}(\mathbf{T}) = \begin{pmatrix} F_{11}(\mathbf{T}^{(2)}) & F_{12}(\mathbf{T}^{(3)}) & \cdots & F_{1(c-1)}(\mathbf{T}^{(c)}) \\ F_{21}(\mathbf{T}^{(3)}) & F_{22}(\mathbf{T}^{(4)}) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ F_{(c-1)1}(\mathbf{T}^{(c)}) & 0 & 0 & 0 \end{pmatrix},$$

where $F_{ij}(\mathbf{T}^{(i+j)})$ is the zero matrix if $i + j > c$, and $F_{ij}(\mathbf{T}^{(i+j)}) = -F_{ji}^{\mathrm{tr}}(\mathbf{T}^{(i+j)})$.

In order to use Theorem 5.3 to compute the faithful dimension of $\exp(\mathfrak{f}_{n,c} \otimes_{\mathbb{Z}} \mathbb{F}_q)$ we need to find $r_n(c)$ vectors $\mathbf{a}_\ell = (\mathbf{a}_\ell^{(k)})$, $2 \leqslant k \leqslant c$, with $\mathbf{a}_\ell^{(k)} = (a_{\ell 1}^{(k)}, \dots, a_{\ell r_n(k)}^{(k)})$ such that the vectors $\mathbf{a}_\ell$ minimize

$$\sum_{\ell=1}^{r_n(c)} f q^{\mathrm{rk}_{\mathbb{F}_q}(F_{\mathfrak{f}_{n,c}}(\mathbf{a}_\ell))/2},$$

subject to the condition

$$\begin{pmatrix} a_{11}^{(c)} & a_{12}^{(c)} & \cdots & a_{1r_n(c)}^{(c)} \\ \vdots & & & \vdots \\ a_{r_n(c)1}^{(c)} & a_{r_n(c)2}^{(c)} & \cdots & a_{r_n(c)r_n(c)}^{(c)} \end{pmatrix} \in \mathrm{GL}_{r_n(c)}(\mathbb{F}_q). \tag{33}$$

Let us define the *reduced commutator matrix* of $\mathfrak{f}_{n,c}$ to be

$$F_{\mathfrak{f}_{n,c}}^{\mathrm{red}}(\mathbf{T_c}) = \begin{pmatrix} 0 & 0 & \cdots & 0 & F_{1(c-1)}(\mathbf{T}^{(c)}) \\ 0 & 0 & \cdots & F_{2(c-2)}(\mathbf{T}^{(c)}) & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & F_{(c-2)2}(\mathbf{T}^{(c)}) & 0 & \cdots & 0 \\ F_{(c-1)1}(\mathbf{T}^{(c)}) & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

In other words, $F_{\mathfrak{f}_{n,c}}^{\mathrm{red}}$ is the matrix obtained from $F_{\mathfrak{f}_{n,c}}$ by setting the variables $\mathbf{T}^{(k)}$ equal to zero when $k \neq c$, so that the $(i, c-i)$-block of $F_{\mathfrak{f}_{n,c}}^{\mathrm{red}}$ is equal to $F_{i(c-i)}(\mathbf{T}^{(c)})$ for $1 \leqslant i \leqslant c-1$, and all other blocks in $F_{\mathfrak{f}_{n,c}}^{\mathrm{red}}$ are equal to zero. For instance in Example 7.3, the reduced commutator matrix is

$$\begin{pmatrix} 0 & F_{12} \\ -F_{12}^{\mathrm{tr}} & 0 \end{pmatrix}.$$

Note that for each $2 \leqslant k \leqslant c$, the variables $\mathbf{T}^{(k)}$ only occur in the matrices F_{ij} with $i+j = k$. Clearly,

$$\mathrm{rk}_{\mathbb{F}_q}(F_{\mathfrak{f}_{n,c}}(\mathbf{a}_\ell)) \geqslant \sum_{i+j=c} \mathrm{rk}_{\mathbb{F}_q}(F_{ij}(\mathbf{a}_\ell^{(c)})). \tag{34}$$

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

Note that the only entries of $\mathbf{a}_\ell$ that appear in the invertibility condition (33) are those of $\mathbf{a}_\ell^{(c)}$. Further, by setting all of the components of $\mathbf{a}_\ell^k$ to zero for $2 \leqslant k < c$, we do not increase the rank of the matrix $F_{\mathfrak{f}_{n,c}}(\mathbf{a}_\ell)$. Therefore the minima of the two sides of (34) are equal. Thus from Theorem 5.3 we can conclude the following proposition.

