POLYNOMIALITY OF THE FAITHFUL DIMENSION FOR NILPOTENT GROUPS OVER FINITE TRUNCATED VALUATION RINGS

MOHAMMAD BARDESTANI, KEIVAN MALLAHI-KARAI, DZMITRY RUMIANTSAU, AND HADI SALMASIAN

ABSTRACT. Given a finite group G, the *faithful dimension* of G over $\mathbb{C}$, denoted by $m_{\mathrm{faithful}}(\mathrm{G})$, is the smallest integer n such that G can be embedded in $\mathrm{GL}_n(\mathbb{C})$. Continuing the work initiated in [BMKS19], we address the problem of determining the faithful dimension of a finite p-group of the form $\mathscr{G}_R := \exp(\mathfrak{g}_R)$ associated to $\mathfrak{g}_R := \mathfrak{g} \otimes_{\mathbb{Z}} R$ in the Lazard correspondence, where $\mathfrak{g}$ is a nilpotent $\mathbb{Z}$-Lie algebra and R ranges over finite truncated valuation rings.

Our first main result is that if R is a finite field with p^f elements and p is sufficiently large, then $m_{\mathrm{faithful}}(\mathscr{G}_R) = fg(p^f)$ where $g(T)$ belongs to a finite list of polynomials $g_1, \dots, g_k$, with non-negative integer coefficients. The latter list of polynomials is uniquely determined by the Lie algebra $\mathfrak{g}$. Furthermore, for each $1 \leq i \leq k$ the set of pairs (p, f) for which $g = g_i$ is a finite union of Cartesian products $\mathscr{P} \times \mathscr{F}$, where $\mathscr{P}$ is a Frobenius set of prime numbers and $\mathscr{F}$ is a subset of $\mathbb{N}$ that belongs to the Boolean algebra generated by arithmetic progressions. Previously, existence of such a polynomial-type formula for $m_{\mathrm{faithful}}(\mathscr{G}_R)$ was only established under the assumption that either $f = 1$ or p is fixed.

Next we formulate a conjectural polynomiality property for the value of $m_{\mathrm{faithful}}(\mathscr{G}_R)$ in the more general setting where R is a finite truncated valuation ring, and prove special cases of this conjecture. In particular, we show that for a vast class of Lie algebras $\mathfrak{g}$ that are defined by partial orders, $m_{\mathrm{faithful}}(\mathscr{G}_R)$ is given by a single polynomial-type formula.

Finally, we compute $m_{\mathrm{faithful}}(\mathscr{G}_R)$ precisely in the case where $\mathfrak{g}$ is the free metabelian nilpotent Lie algebra of class c on n generators and R is a finite truncated valuation ring.

1. INTRODUCTION

The *faithful dimension* of a finite group G over $\mathbb{C}$ is the smallest possible dimension of a faithful complex representation of G. Throughout this paper we denote the faithful dimension of G by $m_{\mathrm{faithful}}(\mathrm{G})$. It is known that $\mathrm{ed}_{\mathbb{C}}(\mathrm{G}) \leq m_{\mathrm{faithful}}(\mathrm{G})$ for a finite group G (see [BF03, Proposition 4.15]), where $\mathrm{ed}_{\mathbb{K}}(\mathrm{G})$ denotes the essential dimension of G over a field $\mathbb{K}$ as defined by Buhler and Reichstein [BR97]. It follows from a theorem of Karpenko and Merkurjev [KM08] that equality holds for all finite p-groups (see also [Mer17]).

The current work is a continuation of [BMKS19] in which the question of determining the faithful dimension was systematically studied for finite p-groups associated to $\mathbb{Z}$-Lie algebras via the *Lazard correspondence*. Let $\mathfrak{f}$ be a finite $\mathbb{Z}$-Lie algebra which is nilpotent and has cardinality p^k for a prime number p that is strictly larger than the nilpotency class of $\mathfrak{f}$. Then to $\mathfrak{f}$ we can associate a finite p-group with underlying set $\mathfrak{f}$ and with group multiplication defined by the Baker-Campbell-Hausdorff formula, that is

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

for $x, y \in \mathfrak{f}$. By a result of Lazard [Khu98, Chapter 9] every finite p-group of nilpotency class strictly smaller than p is obtained in this way from a unique Lie algebra $\mathfrak{f}$. It is natural to denote this p-group by $\exp(\mathfrak{f})$.

A general class of examples of the above construction can be given as follows. Let $\mathfrak{g}$ be a nilpotent $\mathbb{Z}$-Lie algebra that is finitely generated as an abelian group, and let R be a finite commutative unital ring of cardinality p^k where p is a prime number strictly larger than the nilpotency class of $\mathfrak{g}$. Then the above construction yields a finite p-group $\mathscr{G}_R := \exp(\mathfrak{g}_R)$ where $\mathfrak{g}_R := \mathfrak{g} \otimes_{\mathbb{Z}} R$. For example, for $p \geq n \geq 2$ the group of $n \times n$ unitriangular matrices over R is obtained in this fashion from the Lie algebra of $n \times n$ strictly upper triangular matrices over R (which has nilpotency class $n-1$).

Let $\mathbb{F}_q$ denote a finite field of order $q := p^f$. A central result of our previous work [BMKS19] is about the dependence of $m_{\text{faithful}}(\mathscr{G}_{\mathbb{F}_q})$ on p and f. More precisely, we proved the following two assertions (see Theorems 2.5 and 2.7 of [BMKS19]):

(A) There exist finitely many polynomials $g_1, \ldots, g_k$ with non-negative integer coefficients such that for every prime p we have $m_{\text{faithful}}(\mathscr{G}_{\mathbb{F}_p}) = g(p)$ where $g = g_i$ for some $1 \leq i \leq k$. The set of p for which $g = g_i$ is definable in terms of existence of solutions of polynomial systems modulo p.

(B) Given any sufficiently large prime p, there exist finitely many polynomials $g_1, \ldots, g_k$, depending only on $\mathfrak{g}$ and on p, such that for every $q := p^f$ with $f \in \mathbb{N}$ we have $m_{\text{faithful}}(\mathscr{G}_{\mathbb{F}_q}) = fg(q)$ where $g = g_i$ for some $1 \leq i \leq k$. The set of $f \in \mathbb{N}$ for which $g = g_i$ is a finite union of arithmetic progressions.

In statement A only p varies, while in statement B only f varies and it is not clear how the g_i depend on p. Statements A and B suggest that $m_{\text{faithful}}(\mathscr{G}_{\mathbb{F}_q})$ should possess a stronger polynomiality-type property, where both p and f are allowed to vary simultaneously. We did not succeed in proving a unifying assertion in [BMKS19] (see Remark 2.8 of the latter reference).

The first major result of the present paper (Theorem 1.1) proves such a unifying assertion. For a polynomial $g(T) \in \mathbb{Z}[T]$, we denote the set of primes p for which the congruence $g(T) \equiv 0 \pmod{p}$ has a solution by V_g. We call a set of prime numbers a *Frobenius set* if it is in the Boolean algebra generated by the sets V_g. The Frobenius sets are closely related to Serre's Frobenian sets (see [BMKS19] or [Lag83] for a precise statement). Henceforth, by an arithmetic progression in $\mathbb{N}$ we mean a subset of $\mathbb{N}$ of the form $\{a + kb : k \in \mathbb{Z}^{\geq 0}\}$ where $a \in \mathbb{N}$ and $b \in \mathbb{Z}^{\geq 0}$.

Theorem 1.1. *Let $\mathfrak{g}$ be a nilpotent $\mathbb{Z}$-Lie algebra which is finitely generated as an abelian group. Then there exist*

(a) *a constant $M = M(\mathfrak{g})$ only depending on $\mathfrak{g}$,*
(b) *a partition $\{\mathscr{P}_1, \ldots, \mathscr{P}_r\}$ of the set of primes larger than M into Frobenius sets,*
(c) *a partition $\{\mathscr{F}_1, \ldots, \mathscr{F}_s\}$ of natural numbers into arithmetic progressions, and*
(d) *polynomials $g_{ij}(T)$, for $1 \leq i \leq r$ and $1 \leq j \leq s$, with non-negative integer coefficients,*

such that for all $q := p^f$ where $(p, f) \in \mathscr{P}_i \times \mathscr{F}_j$ for some $1 \leq i \leq r$ and $1 \leq j \leq s$, we have

$$m_{\text{faithful}}(\mathscr{G}_{\mathbb{F}_q}) = fg_{ij}(q).$$

We remark that the groups $\mathscr{G}_{\mathbb{F}_q}$ have exponent p, so that by a result of Brauer $\mathbb{Q}(e^{2\pi i/p})$ is a splitting field of $\mathscr{G}_{\mathbb{F}_q}$. It follows from [KM08] that $\mathrm{ed}_{\mathbb{K}}(\mathscr{G}_{\mathbb{F}_q}) = m_{\text{faithful}}(\mathscr{G}_{\mathbb{F}_q})$ for every field $\mathbb{K}$ that contains $\mathbb{Q}(e^{2\pi i/p})$.

A natural extension of the class of p-groups $\mathscr{G}_{\mathbb{F}_q}$ is the groups $\mathscr{G}_R$ with $R \cong \mathcal{O}/\mathfrak{p}^d$, where $\mathcal{O}$ is the valuation ring of a local field and $\mathfrak{p}$ is the prime ideal of $\mathcal{O}$. Up to isomorphism, every finite local ring with a nilpotent and principal maximal ideal is of the form $\mathcal{O}/\mathfrak{p}^d$ (see [Del84, McL73]). Such rings are called *finite truncated valuation rings*.

Let R be a finite truncated valuation ring with maximal ideal $\mathfrak{m}$. We use $d = d_R$ to denote the smallest positive integer satisfying $\mathfrak{m}^d = 0$. If $p = p_R := \mathrm{char}(R/\mathfrak{m})$, then $pR = \mathfrak{m}^e$ for some $e = e_R \geq 1$ and $\mathcal{O}/\mathfrak{m} \cong \mathbb{F}_{p^f}$ for some $f = f_R \geq 1$. Henceforth we refer to the quadruple (d, p, e, f) as the *associated parameters* of R. It turns out that we can formulate the problem (and our results) only in terms of (d, p, e, f), even though these parameters do not identify R uniquely up to isomorphism. We conjecture the following extension of Theorem 1.1 for $m_{\text{faithful}}(\mathscr{G}_R)$.

Conjecture 1.2. *Let $\mathfrak{g}$ be as in Theorem 1.1. Then the constant $M(\mathfrak{g})$, the partitions $\{\mathscr{P}_1, \dots, \mathscr{P}_r\}$ and $\{\mathscr{F}_1, \dots, \mathscr{F}_s\}$, and the polynomials $g_{ij}(T)$ can be chosen such that for every finite truncated valuation ring R with associated parameters (d, p, e, f) we have*

$$m_{\text{faithful}}(\mathscr{G}_R) = f \sum_{\ell=0}^{e-1} g_{ij}(p^{f(d-\ell)}) \quad \textit{whenever } (p, f) \in \mathscr{P}_i \times \mathscr{F}_j.$$

We are unable to prove Conjecture 1.2 in full generality, but we establish two results that support this conjecture. The first result, Theorem 1.3, shows that $m_{\text{faithful}}(\mathscr{G}_R)$ is not greater than the conjectural value, but grows with the same rate as d tends to infinity.

Theorem 1.3. *Let $\mathfrak{g}$, $\{\mathscr{P}_i\}_{i=1}^r$, $\{\mathscr{F}_i\}_{i=1}^s$, and the $g_{ij}(T)$ be as in Theorem 1.1. Fix $1 \leq i_\circ \leq r$ and $1 \leq j_\circ \leq s$. Then there exists a constant $M > 0$ such that for every finite truncated valuation ring R with associated parameters (d, p, e, f) satisfying $(p, f) \in \mathscr{P}_{i_\circ} \times \mathscr{F}_{j_\circ}$ and $p > M$, we have*

$$f g_{i_\circ j_\circ}(p^{fd}) \leq m_{\text{faithful}}(\mathscr{G}_R) \leq f \sum_{\ell=0}^{e-1} g_{i_\circ j_\circ}(p^{f(d-\ell)}).$$

Remark 1.4. Note that the above theorem establishes Conjecture 1.2 in the case $e = 1$. In this case, the rings R are of the form $\mathcal{O}/\mathfrak{p}^d$ where $\mathcal{O}$ is the ring of integers of a finite unramified extension of $\mathbb{Q}_p$.

The second result, Theorem 1.5, establishes the conjecture for groups associated to *pattern Lie algebras*. Before stating Theorem 1.5 we recall some definitions. Let $\prec$ be a partial order on the set $[n] := \{1, 2, \dots, n\}$. To this partial order, we assign the $\mathbb{Z}$-Lie subalgebra $\mathfrak{g}_\prec$ of $\mathfrak{gl}(n, \mathbb{Z})$ that is spanned by the e_{ij} satisfying $i \prec j$, where the e_{ij} denote the standard basis vectors of $\mathfrak{gl}(n, \mathbb{Z})$. Many nilpotent Lie algebras of interest (e.g., nilradicals of parabolic subalgebras of semisimple Lie algebras) are pattern Lie algebras.

Without loss of generality we assume that $\prec$ is compatible with the usual ordering of $[n]$, so that elements of $\mathfrak{g}_\prec$ are strictly upper triangular matrices. For any $i \prec j$ define

$$\alpha(i, j) := \#\{k \in [n] : i \prec k \prec j\}. \tag{1.1}$$

A pair (i, j) with $i \prec j$ is called *extreme* if i is minimal and j is maximal with respect to $\prec$. The set of extreme pairs will be denoted by I_{ex}.

Theorem 1.5. *Let $\mathfrak{g} := \mathfrak{g}_\prec$ with $\mathfrak{g}_\prec$ as above, and let R be a finite truncated valuation ring with associated parameters (d, p, e, f) such that*

$$p > \max\{\alpha(i,j) : i \prec j\} + 1.$$

Then

$$m_{\text{faithful}}(\mathscr{G}_R) = \sum_{\ell=0}^{e-1} \sum_{(i,j)\in I_{\text{ex}}} fp^{f(d-\ell)\alpha(i,j)}. \tag{1.2}$$

Special cases of Theorem 1.5 were proved in [BMKS19] (for $R = \mathbb{F}_q$) and [BMKS16] (for Heisenberg and unitriangular groups over general R). The Heisenberg Lie algebra (which is the nilradical of the parabolic subalgebra of $\mathfrak{gl}_n$ with Levi factor $\mathfrak{gl}_1 \oplus \mathfrak{gl}_{n-2} \oplus \mathfrak{gl}_1$) corresponds to the partial order

$$1 \prec 2, 3, \ldots, n-1 \prec n,$$

and the unitriangular Lie algebra corresponds to the total order $1 \prec \cdots \prec n$.

We conclude this paper by computing $m_{\text{faithful}}(\mathscr{G}_R)$ when $\mathfrak{g} \cong \mathfrak{m}_{n,c}$, where $\mathfrak{m}_{n,c}$ is the free metabelian nilpotent Lie algebra of class c on n generators. Recall that

$$\mathfrak{m}_{n,c} := \mathfrak{f}_{n,c}/[[\mathfrak{f}_{n,c}, \mathfrak{f}_{n,c}], [\mathfrak{f}_{n,c}, \mathfrak{f}_{n,c}]],$$

where $\mathfrak{f}_{n,c}$ denotes the free nilpotent $\mathbb{Z}$-Lie algebra of class c on n generators. Indeed $\mathfrak{m}_{n,c}$ is the largest metabelian quotient of $\mathfrak{f}_{n,c}$. The following theorem is a generalization of [BMKS16, Theorem 2.15], which corresponds to the special case $\mathfrak{m}_{2,c}$. Special cases of $\mathfrak{m}_{3,5}, \mathfrak{m}_{3,6}$ and $\mathfrak{m}_{n,4}$ for all $n \geq 2$ over finite fields were computed by Tielker [Tie18].

Theorem 1.6. *Set $\mathfrak{g} := \mathfrak{m}_{n,c}$ where $n, c \geq 2$. Then for p sufficiently large we have*

$$m_{\text{faithful}}(\mathscr{G}_R) = (c-1)\binom{n+c-2}{c} \sum_{\ell=0}^{e-1} fp^{f(d-\ell)}.$$

Let us now explain the key ideas that are used in the present paper. Similar to our previous work [BMKS19], we heavily use the Kirillov orbit method for finite p-groups, as well as the notion of the commutator matrix associated to a nilpotent Lie algebra, defined originally by Grunewald and Segal [GS84]. Another important tool is a theorem from [BMKS19] which relates the faithful dimension to the question of existence of rational points in general position on certain rank varieties. However, the proof of Theorem 1.1 requires two new ideas: first, a theorem of Ax from his seminal work [Ax68] (see also [vdD91]) which roughly states that any elementary statement in the language of finite fields is equivalent to one about single-variable polynomials; second, a theorem of Dedekind about factorization of the reduction modulo p of a monic polynomial with integer coefficients. In addition, in the proof of Theorem 1.3 we need a (not so well known) variant of the multivariate Hensel's lemma that does not require any smoothness or genericity assumption (see Proposition 3.4). This variant was first established by Ax and Kochen [AK65] using ultrafilter methods (for further references, see Section 3).