Proposition 7.4. *Let $F := F^{\mathrm{red}}_{\mathfrak{f}_{n,c}}$ be the reduced commutator matrix of $\mathfrak{f}_{n,c}$. Then the faithful dimension of $\exp(\mathfrak{f}_{n,c} \otimes_{\mathbb{Z}} \mathbb{F}_q)$ is*

$$\min\left\{\sum_{\ell=1}^{r_n(c)} f q^{\mathrm{rk}_{\mathbb{F}_q}(F(a_{\ell 1},\dots,a_{\ell r_n(c)}))/2} : \begin{pmatrix} a_{11} & \cdots & a_{1r_n(c)} \\ \vdots & \ddots & \vdots \\ a_{r_n(c)1} & \cdots & a_{r_n(c)r_n(c)} \end{pmatrix} \in \mathrm{GL}_{r_n(c)}(\mathbb{F}_q)\right\}.$$

7.2 Proof of Theorem 2.13

We now prove Theorem 2.13. The proof relies upon an explicit description of the commutator matrix and so it is combinatorial in nature. First we consider the statement for $\mathfrak{f}_{n,2}$. The image of the set

$$\mathcal{H}^1 \cup \mathcal{H}^2 = \{x_1, \dots, x_n, x_{ij} : 1 \leqslant i < j \leqslant n\},$$

where $x_{ij} := [x_i, x_j]$ for $1 \leqslant i < j \leqslant n$, is a basis of $\mathfrak{f}_{n,2}$. Thus the commutator matrix of $\mathfrak{f}_{n,2}$ is

$$F_{\mathfrak{f}_{n,2}}(\mathbf{T}) = \begin{pmatrix} 0 & T_{12} & T_{13} & \cdots & T_{1n} \\ -T_{12} & 0 & T_{23} & \cdots & T_{2n} \\ -T_{13} & -T_{23} & 0 & \cdots & T_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -T_{1n} & -T_{2n} & -T_{3n} & \cdots & 0 \end{pmatrix}.$$

Observe that each variable T_{ij}, $1 \leqslant i < j \leqslant n$, appears exactly twice. Therefore if exactly one of the T_{ij} is non-zero, then the rank of the above matrix will be equal to 2. Now by applying Proposition 7.4, we obtain the statement of the theorem for $\mathfrak{f}_{n,2}$.

Let us now turn to the case of $\mathfrak{f}_{n,3}$. First note that the reduced commutator matrix of $\mathfrak{f}_{n,3}$ is equal to

$$F(\mathbf{T}^{(3)}) := F^{\mathrm{red}}_{\mathfrak{f}_{n,3}}(\mathbf{T}^{(3)}) = \begin{pmatrix} 0 & F_{12}(\mathbf{T}^{(3)}) \\ -F_{12}^{\mathrm{tr}}(\mathbf{T}^{(3)}) & 0 \end{pmatrix}.$$

In particular, $\mathrm{rk}_{\mathbb{F}_q}(F(\mathbf{T}^{(3)})) = 2\mathrm{rk}_{\mathbb{F}_q}(F_{12}(\mathbf{T}^{(3)}))$. Our goal is to find $F_{12}(\mathbf{T}^{(3)})$ explicitly with respect to the basis obtained by the image of $\mathcal{H}^1 \cup \mathcal{H}^2 \cup \mathcal{H}^3$. The latter set consists of

$$\begin{aligned} \mathcal{H}^1 &= \{x_i : 1 \leqslant i \leqslant n\}, \\ \mathcal{H}^2 &= \{x_{ij} := [x_i, x_j] : 1 \leqslant i < j \leqslant n\}, \\ \mathcal{H}^3 &= \{x_{ijk} := [x_i, [x_j, x_k]] : 1 \leqslant j \leqslant i \leqslant n, 1 \leqslant j < k \leqslant n\}. \end{aligned}$$

Consider the sets $R_1 := \{1, 2, \dots, n\}$, $R_2 := \{(i, j) : 1 \leqslant i < j \leqslant n\}$, and

$$R_3 := \{(i, j, k) : 1 \leqslant j \leqslant i \leqslant n, 1 \leqslant j < k \leqslant n\}.$$