Acknowledgement. The authors thank Emmanuel Breuillard, Jamshid Derakhshan, Julia Gordon, Zinovy Reichstein, and Christopher Voll for stimulating conversations, and the anonymous referees for reading the paper carefully. The research of Hadi Salmasian was partially supported by an NSERC Discovery Grant (RGPIN-2018-04044).

2. Polynomiality along all finite fields

In this section we will prove Theorem 1.1. We begin with recalling a result of Ax from model theory of finite fields. Let $\mathcal{Q} := \{p^f : p \text{ is prime and } f \in \mathbb{N}\}$ be the set of all prime powers. For $n \geq 1$, denote by $\mathcal{B}_n$ the Boolean algebra on $\mathcal{Q}$ generated by the subsets

$$Z_{h_1,\dots,h_k} := \{q \in \mathcal{Q} : \text{ the equations } h_i(T_1,\dots,T_n) = 0, 1 \leq i \leq k, \text{ have a solution in } \mathbb{F}_q\},$$

where $h_1,\dots,h_k$ range over all polynomials in $\mathbb{Z}[T_1,\dots,T_n]$. Also, let $\mathcal{B}$ be the Boolean algebra generated by finite subsets of $\mathcal{Q}$ and the sets Z_h where $h \in \mathbb{Z}[T_1]$. In [Ax68, Theorem 11], Ax proved that for all $n \geq 1$, we have $\mathcal{B}_n \subseteq \mathcal{B}$. This statement generalizes [Ax67, Theorem 1], which proves a similar assertion for primes. It also follows from a result of van den Dries in [vdD91, Subsec. (2.3)].

In order to prove Theorem 1.1 we need a refinement of the aforementioned result of Ax (see Proposition 2.4). This refinement may be well known to the experts in the field (see e.g. [Ax68, Theorem 11'] for a somewhat similar statement), but we were unable to locate the required formulation in the literature. For this reason and for convenience of the reader we will supply a proof. We would like to thank J. Derakhshan for communicating the main steps of this proof to us.

Let us recall some basic facts from algebraic number theory. Let $h(T) \in \mathbb{Z}[T]$ be a monic polynomial. The discriminant of $h(T)$ is defined to be

$$\mathrm{Disc}_h := \prod_{1\leq i<j\leq n} (\alpha_i - \alpha_j)^2,$$

where $\alpha_1,\dots,\alpha_n$ are the roots of $h(T)$. Note that since $h(T)$ is monic, $\mathrm{Disc}_h \in \mathbb{Z}$. We denote the splitting field of $h(T)$ by E, that is, $E := \mathbb{Q}(\alpha_1,\dots,\alpha_n)$, and the ring of algebraic integers of E by $\mathcal{O}_E$.

Let p be a prime number that does not divide Disc_h. Then p is unramified in every simple extension $\mathbb{Q}(\alpha_i)$ (see [Mar18, Theorem 3.24]), hence by [Mar18, Theorem 4.31] it is also unramified in the compositum of the $\mathbb{Q}(\alpha_i)$, that is, in E. Therefore to every prime ideal $\mathfrak{q}$ of $\mathcal{O}_E$ that lies over $p\mathbb{Z}$ (i.e., $\mathfrak{q} \cap \mathbb{Z} = p\mathbb{Z}$) one can associate a Frobenius automorphism [Mar18, Theorem 4.32], which is the unique element $\sigma_\mathfrak{q} \in \mathrm{Gal}(E/\mathbb{Q})$ that satisfies

$$\sigma_\mathfrak{q}(\alpha) \equiv \alpha^p \mod \mathfrak{q} \quad \text{for all } \alpha \in \mathcal{O}_E.$$

The $\sigma_\mathfrak{q}$ form a conjugacy class of $\mathrm{Gal}(E/\mathbb{Q})$, denoted by the Artin symbol $\left(\frac{E/\mathbb{Q}}{p}\right)$.

Denote the reduction of $h(T)$ modulo p by $\bar{h}(T)$. Since $p \nmid \mathrm{Disc}_h$, the roots of $\bar{h}(T)$ are also simple. For the proof of the next theorem, see [Jac85, Theorems 4.37 and 4.38].

Theorem 2.1 (Dedekind)**.** *Let $h(T)$ and p be as above. Suppose*

$$\bar{h}(T) = h_1(T)\cdots h_r(T) \tag{2.1}$$

is the factorization of $\bar{h}(T)$ into irreducible polynomials over $\mathbb{F}_p$. Set $n_i := \deg h_i$ for $1 \leq i \leq r$. Let $\mathfrak{q}$ be a prime ideal of $\mathcal{O}_E$ that lies over $p\mathbb{Z}$. Then the cycle decomposition of $\sigma_\mathfrak{q}$, when viewed as a permutation of the roots of $h(T)$, is of the form $\varsigma_1\cdots\varsigma_r$ with each ς_i a cycle of length n_i.

Remark 2.2. Theorem 2.1 is not stated in [Jac85] exactly in the given form. Jacobson proves (by an argument originally due to Tate) that for every prime ideal $\mathfrak{p}$ of $\mathcal{O}_h := \mathbb{Z}[\alpha_1,\dots,\alpha_n]$ that lies over $p\mathbb{Z}$, there exists a unique $\sigma_\mathfrak{p} \in \mathrm{Gal}(E/\mathbb{Q})$ such that for all $\alpha \in \mathcal{O}_h$ one has $\sigma_\mathfrak{p}(\alpha) \equiv \alpha^p \mod \mathfrak{p}$, and furthermore the restriction of $\sigma_\mathfrak{p}$ to the roots of $h(T)$ has

the desired cycle decomposition. Now if $\mathfrak{q} \subset \mathcal{O}_E$ is a prime ideal that lies over $p\mathbb{Z}$, then $\sigma_\mathfrak{q}$ also satisfies $\sigma_\mathfrak{q}(\alpha) \equiv \alpha^p \mod \mathfrak{p}$ for $\alpha \in \mathcal{O}_h$, where $\mathfrak{p} := \mathfrak{q} \cap \mathcal{O}_h$. Thus by the uniqueness of $\sigma_\mathfrak{p}$ we obtain $\sigma_\mathfrak{p} = \sigma_\mathfrak{q}$.

Lemma 2.3. *Let $h(T)$, p, $\sigma_\mathfrak{q}$, and n_i for $1 \leq i \leq r$ be as in Theorem 2.1. Denote by $S_p(h)$ the set of integers $f \geq 1$ such that $\bar{h}(T)$ has a root in $\mathbb{F}_{p^f}$. Then*

$$S_p(h) = \bigcup_{i=1}^{r} n_i\mathbb{N} = \{k \geq 1 : \mathrm{Fix}(\sigma_\mathfrak{q}^k) \neq \varnothing\},$$

where $\mathrm{Fix}(\sigma_\mathfrak{q}^k)$ is the set of fixed points of $\sigma_\mathfrak{q}^k$, viewed as a permutation of the roots of $h(T)$.

Proof. From the cycle decomposition of $\sigma_\mathfrak{q}$ in Theorem 2.1 it follows immediately that $\sigma_\mathfrak{q}^k$ has a fixed point if and only if $n_i | k$ for some $1 \leq i \leq r$. This proves the second equality. Thus it remains to verify that $S_p(h) = \bigcup_{i=1}^r n_i\mathbb{N}$.

First observe that for each $1 \leq i \leq r$, the quotient $\mathbb{F}_p[x]/(h_i(x))$ is a field of order p^{n_i} in which $\bar{h}(x)$ has a root. Recall that $k|l$ if and only if $\mathbb{F}_{p^l}$ has a subfield isomorphic to $\mathbb{F}_{p^k}$. Thus if $k \in n_i\mathbb{N}$ for some $1 \leq i \leq r$, then $\bar{h}(x)$ has a root in $\mathbb{F}_{p^k}$. This proves $S_p(h) \supseteq \bigcup_{i=1}^r n_i\mathbb{N}$. For the reverse inclusion, assume that $\bar{h}(x)$ has a root in $\mathbb{F}_{p^k}$. It follows that there exists $1 \leq i \leq r$ such that $h_i(x)$ has a root in $\mathbb{F}_{p^k}$. Call this root α. Since $h_i(x)$ is irreducible over $\mathbb{F}_p$, it follows that the subfield $\mathbb{F}_p(\alpha)$ has p^{n_i} elements. Thus $\mathbb{F}_{p^{n_i}}$ is isomorphic to a subfield of $\mathbb{F}_{p^k}$, and consequently n_i divides k. □

Define an equivalence relation $\sim$ on $\mathrm{Gal}(E/\mathbb{Q})$ by

$$\tau_1 \sim \tau_2 \text{ iff } \tau_1 = \sigma\tau_2^j\sigma^{-1} \text{ for some } \sigma \in \mathrm{Gal}(E/\mathbb{Q}),$$

where $\gcd(j, \mathrm{ord}(\tau_2)) = 1$. An equivalence class of $\sim$ is called a division, or an *Abteilung*. Following [Lag83], for any division $C \subseteq \mathrm{Gal}(E/\mathbb{Q})$ we consider the set

$$\mathscr{E}(C) := \left\{ p \ : \ \left(\frac{E/\mathbb{Q}}{p}\right) \subseteq C \right\}.$$

In the following proposition, let $S(h; M)$ for $M > 0$ and a monic polynomial $h \in \mathbb{Z}[T]$ denote the set of pairs (p, f) where $p > M$ is prime, $f \geq 1$, and the reduction modulo p of $h(T)$ has a root in $\mathbb{F}_{p^f}$.

Proposition 2.4. *Let $h(T) \in \mathbb{Z}[T]$ be monic. Then there exists $M_\circ > 0$, only depending on $h(T)$, such that $S(h; M_\circ) = \bigcup_{i=1}^r \mathcal{P}_i \times \mathcal{N}_i$ for some $r \in \mathbb{N}$, where the $\mathcal{P}_i$ and the $\mathcal{N}_i$ satisfy the following properties:*

(a) *The $\mathcal{P}_i$ form a partition of the set of primes bigger than $M_\circ$ into Frobenius sets, and*
(b) *Each $\mathcal{N}_i$ is a finite union of sets of the form $k\mathbb{N}$ for $k \in \mathbb{N}$.*

Proof. Without loss of generality we can assume that $h(T)$ is irreducible over $\mathbb{Q}$. As before let E denote the splitting field of $h(T)$. We denote the divisions of $\mathrm{Gal}(E/\mathbb{Q})$ by $C_1, \ldots, C_r$. We set $M_\circ := 1 + |\mathrm{Disc}_h|$. First we show that if $p, p' > M_\circ$ are primes such that

$$\left(\frac{E/\mathbb{Q}}{p}\right) \cup \left(\frac{E/\mathbb{Q}}{p'}\right) \subseteq C_i \text{ for some } 1 \leq i \leq r,$$

then $S_p(h) = S_{p'}(h)$. Choose $\sigma_\mathfrak{q} \in \left(\frac{E/\mathbb{Q}}{p}\right)$ and $\sigma_{\mathfrak{q}'} \in \left(\frac{E/\mathbb{Q}}{p'}\right)$. Then $\sigma_{\mathfrak{q}'} = \tau\sigma_\mathfrak{q}^j\tau^{-1}$, where $\gcd(j, \mathrm{ord}(\sigma_\mathfrak{q})) = 1$. By Lemma 2.3, if $n \in S_p(h)$ then $\mathrm{Fix}(\sigma_\mathfrak{q}^n) \neq \varnothing$, hence also $\mathrm{Fix}(\sigma_\mathfrak{q}^{nj}) \neq \varnothing$.

Since $\sigma_{\mathfrak{q}'}^n$ is conjugate to $\sigma_{\mathfrak{q}'}^{nj}$, it follows that $\mathrm{Fix}(\sigma_{\mathfrak{q}'}^n) \neq \varnothing$, so that $n \in S_{p'}(h)$. This proves $S_p(h) \subseteq S_{p'}(h)$, and by symmetry we have the reverse inclusion, hence $S_p(h) = S_{p'}(h)$.

From what we just proved it follows that $S_p(h)$ depends only on the index $1 \leq i \leq r$ for which $\left(\frac{E/\mathbb{Q}}{p}\right) \subseteq C_i$. It is shown in [Lag83, Theorem 1.1] that every set of primes that differs by only a finite set from $\mathscr{E}(C)$ for some division C is a Frobenius set.[1] Thus we can set $\mathcal{P}_i := \mathscr{E}(C_i)$ for $1 \leq i \leq r$. The existence of the $\mathcal{N}_i$ now follows from Lemma 2.3. □

Remark 2.5. Let $\mathcal{Q}_1 \subseteq \mathcal{Q}$ denote the set of prime numbers. Then $S(h, M)$ is the inverse image of $Z_h \cap \mathcal{Q}^M$, where $Q^M := \{p^f \in \mathcal{Q} : p > M\}$, under the bijection $\mathcal{Q}_1 \times \mathbb{N} \to \mathcal{Q}$ given by $(p, f) \mapsto p^f$.

For the proof of Theorem 1.1 we need one more ingredient: a result from our previous work [BMKS19] which relies on the Kirillov orbit method for finite p-groups. To state this result, we need to recall the notion of the *commutator matrix* of a nilpotent $\mathbb{Z}$-Lie algebra.

Given a finitely generated abelian group Γ, we call a subset $S \subseteq \Gamma$ 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 $\#S = \mathrm{rk}_{\mathbb{Z}}\Gamma$, where $\mathrm{rk}_{\mathbb{Z}}\Gamma$ is the rank of Γ as a $\mathbb{Z}$-module.

Now let $\mathfrak{g}$ be a nilpotent $\mathbb{Z}$-Lie algebra which is finitely generated as an abelian group. Let $\mathbf{w}_1, \ldots, \mathbf{w}_{l_1}$ be a semibasis of $\mathrm{Z}(\mathfrak{g}) \cap [\mathfrak{g}, \mathfrak{g}]$. Let $\mathbf{w}_{l_1+1}, \ldots, \mathbf{w}_m$ be elements of $\mathfrak{g}$ that represent a semibasis of $[\mathfrak{g}, \mathfrak{g}]/(\mathrm{Z}(\mathfrak{g}) \cap [\mathfrak{g}, \mathfrak{g}])$. Finally, let $\mathbf{z}_1, \ldots, \mathbf{z}_{l_2}$ be elements of $\mathfrak{g}$ that represent a semibasis of $\mathrm{Z}(\mathfrak{g})/(\mathrm{Z}(\mathfrak{g}) \cap [\mathfrak{g}, \mathfrak{g}])$. Then the vectors $\{\mathbf{w}_1, \ldots, \mathbf{w}_m, \mathbf{z}_1, \ldots, \mathbf{z}_{l_2}\}$ are $\mathbb{Z}$-linearly independent and $\mathrm{rk}_{\mathbb{Z}}(\mathrm{Z}(\mathfrak{g}) + [\mathfrak{g}, \mathfrak{g}]) = l_2 + m$.

Let $\mathbf{v}'_1, \ldots, \mathbf{v}'_n$ be elements of $\mathfrak{g}$ that represent a semibasis of $\mathfrak{g}/\mathrm{Z}(\mathfrak{g})$. For $1 \leq i < j \leq n$, there exist integers η_{ij}^k, $l_1 + 1 \leq k \leq m$, such that if we set

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

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

$$[\mathbf{v}_i, \mathbf{v}_j] - \sum_{k=1}^{m} \lambda_{ij}^k \mathbf{w}_k \in \big([\mathfrak{g}, \mathfrak{g}] \cap \mathrm{Z}(\mathfrak{g})\big)_{\mathrm{tor}} \text{ for } 1 \leq i < j \leq n.$$

We remark that $\lambda_{ij}^k = K^2 \eta_{ij}^k$ for $l_1 + 1 \leq k \leq m$. We set $\lambda_{ii}^k := 0$, and for $i > j$ we define $\lambda_{ij}^k := -\lambda_{ji}^k$. Finally, for $1 \leq i, j \leq n$ 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 $1 \leq i, j \leq n$. The *commutator matrix of* $\mathfrak{g}$ (relative to the chosen ordered basis) is the $n \times n$ skew-symmetric matrix of linear forms defined by

$$F_{\mathfrak{g}}(T_1, \ldots, T_m) := [\Lambda_{ij}(T_1, \ldots, T_m)]_{1 \leq i,j \leq n}. \tag{2.2}$$

[1] We remark that Lagarias uses different terminology. In particular, in [Lag83] our Frobenius sets are called SPC sets, the sets $\mathscr{E}(C)$ are called elementary Frobenius sets, and the sets in the Boolean algebra generated by the $\mathscr{E}(C)$ for divisions C are called Frobenius sets.