The elements of the R_i parameterize the sets $\mathcal{H}^1, \mathcal{H}^2$ and $\mathcal{H}^3$. Set

$$d := \#R_3 = r_n(3) = (n^3 - n)/3,$$

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

and define

$$R_3^0 := \{(i,j,i) : 1 \leqslant j < i \leqslant n\} \cup \{(i,i,k) : 1 \leqslant i < k \leqslant n\},$$
$$R_3^+ := \{(i,j,k) \in R_3 : j < i < k\},$$
$$R_3^- := \{(i,j,k) \in R_3 : j < k < i\}.$$

It is clear that $R_3 = R_3^0 \cup R_3^+ \cup R_3^-$ is a partition of R_3. We will now give an explicit description of $F_{12}(\mathbf{T}^{(3)})$ in terms of these sets. It will be more convenient to use the variables T_α with $\alpha \in R_3$ instead of $\mathbf{T}^{(3)} = (T_1^{(3)}, \dots, T_{r_n(3)}^{(3)})$. We will also use $\mathbf{T}$ to denote the vector with entries T_α with $\alpha \in R_3$. For instance T_{213} and T_{312} correspond, respectively, to T_4 and T_6 in Example 7.3. For $i \in R_1$ and $(j,k) \in R_2$, a simple computation shows that

$$[x_i, [x_j, x_k]] = \begin{cases} x_{ijk} & \text{if } (i,j,k) \in R_3, \\ x_{jik} - x_{kij} & \text{otherwise.} \end{cases} \tag{35}$$

Therefore the entry of the matrix F_{12} in the row associated to $i \in R_1$ and column associated to $(j,k) \in R_2$ is given by T_{ijk} if $(i,j,k) \in R_3$ and by $T_{jik} - T_{kij}$ otherwise.

LEMMA 7.5. *For $1 \leqslant i,j,k \leqslant n$ the following hold.*

(a) *For $i < k$, the variable T_{iik} appears exactly once in $F_{12}(\mathbf{T})$, namely, in row i and column (i,k).*
(b) *For $j < i$, the variable T_{iji} appears exactly once in $F_{12}(\mathbf{T})$, namely, in row i and column (j,i).*
(c) *For $(i,j,k) \in R_3^+$, the variable T_{ijk} appears exactly twice in the entries of $F_{12}(\mathbf{T})$. Namely, the entry in row i and column (j,k) is equal to T_{ijk}, and the entry in row j and column (i,k) is equal to $T_{ijk} - T_{kji}$.*
(d) *For $(i,j,k) \in R_3^-$, the variable T_{ijk} appears exactly twice in $F_{12}(\mathbf{T})$. Namely, the entry in row i and column (j,k) is equal to T_{ijk}, and the entry in row j and column (k,i) is equal to $T_{kji} - T_{ijk}$.*

Proof of the Lemma 7.5. Parts (a) and (b) of the lemma are clear, since if T_{ijk} appears twice then i,j,k must be pairwise distinct. We will now prove part (c). Suppose $j < i < k$. It is clear from (35) that T_{ijk} can only potentially appear in a bracket of the form $[x_\alpha, [x_\beta, x_\gamma]]$, where the indices are permutations of i,j,k and $\beta < \gamma$. This leaves three possibilities $(\alpha,\beta,\gamma) = (i,j,k), (j,i,k), (k,j,i)$. However, since $[x_k, [x_j, x_i]] = x_{kji} \in \mathcal{H}^3$, the third possibility does not occur. Moreover,

$$[x_j, [x_i, x_k]] = [x_i, [x_j, x_k]] - [x_k, [x_j, x_i]] = x_{ijk} - x_{kji},$$

which proves the statement. Part (d) can be proven in a similar way. □

From this it follows that $\mathrm{rk}_{\mathbb{F}_q}(F_{12}(\mathbf{a})) \geqslant 1$ for every non-zero vector $\mathbf{a} \in \mathbb{F}_q^d$, where $d := r_n(3)$. In the rest of this section, for each $\alpha \in R_3$, we will find a vector $\mathbf{a}_\alpha = (a_{1,\alpha}, \dots, a_{d,\alpha}) \in \mathbb{F}_q^d$ such that the rank of $M_\alpha := F_{12}(\mathbf{a}_\alpha)$ is equal to 1 and the M_α are linearly independent matrices over $\mathbb{F}_q$. It follows that the $\mathbf{a}_\alpha$ are linearly independent over $\mathbb{F}_q$ and thus the matrix $(\mathbf{a}_\alpha)_{\alpha \in R_3}$ is invertible. Then from Proposition 7.4 we conclude that the faithful dimension of $\exp(\mathfrak{f}_{n,3} \otimes_{\mathbb{Z}} \mathbb{F}_q)$ is equal to $r_n(3)fq$ when $p \geqslant 5$.