See [GS84, Vol05, Vol04, OV15, AKOV13, SV14] as other references for $F_{\mathfrak{g}}$. In the following theorem, $\mathrm{rk}_{\mathbb{F}_q}(\cdot)$ denotes the rank of a matrix with entries in the field $\mathbb{F}_q$.

For a given $\mathfrak{g}$ we set $\mathcal{SB}_{\mathfrak{g}} := (\mathbf{w}_1, \dots, \mathbf{w}_m, \mathbf{z}_1, \dots, \mathbf{z}_{l_2}, \mathbf{v}'_1, \dots, \mathbf{v}'_n)$. This $(m + l_2 + n)$-tuple of vectors is the semibasis data that uniquely determines $F_{\mathfrak{g}}$. For an isomorphism class of $\mathfrak{g}$ we can fix this semibasis data, thereby fixing the commutator matrix $F_{\mathfrak{g}}$ whenever needed.

Theorem 2.6. *Let $\mathfrak{g}$ be a nilpotent $\mathbb{Z}$-Lie algebra which is finitely generated as an abelian group. Then there exists a constant $M > 0$, depending only on $\mathfrak{g}$ and the choice of $\mathcal{SB}_{\mathfrak{g}}$, such that for every prime power $q := p^f$ with $p > M$ and $f \geq 1$ we have*

$$m_{\text{faithful}}(\mathscr{G}_q) = \min\left\{ \sum_{\ell=1}^{l_1} f q^{\frac{\mathrm{rk}_{\mathbb{F}_q}(F_{\mathfrak{g}}(x_{\ell 1}, \dots, x_{\ell m}))}{2}} : \begin{pmatrix} x_{11} & \dots & x_{1l_1} \\ \vdots & \ddots & \vdots \\ x_{l_1 1} & \dots & x_{l_1 l_1} \end{pmatrix} \in \mathrm{GL}_{l_1}(\mathbb{F}_q) \right\} + f l_2, \tag{2.3}$$

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

Proof. This is proved in [BMKS19, Theorem 5.3]. □

Remark 2.7. (a) Let $X \subseteq \mathbb{N}$ belong to the Boolean algebra generated by arithmetic progressions. Then X can be expressed as a disjoint union of arithmetic progressions (note that any singleton $\{a\} \subset \mathbb{N}$ is also considered an arithmetic progression). This can be seen as follows. Set $A_{a,b} := \{a + kb : k \in \mathbb{Z}^{\geq 0}\}$ where $a \in \mathbb{N}$ and $b \in \mathbb{Z}^{\geq 0}$. Then $A_{a,b} \cap A_{a',b'}$ is either the empty set, or a singleton, or a set of the form $A_{a'',b''}$ where b'' is the least common multiple of b and b'. Furthermore,

$$\mathbb{N} \setminus A_{a,b} = \bigcup_{1 \leq a' \neq a \leq b} A_{a',b} \cup \bigcup_{\substack{a'' \equiv a \bmod b \\ 1 \leq a'' < a}} \{a''\}.$$

Finally, by De Morgan's Law the case of $A_{a,b} \cup A_{a',b'}$ can be reduced to the cases of intersection and complement. From these observations it follows that every subset of $\mathbb{N}$ that is obtained by finite intersection, complements, and finite unions is expressible as a disjoint union of the sets $A_{a,b}$.

(b) Recall that $\mathcal{Q}_1 \subseteq \mathcal{Q}$ denotes the set of prime numbers. Suppose that $X \subseteq \mathcal{Q}_1 \times \mathbb{N}$ belongs to the Boolean algebra generated by product sets $\mathcal{P} \times \mathcal{F}$ where $\mathcal{P} \subseteq \mathcal{Q}_1$ is a Frobenius set and $\mathcal{F} \subseteq \mathbb{N}$ is in the Boolean algebra generated by arithmetic progressions. Then X can be expressed as a union of the generators $\mathcal{P} \times \mathcal{F}$. This is a consequence of part (a) and the following relations:

(i) $(\mathcal{P} \times \mathcal{F}) \cap (\mathcal{P}' \times \mathcal{F}') = (\mathcal{P} \cap \mathcal{P}') \times (\mathcal{F} \cap \mathcal{F}')$.

(ii) $(\mathcal{Q}_1 \times \mathbb{N}) \setminus (\mathcal{P} \times \mathcal{F}) = ((\mathcal{Q}_1 \setminus \mathcal{P}) \times \mathcal{F}) \cup (\mathcal{Q}_1 \times (\mathbb{N} \setminus \mathcal{F})) \cup ((\mathcal{Q}_1 \setminus \mathcal{P}) \times (\mathbb{N} \setminus \mathcal{F}))$.

Note that as in (a), the union $(\mathcal{P} \times \mathcal{F}) \cup (\mathcal{P}' \times \mathcal{F}')$ can be expressed by intersection and complement.

Lemma 2.8. *Let $\mathscr{X}$ and $\mathscr{Y}$ be two arbitrary sets, and let $\{\mathscr{Z}_i\}_{i \in \mathcal{I}}$ be a partition of $\mathscr{X} \times \mathscr{Y}$ into finitely many sets such that $\mathscr{Z}_i = \bigcup_{j=1}^{N_i} X_{i,j} \times Y_{i,j}$ for $i \in \mathcal{I}$, where $N_i \in \mathbb{N}$. Then there exist partitions $\{X_k\}_{k \in \mathcal{I}_X}$ of $\mathscr{X}$ and $\{Y_l\}_{l \in \mathcal{I}_Y}$ of $\mathscr{Y}$, where $|\mathcal{I}_X|, |\mathcal{I}_Y| < \infty$, such that the following hold.*

(a) *The X_k belong to the Boolean algebra generated by the $X_{i,j}$.*

(b) *The Y_l belong to the Boolean algebra generated by the $Y_{i,j}$.*

(c) *Each $\mathscr{Z}_i$ is a union of Cartesian product sets of the form $X_k \times Y_l$.*

Proof. Every finite Boolean algebra is isomorphic to the power set of a finite set. From this statement it follows that there exists a finite family of disjoint sets $\mathscr{F}_{\mathscr{X}} := \{X_k\}_{k\in\mathcal{I}_X}$ in the Boolean algebra generated by the $X_{i,j}$ such that each $X_{i,j}$ can be expressed as the union of elements of a subset of $\mathscr{F}_{\mathscr{X}}$. Similarly, there exists a finite family of disjoint sets $\mathscr{F}_{\mathscr{Y}} := \{Y_l\}_{l\in\mathcal{I}_Y}$ in the Boolean algebra generated by the $Y_{i,j}$ such that each $Y_{i,j}$ can be expressed as the union of elements of a subset of $\mathscr{F}_{\mathscr{Y}}$. It is clear that each $\mathscr{Z}_i$ is a union of the sets $X_k \times Y_l$. Since $\bigcup_{i\in\mathcal{I}} \mathscr{Z}_i = \mathscr{X}\times\mathscr{Y}$, we have $\bigcup_{i\in\mathcal{I}}\bigcup_{1\le j\le N_i} X_{i,j} = \mathscr{X}$ and $\bigcup_{i\in\mathcal{I}}\bigcup_{1\le j\le N_i} Y_{i,j} = \mathscr{Y}$, hence $\bigcup_{k\in\mathcal{I}_X} X_k = \mathscr{X}$ and $\bigcup_{l\in\mathcal{I}_Y} Y_k = \mathscr{Y}$. □

Proof of Theorem 1.1. Let p be a prime number and set $q := p^f$ for some $f \ge 1$. Since $F_{\mathfrak{g}}(T_1,\dots,T_m)$ is a skew-symmetric $n\times n$ matrix where $n := \mathrm{rk}_{\mathbb{Z}}(\mathfrak{g}/\mathrm{Z}(\mathfrak{g}))$, the rank of $F_{\mathfrak{g}}(x_1,\dots,x_m)$ for $x_1,\dots,x_m\in\mathbb{F}_q$ is an even number no larger than n. Let $\mathcal{M}$ be the set of all integer vectors $\mu = (a_1,\dots,a_{l_1}) \in \mathbb{Z}^{l_1}$ satisfying $0\le a_1\le\cdots\le a_{l_1}\le n/2$. To each $\mu\in\mathcal{M}$ we assign a polynomial $g_\mu(T)$ defined by

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

We order the vectors μ according to the *reverse lexicographical order* $\lhd$, defined by $\mu\lhd\mu'$ 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

$$g_\mu(q) < g_{\mu'}(q). \tag{2.4}$$

We sort elements of $\mathcal{M}$ as $\mu_1\lhd\cdots\lhd\mu_N$, where $N := \#\mathcal{M}$. For $\mu = (a_1,\dots,a_{l_1})\in\mathcal{M}$, we define an affine variety

$$\mathbf{X}_\mu := \left\{(x_{ij}) \in \mathrm{Mat}_{l_1\times m}(\mathbb{C}) : \mathrm{rk}_{\mathbb{C}} F_{\mathfrak{g}}(x_{i1},\dots,x_{im}) = 2a_i \text{ for } 1\le i\le l_1,\ \det(x_{ij})_{1\le i,j\le l_1}\neq 0\right\}.$$

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. For $\mu\in\mathcal{M}$ set

$$\Sigma_\mu := \left\{p^f \,:\, p \text{ is prime},\ p > \max\{l_1, M_1\},\ f\ge 1,\ \text{ and } \mathbf{X}_\mu(\mathbb{F}_{p^f})\neq\varnothing\right\},$$

where M_1 is the lower bound constant of Theorem 2.6. Theorem 2.6 and (2.4) imply that $m_{\text{faithful}}(\mathscr{G}_{p^f}) = f g_{\mu_k}(p^f)$ for the value of k that satisfies

$$p^f \in \mathscr{Q}_k := \Sigma_{\mu_k} \setminus \bigcup_{1\le i<k} \Sigma_{\mu_i}.$$

Recall that $\mathcal{Q}$ denotes the set of prime powers. By Ax's theorem [Ax68, Theorem 11] stated in the beginning of this section, the sets $\mathscr{Q}_k$ can be expressed in terms of unions, intersections, and complements of finitely many of the generators of the Boolean algebra $\mathcal{B}$, that is, finite subsets of $\mathcal{Q}$ and the sets Z_h for $h(T)\in\mathbb{Z}[T]$. Recall that for $M>0$ we set

$$\mathcal{Q}^M := \{p^f\in\mathcal{Q} \,:\, p > M\}.$$

For a non-constant polynomial $h(T)\in\mathbb{Z}[T]$, there exists a monic polynomial $h_1(T)\in\mathbb{Z}[x]$ and a constant $M_h>0$ such that $Z_h\cap\mathcal{Q}^{M_h} = Z_{h_1}\cap\mathcal{Q}^{M_h}$ (we obtain h_1 from h by a suitable change of variable $T\mapsto T/T_0$ and then clearing the denominators, so that it suffices to choose $M_h > |T_0|$). It follows that for M' sufficiently large, the sets $\mathscr{Q}_k\cap\mathcal{Q}^{M'}$ are in the Boolean algebra of subsets of $\mathcal{Q}^{M'}$ that is generated by the sets $Z_h\cap\mathcal{Q}^{M'}$ for monic $h(T)\in\mathbb{Z}[T]$. Proposition 2.4, Remark 2.5 and Remark 2.7(b) imply that there exists a constant $M(\mathfrak{g})$ such that each of the sets $\tilde{\mathscr{Q}}_k := \left\{(p,f) \,:\, p^f\in\mathscr{Q}_k \text{ and } p > M(\mathfrak{g})\right\}$ for

$1 \leq k \leq N$ is a finite union of Cartesian products $\mathcal{P} \times \mathcal{N}$ where $\mathcal{P}$ is a Frobenius set and $\mathcal{N}$ is an arithmetic progression. The existence of the desired partitions $\mathscr{P}_1, \ldots, \mathscr{P}_r$ and $\mathscr{F}_1, \ldots, \mathscr{F}_s$ now follows from Lemma 2.8 where we set $\mathscr{X} := \mathcal{Q}^{M(\mathfrak{g})}$, $\mathscr{Y} := \mathbb{N}$, and $\mathscr{Z}_k := \tilde{\mathscr{D}}_k$ for $1 \leq k \leq N$. □

The proof of Theorem 1.1 has the following consequence, which we will need when considering $m_{\text{faithful}}(\mathscr{G}_R)$ for finite truncated valuation rings R.

Corollary 2.9. *Let $\mathfrak{g}$, $\{\mathscr{P}_i\}_{i=1}^r$, $\{\mathscr{F}_i\}_{i=1}^s$, and the $g_{ij}(T)$ be as in Theorem 1.1. Fix $1 \leq i_\circ \leq r$ and $1 \leq j_\circ \leq s$. Set $\mathscr{P} := \mathscr{P}_{i_\circ}$, $\mathscr{F} := \mathscr{F}_{j_\circ}$, and $g(T) := g_{i_\circ j_\circ}(T)$. Then $g(T) = l_2 + \hat{g}(T)$, where $\hat{g}(T) \in \mathbb{Z}[T]$, such that the following statements hold.*

(a) *$\hat{g}(T) = \sum_{i=0}^{\deg(\hat{g})} \hat{g}_i T^i$ where the $\hat{g}_i$ are non-negative integers and $\sum_{i=0}^{\deg(\hat{g})} \hat{g}_i = l_1$.*

(b) *For any $q := p^f$ where $(p, f) \in \mathscr{P} \times \mathscr{F}$, there exist l_1 vectors $\mathbf{a}_i \in \mathbb{F}_q^{\oplus m}$, $1 \leq i \leq l_1$, such that their projections on the first l_1 components form an $\mathbb{F}_q$-basis of $\mathbb{F}_q^{\oplus l_1}$ and*

$$\#\left\{i \,:\, 1 \leq i \leq l_1 \text{ and } \mathrm{rk}_{\mathbb{F}_q}(F_{\mathfrak{g}}(\mathbf{a}_i)) = 2j\right\} = \hat{g}_j \quad \text{for } 0 \leq j \leq \deg(\hat{g}).$$

Proof. From the right hand side of (2.3) it is clear that $g(T) - l_2$ is expressible as a sum of l_1 powers of q with non-negative coefficients. Indeed the coefficient $\hat{g}_i$ is equal to the number of summands q^i. This proves (a). The minimum value on the right hand side of (2.3) corresponds to a choice of l_1 vectors $\mathbf{a}_1, \ldots, \mathbf{a}_{l_1}$ that satisfy the assumptions of (b). □

3. Bounds for $m_{\text{faithful}}(\mathscr{G}_R)$

In this section we turn our attention to $m_{\text{faithful}}(\mathscr{G}_R)$, where R is a finite truncated valuation ring. It is known (see for example [McL73]) that any such R is isomorphic to $\mathcal{O}/\mathfrak{p}^d$ for some $d \geq 1$, where $\mathcal{O}$ is the ring of integers of a p-adic field and $\mathfrak{p}$ is the maximal ideal of $\mathcal{O}$ (thus, in the notation of Section 1 we have $\mathfrak{m} = \mathfrak{p}/\mathfrak{p}^d$). Henceforth we assume that $R = \mathcal{O}/\mathfrak{p}^d$.

By analogy with the special case where R is a finite field, one expects that a suitable variation of Theorem 2.6 holds for $m_{\text{faithful}}(\mathscr{G}_R)$. Indeed the method of proof of Theorem 2.6 can be adapted to prove Proposition 3.2 below. Recall that $p = \mathrm{char}(\mathcal{O}/\mathfrak{p})$, $\#\mathcal{O}/\mathfrak{p} = p^f$, and $p(\mathcal{O}/\mathfrak{p}^d) = \mathfrak{p}^e/\mathfrak{p}^d$. It follows that $\mathcal{O}/\mathfrak{p}^e$ is an $\mathbb{F}_p$-vector space. We define the map

$$\mathsf{proj} : (\mathcal{O}/\mathfrak{p}^d)^{\oplus m} \to (\mathcal{O}/\mathfrak{p}^e)^{\oplus l_1} \tag{3.1}$$

to be the natural projection on the first l_1 components, i.e.,

$$\mathsf{proj}(a_1, \ldots, a_m) := (\bar{a}_1, \ldots, \bar{a}_{l_1}),$$

where $a \mapsto \bar{a}$ denotes the natural projection $\mathcal{O}/\mathfrak{p}^d \to \mathcal{O}/\mathfrak{p}^e$.