We now construct M_α for $\alpha \in R_3$. For every $\delta = (i,j,k)$ with $1 \leqslant i,j,k \leqslant n$, define

$$\delta^+ := \max\{i,j,k\}, \quad \delta^- := \min\{i,j,k\}, \quad \delta^0 := i + j + k - \delta^+ - \delta^-.$$

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

(I): Suppose $\alpha = (i,j,k) \in R_3^0$, that is $i = k$ or $i = j$. In either case, T_{ijk} appears only once in $F_{12}(\mathbf{T})$ by parts (a) and (b) of Lemma 7.5. Let M_α be the matrix obtained from $F_{12}(\mathbf{T})$ by setting $T_{ijk} = 1$ and letting the rest of variables to be zero. Then the rank of M_α is 1.

(II): Let $\alpha = (i,j,k) \in R_3^+$, that is $j < i < k$. Let M_α be the matrix obtained from $F_{12}(\mathbf{T})$ by setting $T_{ijk} = T_{iik} = T_{jjk} = 1$, and zero for the rest of variables. From part (c) of Lemma 7.5 we can see that in this case

$$M_\alpha = \begin{array}{c} \\ j \\ \\ i \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccc} & (j,k) & & (i,k) & \end{array} \\ \begin{pmatrix} \cdots & \vdots & \cdots & \vdots & \cdots \\ \cdots & T_{jjk} & \cdots & T_{ijk} - T_{kji} & \cdots \\ \cdots & \vdots & \cdots & \vdots & \cdots \\ \cdots & T_{ijk} & \cdots & T_{iik} & \cdots \\ \cdots & \vdots & \cdots & \vdots & \cdots \end{pmatrix} \end{array} = \begin{array}{c} \\ j \\ \\ i \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccc} & (j,k) & & (i,k) & \end{array} \\ \begin{pmatrix} \cdots & \vdots & \cdots & \vdots & \cdots \\ \cdots & 1 & \cdots & 1 & \cdots \\ \cdots & \vdots & \cdots & \vdots & \cdots \\ \cdots & 1 & \cdots & 1 & \cdots \\ \cdots & \vdots & \cdots & \vdots & \cdots \end{pmatrix} \end{array}.$$

Note that this matrix has rank 1 and the rows in which non-zero entries are located correspond to the α^- and α^0.

(III): Let $\alpha = (i,j,k) \in R_3^-$, that is $j < k < i$. Let M_α be the matrix obtained from $F_{12}(\mathbf{T})$ by setting $T_{jjk} = T_{ijk} = 1$ and $T_{iki} = -1$ and zero elsewhere. One can verify that in this case

$$M_\alpha = \begin{array}{c} \\ j \\ \\ i \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccc} & (j,k) & & (k,i) & \end{array} \\ \begin{pmatrix} \cdots & \vdots & \cdots & \vdots & \cdots \\ \cdots & T_{jjk} & \cdots & T_{kji} - T_{ijk} & \cdots \\ \cdots & \vdots & \cdots & \vdots & \cdots \\ \cdots & T_{ijk} & \cdots & T_{iki} & \cdots \\ \cdots & \vdots & \cdots & \vdots & \cdots \end{pmatrix} \end{array} = \begin{array}{c} \\ j \\ \\ i \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccc} & (j,k) & & (k,i) & \end{array} \\ \begin{pmatrix} \cdots & \vdots & \cdots & \vdots & \cdots \\ \cdots & 1 & \cdots & -1 & \cdots \\ \cdots & \vdots & \cdots & \vdots & \cdots \\ \cdots & 1 & \cdots & -1 & \cdots \\ \cdots & \vdots & \cdots & \vdots & \cdots \end{pmatrix} \end{array}.$$

Note that this matrix has rank 1 and the rows in which non-zero entries are located correspond to the α^- and α^+.

Let us show that the matrices constructed above are linearly independent. Suppose that

$$M = \sum_{\alpha \in R_3} c_\alpha M_\alpha = 0.$$

We will show that $c_\alpha = 0$ for all $\alpha \in R_3$. Let $\beta = (s,r,t) \in R_3^+$ be an arbitrary element. The definition of R_3^+ implies that $r < s < t$. Consider the entry of M associated to row s and column (r,t). Note that since $s = \beta^0$, a case by case verification shows that the $(s,(r,t))$ entry of every matrix M_α with $\alpha \in R_3^0 \cup R_3^-$ is equal to zero. Furthermore, the only $\alpha \in R_3^+$ for which M_α has a non-zero entry in row s and column (r,t) is $\alpha = \beta$. This gives $c_\beta = 0$, which, in turn, shows that $c_\beta = 0$ for all $\beta \in R_3^+$.

Now let $\gamma = (t',r',s') \in R_3^-$ be an arbitrary element. Then from the definition of R_3^- we have $r' < s' < t'$. Consider the entry of M associated to row t' and column (r',s'). The $(t',(r',s'))$ entry of every matrix M_α with $\alpha \in R_3^0$ is equal to zero. Furthermore, the only $\alpha \in R_3^-$ for which M_α has a non-zero entry in row t' and column (r',s') is $\alpha = \gamma$. Comparing coefficients yields $c_\gamma = 0$. This shows that $c_\gamma = 0$ for all $\gamma \in R_3^-$. Hence

$$M = \sum_{\alpha \in R_3^0} c_\alpha M_\alpha = 0.$$

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

It is however clear that for distinct $\alpha_1, \alpha_2 \in R_3^0$ non-zero entries of M_α do not overlap. This implies that $c_\alpha = 0$ for all $\alpha \in R_3^0$, and the proof is complete.

7.3 Proof of Theorem 2.15

We first note that, similar to the case of $\mathfrak{f}_{n,c}$, one can define the *reduced commutator matrix* of $\mathfrak{m}_{n,c}$ and prove the same result as Proposition 7.4. Let us now turn to the Lie algebra $\mathfrak{m}_{2,c}$ generated by x_1 and x_2. Note that since $\mathfrak{m}_{2,c}$ is metabelian, the only elements of the Hall basis whose images in $\mathfrak{m}_{2,c}$ are non-zero are of the form

$$[x_{i_k}, [x_{i_{k-1}}, \dots, [x_{i_1}, x_2] \cdots]], \tag{36}$$

where $k \leqslant c-1$ and $1 = i_1 \leqslant i_2 \leqslant \cdots \leqslant i_k \leqslant 2$. Moreover, the images in $\mathfrak{m}_{2,c}$ of the words in (36) with $k = c-1$ form a basis of the centre of $\mathfrak{m}_{2,c}$. Write y_ℓ^k for the image in $\mathfrak{m}_{2,c}$ of the unique element of the Hall basis of the form (36) of length k in which the generator x_2 occurs ℓ times. For instance, $y_1^3 = [x_1, [x_1, x_2]]$ and $y_2^3 = [x_2, [x_1, x_2]]$. Then the image of $\{y_1^c, \dots, y_{c-1}^c\}$ is a basis of $\mathfrak{m}_{2,c}^c = \mathrm{Z}(\mathfrak{m}_{2,c})$ and the image of $\{y_1^{c-1}, \dots, y_{c-2}^{c-1}, y_1^c, \dots, y_{c-1}^c\}$ is a basis of $\mathfrak{m}_{2,c}^{c-1}$. The fact that $\mathfrak{m}_{2,c}$ is metabelian implies that

$$y_\ell^{k+1} = [x_1, y_\ell^k], \quad y_{\ell+1}^{k+1} = [x_2, y_\ell^k]. \tag{37}$$

Thus the reduced commutator matrix of $\mathfrak{m}_{2,c}$ is of the form

$$\begin{pmatrix} 0 & F \\ -F^{\mathrm{tr}} & 0 \end{pmatrix},$$

where F is a $2 \times (c-2)$ matrix of the form

$$F(T_1, \dots, T_{c-1}) = \begin{pmatrix} T_1 & T_2 & \cdots & T_{c-2} \\ T_2 & T_3 & \cdots & T_{c-1} \end{pmatrix}.$$

Note that $\mathrm{rk}_{\mathbb{F}_q}(F(\mathbf{a})) \geqslant 1$ for every non-zero vector $\mathbf{a} \in \mathbb{F}_q^{c-1}$, and the matrix $F(T_1, \dots, T_{c-1})$ has rank 1 if we set $T_i = \lambda^{i-1}$, where $\lambda \in \mathbb{F}_q$. Since $q \geqslant p > c$, we can find at least $c-1$ distinct elements $\lambda_1, \dots, \lambda_{c-1}$ in $\mathbb{F}_q$. Consider the $(c-1) \times (c-1)$ matrix with the ith row given by

$$(T_1, \dots, T_{c-1}) = (1, \lambda_i, \dots, \lambda_i^{c-2}).$$

This is the well-known Vandermonde matrix, whose determinant is non-zero. Similar to the proof of Proposition 7.4, the claim follows from Theorem 5.3.