Remark 3.1. Any finitely generated abelian group A can be expressed as a direct sum $A \cong A_F \oplus A_T$ where A_F is free abelian and A_T is torsion. Tensoring A (over $\mathbb{Z}$) with a commutative ring R whose characteristic is a prime number larger than the exponent of A_T annihilates A_T. Furthermore, if A and B are finitely generated abelian groups and $A \to B$ is an injective group homomorphism, then the induced map $A_F \to B/B_T \cong B_F$ is also an injection. In particular a basis of A_F is mapped to a linearly independent set of vectors. After tensoring with R, if the charatecteristic of R is a sufficiently large prime, the image of the basis still remains linearly independent (because the determinant of a square minor of maximum size will remain nonzero). It follows that a short exact sequence of

finitely generated abelian groups will remain exact upon tensoring with a finite truncated valuation ring R as long as p is sufficiently large (depending on the exact sequence).

In the proof of Theorem 1.3 we need the following extension of Theorem 2.6.

Proposition 3.2. *Let $\mathfrak{g}$ be as in Theorem 2.6 and let R be a finite truncated local ring. Let $\mathcal{O}(d,m,e,l_1)$ denote the set of fel_1-tuples $(\mathbf{a}_1,\dots,\mathbf{a}_{fel_1})$ such that $\mathbf{a}_i \in (\mathcal{O}/\mathfrak{p}^d)^{\oplus m}$ for all $1 \le i \le fel_1$, and the projections $\{\mathsf{proj}(\mathbf{a}_i)\}_{i=1}^{fel_1}$ form a basis of the $\mathbb{F}_p$-vector space $(\mathcal{O}/\mathfrak{p}^e)^{\oplus l_1}$. Then there exists a constant $M>0$, depending only on $\mathfrak{g}$ and the choice of the semibasis data $\mathcal{SB}_{\mathfrak{g}}$ that is used to define $F_{\mathfrak{g}}$, such that for $p>M$ we have*

$$m_{\text{faithful}}(\mathscr{G}_R) = fl_2e + \min\left\{ \sum_{i=1}^{fel_1} \left(\frac{p^{fd(\mathrm{rk}_{\mathbb{Z}}(\mathfrak{g})-l_1-l_2)}}{\#\ker_{\mathcal{O}/\mathfrak{p}^d}(F_{\mathfrak{g}}(\mathbf{a}_i))} \right)^{\frac{1}{2}} \;:\; (\mathbf{a}_1,\dots,\mathbf{a}_{fel_1}) \in \mathcal{O}(d,m,e,l_1) \right\}.$$

Proof. Since the argument is nearly identical to the proof of Theorem 2.6, we will only explain the points of divergence from [BMKS19]. In what follows, we will refer to the notation of [BMKS19]. We will not give an explicit value of M, but it can be computed similar to [BMKS19]. Using Remark 3.1 and some elementary arguments, one can verify that $Z(\mathfrak{g}_R) = Z(\mathscr{G}_R) = Z(\mathfrak{g})_R$, $[\mathfrak{g}_R,\mathfrak{g}_R] = [\mathfrak{g},\mathfrak{g}]_R$, and $Z(\mathfrak{g})_R \cap [\mathfrak{g}_R,\mathfrak{g}_R] = (Z(\mathfrak{g}) \cap [\mathfrak{g},\mathfrak{g}])_R$. In addition, the latter R-modules embed as free submodules of $\mathfrak{g}_R$. We choose a primitive additive character $\psi : \mathcal{O}/\mathfrak{p}^d \to \mathbb{C}^*$ as follows. Let $\psi_\circ : \mathbb{Q}_p \to \mathbb{C}^*$ be the additive character defined by $\psi_\circ(x) := e^{2\pi i\{x\}_p}$, where $\{x\}_p$ denotes the p-adic fractional part of x. Note that $\ker\psi_\circ = \mathbb{Z}_p$. Now let $\mathbb{K}$ denote the fraction field of $\mathcal{O}$, and set

$$\mathfrak{D} := \left\{ x \in \mathcal{O} \;:\; \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}_p}(x\mathcal{O}) \subseteq \mathbb{Z}_p \right\}.$$

Then $\mathfrak{D} = \mathfrak{p}^{-\ell}$ for some $\ell \ge 0$. Fixing a uniformizer $\varpi \in \mathfrak{p}$, we obtain an isomorphism of the character group $\widehat{\mathcal{O}/\mathfrak{p}^d}$ with $\mathcal{O}/\mathfrak{p}^d$ via the map $b+\mathfrak{p}^d \mapsto \psi_b \in \widehat{\mathcal{O}/\mathfrak{p}^d}$, where $\psi_b(x) := \psi_\circ(\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}_p}(\varpi^{-d-\ell}bx))$. Note that $\psi_b(x) = \psi(bx)$ where $\psi := \psi_1$. From this it follows that $\ker(\psi)$ does not contain any nontrivial ideal of $\mathcal{O}/\mathfrak{p}^d$. Choose $\mathbf{u}_1,\dots,\mathbf{u}_{l_3} \in \mathfrak{g}$ to be representatives of a semibasis of $\mathfrak{g}/(Z(\mathfrak{g})+[\mathfrak{g},\mathfrak{g}])$. Then by the above remarks for p sufficiently large $\mathfrak{g}_R$ is a free R-module with generators $\mathbf{w}_1,\dots,\mathbf{w}_m,\mathbf{z}_1,\dots,\mathbf{z}_{l_2},\mathbf{u}_1,\dots,\mathbf{u}_{l_3}$. Consequently, additive characters of $\mathfrak{g}_R$ are of the form

$$\psi_{\mathbf{a}} := \psi\left(\sum_{i=1}^{m} a_i\mathbf{w}_i + \sum_{i=1}^{l_2} b_i\mathbf{z}_i + \sum_{i=1}^{l_3} c_i\mathbf{u}_i \right),$$

where $\mathbf{a} := (a_1,\dots,a_m,b_1,\dots,b_{l_2},c_1,\dots c_{l_3}) \in R^{\oplus(m+l_2+l_3)}$. The dimension of the irreducible representation of $\mathscr{G}_R$ corresponding to $\psi_{\mathbf{a}}$ is equal to

$$\left(\frac{q^{d(\mathrm{rk}_{\mathbb{Z}}(\mathfrak{g})-l_1-l_2)}}{\#\ker_{\mathcal{O}/\mathfrak{p}^d} F_{\mathfrak{g}}(a_1,\dots,a_m)} \right)^{\frac{1}{2}}.$$

The rest of the argument is essentially the same as the proof of Theorem 2.6. We remark that in the proof given in [BMKS19] we used Rado-Horn's Theorem to reduce the mimimum from being over $\mathbb{F}_p$-bases to over $\mathbb{F}_q$-bases. We are unable to extend this step to the setting of finite truncated valuation rings, which is why in the statement of Proposition 3.2 the minimum is taken over a family of $\mathbb{F}_p$-bases. □

Definition 3.3. *Let $\{\phi_i\}_{i\in\mathcal{I}}$ be a finite family of polynomials in $\mathbb{Z}[T_1,\dots,T_m]$. A solution $(z_1,\dots,z_m) \in (\mathcal{O}/\mathfrak{p})^{\oplus m}$ to the system of equations $\phi_i = 0$, $i \in \mathcal{I}$, is called refinable to $\mathcal{O}$ if*

there exists a solution $(\tilde{z}_1, \dots, \tilde{z}_m) \in \mathcal{O}^{\oplus m}$ to this system whose reduction modulo $\mathfrak{p}$ equals $(z_1, \dots, z_m)$.

In the proof of Theorem 1.3 we need a variation of Hensel's Lemma, which has no constraint on the derivative, but assumes that the residual characteristic is sufficiently large. This result (see Proposition 3.4 below) has been proved by Ax and Kochen [AK65] over $\mathbb{Q}_p$ using ultrafilters, and by Greenleaf [Gre65] and Greenberg [Gre74] over arbitrary p-adic fields (with a quantitative lower bound on p) using algebraic geometry. An elementary argument for Greenberg's theorem was given by Kneser in [Kne78]. We remark that a minor adaptation of the proof of Ax and Kochen establishes Proposition 3.4.