Remark 7.6. In the above proof, the issue of finding $c-1$ matrices of rank equal to 1 is intimately related to finding points in general position on the rational normal curve obtained as the image of the Veronese map given by

$$\nu_{c-2} : \mathbf{P}^1(\mathbb{F}_q) \to \mathbf{P}^{c-2}(\mathbb{F}_q), \quad [X_0 : X_1] \mapsto [X_0^{c-2} : X_0^{c-3}X_1 : \cdots : X_1^{c-2}].$$

It is likely that in the cases corresponding to $\mathfrak{m}_{n,c}$ (for $n > 2$) and $\mathfrak{f}_{n,c}$ (for $n \geqslant 2$ and $c > 3$), the faithful dimension can be computed using tools from algebraic geometry.

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

7.4 Outline of the argument for Remark 2.14

We will only consider the case $c = 6$, since the other cases are similar (and the calculations are a bit simpler). For $\mathfrak{f} := \mathfrak{f}_{2,6}$, the reduced commutator matrix is a block matrix of the form

$$F(x_1, \dots, x_9) = \begin{pmatrix} 0 & 0 & 0 & 0 & F_{1,5} \\ 0 & 0 & 0 & F_{2,4} & 0 \\ 0 & 0 & F_{3,3} & 0 & 0 \\ 0 & -F_{2,4}^{\mathrm{tr}} & 0 & 0 & 0 \\ -F_{1,5}^{\mathrm{tr}} & 0 & 0 & 0 & 0 \end{pmatrix},$$

where

$$\begin{aligned} F_{1,5}(x_1, \dots, x_9) &= \begin{pmatrix} x_1 & x_2 + x_6 & x_3 + 2x_7 - x_9 & x_4 + 2x_8 & x_6 & x_7 + x_9 \\ x_2 & x_3 & x_4 & x_5 & x_7 - x_9 & x_8 \end{pmatrix}, \\ F_{2,4}(x_1, \dots, x_9) &= \begin{pmatrix} x_6 & x_7 & x_8 \end{pmatrix}, \\ F_{3,3}(x_1, \dots, x_9) &= \begin{pmatrix} 0 & x_9 \\ -x_9 & 0 \end{pmatrix}. \end{aligned} \tag{38}$$

For $p \geqslant 7$, Proposition 7.4 implies that

$$m_{\mathrm{faithful}}(\mathscr{G}_p) = \min \left\{ \sum_{\ell=1}^{9} p^{\mathrm{rk}_{\mathbb{F}_p}(F(a_{\ell 1}, \dots, a_{\ell 9}))/2} : \begin{pmatrix} a_{11} & \cdots & a_{19} \\ \vdots & \ddots & \vdots \\ a_{91} & \cdots & a_{99} \end{pmatrix} \in \mathrm{GL}_9(\mathbb{F}_p) \right\}. \tag{39}$$

We can easily verify that $\mathrm{rk}_{\mathbb{F}_p}(F_{1,5}(\mathbf{x})) \geqslant 1$ when $0 \neq \mathbf{x} := (x_1, \dots, x_9) \in \mathbb{F}_p^9$. Also,

$$\mathrm{rk}_{\mathbb{F}_p}(F(x_1, \dots, x_9)) \geqslant 4$$

whenever at least one of x_6, x_7 or x_8 is not zero. Similarly, $\mathrm{rk}_{\mathbb{F}_p}(F(x_1, \dots, x_9)) \geqslant 6$ whenever $x_9 \neq 0$.

Now let $\mathbf{x}_i := (x_{i1}, \dots, x_{i9}) \in \mathbb{F}_p^9$, $1 \leqslant i \leqslant 9$, be 9 vectors with $\det(x_{ij}) \neq 0$. Thus after permuting the indices of the $\mathbf{x}_i$, we can assume that all of the diagonal entries x_{ii}, $1 \leqslant i \leqslant 9$, are non-zero. Hence, from (39) and the above discussion we deduce that the faithful dimension of $\mathscr{G}_p$ is at least $p^3 + 3p^2 + 5p$. This dimension can be realized by the rows of following matrix:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & \lambda_1 & \lambda_1^2 & \lambda_1^3 & \lambda_1^4 & 0 & 0 & 0 & 0 \\ 1 & \lambda_2 & \lambda_2^2 & \lambda_2^3 & \lambda_2^4 & 0 & 0 & 0 & 0 \\ 1 & \lambda_3 & \lambda_3^2 & \lambda_3^3 & \lambda_3^4 & 0 & 0 & 0 & 0 \\ 1 & \lambda_4 & \lambda_4^2 & \lambda_4^3 & \lambda_4^4 & 0 & 0 & 0 & 0 \\ 0 & 0 & \mu_1 & 3\mu_1^2 & 5\mu_1^3 & 1 & \mu_1 & \mu_1^2 & 0 \\ 0 & 0 & \mu_2 & 3\mu_2^2 & 5\mu_2^3 & 1 & \mu_2 & \mu_2^2 & 0 \\ 0 & 0 & \mu_3 & 3\mu_3^2 & 5\mu_3^3 & 1 & \mu_3 & \mu_3^2 & 0 \\ 0 & 0 & 0 & \eta & 5\eta^2 & 0 & 1 & 2\eta & 1 \end{pmatrix} \in \mathrm{GL}_9(\mathbb{F}_p),$$

where the λ_i and the μ_i are distinct elements of $\mathbb{F}_p$.

https://doi.org/10.1112/S0010437X19007462 Published online by Cambridge University Press

Acknowledgements

We would like to thank Martin Bays, Emmanuel Breuillard, Tim Clausen, Jamshid Derakhshan, Martin Hils, Alan Huckleberry, Franziska Jahnke, Aleksandra Kwiatkowska, Gunter Malle, Katrin Tent and Pierre Touchard for several useful discussions. Eamonn O'Brien and Christopher Voll brought a mistaken entry in Table 1 to our attention. We thank Christopher Voll for many useful comments. The authors would like to thank the referee for carefully reading the manuscript and for providing numerous suggestions that substantially improved both the content and the exposition of the paper.

References

AKOV13 N. Avni, B. Klopsch, U. Onn and C. Voll, *Representation zeta functions of compact p-adic analytic groups and arithmetic groups*, Duke Math. J. **162** (2013), 111–197.

Ax67 J. Ax, *Solving diophantine problems modulo every prime*, Ann. of Math. (2) **85** (1967), 161–183.

BMS16 M. Bardestani, K. Mallahi-Karai and H. Salmasian, *Minimal dimension of faithful representations for p-groups*, J. Group Theory **19** (2016), 589–608.

BF13 G. Berhuy and G. Favi, *Essential dimension: a functorial point of view (after A. Merkurjev)*, Doc. Math. **8** (2013), 279–330.

Bol86 B. Bollobás, *Combinatorics: set systems, hypergraphs, families of vectors and combinatorial probability* (Cambridge University Press, Cambridge, 1986).

BI04 N. Boston and I. M. Isaacs, *Class numbers of p-groups of a given order*, J. Algebra **279** (2004), 810–819.

Bou98 N. Bourbaki, *Lie groups and Lie algebras, Chapters 1–3* (Springer, Berlin, 1998); reprint of the 1989 English translation.

BS08 M. Boyarchenko and M. Sabitova, *The orbit method for profinite groups and a p-adic analogue of Brown's theorem*, Israel J. Math. **165** (2008), 67–91.

BR97 J. Buhler and Z. Reichstein, *On the essential dimension of a finite group*, Compositio Math. **106** (1997), 159–179.

Cox13 D. A. Cox, *Primes of the form x^2+ny^2: Fermat, class field theory, and complex multiplication*, Pure and Applied Mathematics, second edition (John Wiley, Hoboken, NJ, 2013).

Fla89 D. E. Flath, *Introduction to number theory* (Wiley-Interscience, New York, NY, 1989).

GS84 F. Grunewald and D. Segal, *Reflections on the classification of torsion-free nilpotent groups*, in *Group theory* (Academic Press, London, 1984), 121–158.

Hor55 A. Horn, *A characterization of unions of linearly independent sets*, J. Lond. Math. Soc. (2) **30** (1955), 494–496.

How77a R. E. Howe, *Kirillov theory for compact p-adic groups*, Pacific J. Math. **73** (1977), 365–381.

How77b R. E. Howe, *On representations of discrete, finitely generated, torsion-free, nilpotent groups*, Pacific J. Math. **73** (1977), 281–305.

Jac85 N. Jacobson, *Basic algebra. I*, second edition (W. H. Freeman, New York, NY, 1985).

Jai06 A. Jaikin-Zapirain, *Zeta function of representations of compact p-adic analytic groups*, J. Amer. Math. Soc. **19** (2006), 91–118.

KM08 N. A. Karpenko and A. S. Merkurjev, *Essential dimension of finite p-groups*, Invent. Math. **172** (2008), 491–508.

Kaz77 D. Kazhdan, *Proof of Springer's hypothesis*, Israel J. Math. **28** (1977), 272–286.

Khu88 E. I. Khukhro, *p-automorphisms of finite p-groups*, London Mathematical Society Lecture Note Series, vol. 246 (Cambridge University Press, Cambridge, 1998).

Kir62 A. A. Kirillov, *Unitary representations of nilpotent Lie groups*, Uspekhi Mat. Nauk **17** (1962), 57–110.

Kus67 T. Kusaba, *Remarque sur la distribution des nombres premiers*, C. R. Acad. Sci. Paris Sér. A **265** (1967), 405–407.

Lag83 J. C. Lagarias, *Sets of primes determined by systems of polynomial congruences*, Illinois J. Math. **27** (1983), 224–239.

Lee16 S. Lee, *A class of descendant p-groups of order p^9 and Higman's PORC conjecture*, J. Algebra **468** (2016), 440–447.

Mer17 A. S. Merkurjev, *Essential dimension*, Bull. Amer. Math. Soc. (N.S.) **54** (2017), 635–661.

MR10 A. Meyer and Z. Reichstein, *Some consequences of the Karpenko–Merkurjev theorem*, Doc. Math. Extra vol., Andrei A. Suslin sixtieth birthday (2010), 445–457.

MVdP95 G. Myerson and A. J. van der Poorten, *Some problems concerning recurrence sequences*, Amer. Math. Monthly **102** (1995), 698–705.

Neu99 J. Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322 (Springer, Berlin, 1999); translation of 1992 German original.

O'BV15 E. A. O'Brien and C. Voll, *Enumerating classes and characters of p-groups*, Trans. Amer. Math. Soc. **367** (2015), 7775–7796.

Sch76 W. M. Schmidt, *Equations over finite fields. An elementary approach*, Lecture Notes in Mathematics, vol. 536 (Springer, New York, NY, 1976).

Ser03 J.-P. Serre, *On a theorem of Jordan*, Bull. Amer. Math. Soc. (N.S.) **40** (2003), 429–440.

Ser06 J.-P. Serre, *Lie algebras and Lie groups*, Lecture Notes in Mathematics, vol. 1500, corrected fifth printing of second (1992) edition (Springer, Berlin, 2006).

Ser12 J.-P. Serre, *Lectures on $N_X(p)$*, Chapman & Hall/CRC Research Notes in Mathematics, vol. 11 (CRC Press, Boca Raton, FL, 2012).

SV14 A. Stasinski and C. Voll, *Representation zeta functions of nilpotent groups and generating functions for Weyl groups of type B*, Amer. J. Math. **136** (2014), 501–550.

VdDri91 L. van den Dries, *A remark on Ax's theorem on solvability modulo primes*, Math. Z. **208** (1991), 65–70.

Vol05 C. Voll, *Functional equations for local normal zeta functions of nilpotent groups*, Geom. Funct. Anal. **15** (2005), 274–295.

Vol04 C. Voll, *Zeta functions of groups and enumeration in Bruhat–Tits buildings*, Amer. J. Math. **126** (2004), 1005–1032.

Mohammad Bardestani mohammad.bardestani@gmail.com
DPMMS, Centre for Mathematical Sciences,
Wilberforce Road, Cambridge CB3 0WB, UK

Keivan Mallahi-Karai k.mallahikarai@jacobs-university.de
Jacobs University Bremen, Campus Ring I,
28759 Bremen, Germany

Hadi Salmasian hadi.salmasian@uottawa.ca
Department of Mathematics, University of Ottawa, 585 King Edward,
Ottawa, ON K1N 6N5, Canada