Proposition 3.4. *Let $\{\phi_i\}_{i\in\mathcal{I}}$ be a finite family of multivariate polynomials with integer coefficients. Then there exists a constant $M > 0$ such that for every p-adic field $\mathbb{K}$ with ring of integers $\mathcal{O}$, such that the characteristic of the residue field $\mathcal{O}/\mathfrak{p}$ is bigger than M, every solution in $\mathcal{O}/\mathfrak{p}$ of the system of equations $\phi_i = 0$, $i \in \mathcal{I}$, is refinable to a solution in $\mathcal{O}$.*

Proof of Theorem 1.3. Set $\mathscr{P} := \mathscr{P}_{i_\circ}$, $\mathscr{F} := \mathscr{F}_{j_\circ}$, and $g(T) := g_{i_\circ j_\circ}(T)$. As in Corollary 2.9, we express $g(T)$ as $g(T) = l_2 + \hat{g}(T)$ where $\hat{g}(T) := \sum_{i=0}^{\deg(\hat{g})} \hat{g}_i T^i$. First we prove the upper bound. Set $\tilde{g}_k := \sum_{i=0}^{k} \hat{g}_i$ for $0 \le k \le \deg(\hat{g})$ and $\tilde{g}_{-1} := 0$. Recall that $n := \mathrm{rk}_{\mathbb{Z}}(\mathfrak{g}/\mathrm{Z}(\mathfrak{g}))$ is the size of the commutator matrix $F_{\mathfrak{g}}$. For $0 \le k \le \lfloor \frac{n}{2} \rfloor$ let $D^{(k)}$ be the $n \times n$ diagonal matrix whose diagonal entries are defined by $D^{(k)}_{i,i} = 1$ for $i \le 2k$ and $D^{(k)}_{i,i} = 0$ for $i > 2k$. Consider the system of polynomial equations with integer coefficients in variables $\mathsf{x}^{(i)}_{a,b}$, $\mathsf{y}^{(i)}_{a,b}$, $\mathsf{r}^{(i)}$, $\mathsf{s}^{(i)}$, and $\mathsf{a}^{(i)}_j$, for $1 \le a, b \le n$, $1 \le i \le fl_1$, and $1 \le j \le m := \mathrm{rk}_{\mathbb{Z}}([\mathfrak{g}, \mathfrak{g}])$, that is defined by

$$\text{(3.2)} \quad \begin{cases} X^{(i)} F(\mathsf{a}^{(i)}_1, \dots, \mathsf{a}^{(i)}_m) Y^{(i)} = D^{(k)} & \text{for } f\tilde{g}_{k-1} + 1 \le i \le f\tilde{g}_k \text{ and } 0 \le k \le \deg(\hat{g}), \\ \mathsf{r}^{(i)} \det X^{(i)} = 1 & \text{for } 1 \le i \le fl_1, \\ \mathsf{s}^{(i)} \det Y^{(i)} = 1 & \text{for } 1 \le i \le fl_1, \end{cases}$$

where $X^{(i)}$ and $Y^{(i)}$ are $n \times n$ matrices with entries $\mathsf{x}^{(i)}_{a,b}$ and $\mathsf{y}^{(i)}_{a,b}$, respectively. Now fix $(p, f) \in \mathscr{P} \times \mathscr{F}$, and let $\mathbf{a}_1, \dots, \mathbf{a}_{l_1} \in (\mathcal{O}/\mathfrak{p})^{\oplus m}$ be chosen as in Corollary 2.9. Next choose any $\mathbb{F}_p$-basis $\beta_1, \dots, \beta_f$ for $\mathcal{O}/\mathfrak{p}$, and consider the vectors $\mathbf{a}'_{i,j} := \beta_j \mathbf{a}_i$ for $1 \le i \le l_1$ and $1 \le j \le f$. The projections of the $\mathbf{a}'_{i,j}$ on the first l_1 coordinates form a basis for the $\mathbb{F}_p$-vector space $(\mathcal{O}/\mathfrak{p})^{\oplus l_1}$. Furthermore,

$$\#\left\{(i,j) \,:\, \mathrm{rk}_{\mathcal{O}/\mathfrak{p}}(F(\mathbf{a}'_{i,j})) = 2k\right\} = f\hat{g}_k,$$

because $\#\ker_{\mathcal{O}/\mathfrak{p}}(F(\beta_j \mathbf{a}_i))$ does not depend on j. It follows that for all $(p, f) \in \mathscr{P} \times \mathscr{F}$, the polynomial system (3.2) has a solution in $\mathcal{O}/\mathfrak{p}$, where the vectors $(\mathsf{a}^{(u)}_1, \dots, \mathsf{a}^{(u)}_m)$ for $f\tilde{g}_{k-1} + 1 \le u \le f\tilde{g}_k$ are equal to the $\mathbf{a}'_{i,j}$ satisfying $\mathrm{rk}_{\mathcal{O}/\mathfrak{p}}(F(\mathbf{a}'_{i,j})) = 2k$. By Proposition 3.4, for p sufficiently large (depending only on the system (3.2), hence only on $\mathfrak{g}$) this solution is refinable to a solution in $\mathcal{O}$. In particular there exist vectors $\tilde{\mathbf{a}}_i \in \mathcal{O}^{\oplus m}$ for $1 \le i \le fl_1$ such that $X_i F(\tilde{\mathbf{a}}_i) Y_i = D^{(k)}$ for $f\tilde{g}_{k-1} + 1 \le i \le f\tilde{g}_k$ and $0 \le k \le \deg(\hat{g})$, where X_i and Y_i are invertible $n \times n$ matrices with entries in $\mathcal{O}$. If $\varpi \in \mathfrak{p}$ is a uniformizer then for $0 \le j \le e-1$ we have $\#\ker_{\mathcal{O}/\mathfrak{p}^d} F(\varpi^j \tilde{\mathbf{a}}_i) = p^{fd(n-2k)+2kfj}$. Since $\mathrm{rk}_{\mathbb{Z}}(\mathfrak{g}) - l_1 - l_2 = n$, we obtain

$$\left(\frac{p^{fd(\mathrm{rk}_{\mathbb{Z}}(\mathfrak{g})-l_1-l_2)}}{\#\ker_{\mathcal{O}/\mathfrak{p}^d}(F(\varpi^j \tilde{\mathbf{a}}_i))}\right)^{\frac{1}{2}} = p^{kf(d-j)}.$$

Furthermore, the projections to the first l_1 coordinates of the list of vectors

$$\{\varpi^j \tilde{\mathbf{a}}_i \ : \ 0 \leq j \leq e-1 \text{ and } 1 \leq i \leq fl_1\}$$

forms a basis of the $\mathbb{F}_p$-vector space $(\mathcal{O}/\mathfrak{p}^e)^{\oplus l_1}$. The upper bound part of the theorem follows from Proposition 3.2.

For the lower bound, it suffices to assume that $p > \max\left\{l_1+l_2, l_2+\sum_{i=0}^{\deg(\hat{g})}\hat{g}_i\right\}$. Suppose that the fel_1-tuple $(\mathbf{a}_1,\dots,\mathbf{a}_{fel_1})$ of vectors in $(\mathcal{O}/\mathfrak{p}^d)^{\oplus m}$ corresponds as in Proposition 3.2 to the value of $m_{\text{faithful}}(\mathscr{G}_R)$. Let $\overline{\mathsf{proj}} : (\mathcal{O}/\mathfrak{p}^d)^{\oplus m} \to (\mathcal{O}/\mathfrak{p})^{\oplus l_1}$ be the natural projection map defined similar to proj (see (3.1)). The vectors $\overline{\mathsf{proj}}(\mathbf{a}_i)$ form a spanning set of the $\mathbb{F}_p$-vector space $(\mathcal{O}/\mathfrak{p})^{\oplus l_1}$, hence without loss of generality we can assume that $\{\overline{\mathsf{proj}}(\mathbf{a}_i)\}_{i=1}^{fl_1}$ is an $\mathbb{F}_p$-basis of $(\mathcal{O}/\mathfrak{p})^{\oplus l_1}$. For $d \geq 1$ and $1 \leq i \leq fl_1$ set

$$x_{i,d} := \left(\frac{p^{f(\mathrm{rk}_{\mathbb{Z}}(\mathfrak{g})-l_1-l_2)}}{\#\ker_{\mathcal{O}/\mathfrak{p}^d}(F(\mathbf{a}_i))}\right)^{\frac{1}{2}}.$$

Note that $x_{i,d}^2$ is the cardinality of the subgroup of $(\mathcal{O}/\mathfrak{p}^d)^{\oplus m}$ that is generated by the columns of $F(\mathbf{a}_i)$, and since $F(\mathbf{a}_i)$ is a skew symmetric matrix, we also have $x_{i,d} = p^{fy_{i,d}}$ for a non-negative integer $y_{i,d}$. It follows that $x_{i,d} \geq x_{i,1}^d$. By Proposition 3.2 (for $R = \mathbb{F}_{p^f}$) and Theorem 1.1,

$$fl_2 + \sum_{i=1}^{fl_1} p^{fy_{i,1}} \geq fg(p^f). \tag{3.3}$$

Setting $y_{i,d} = 0$ for $fl_1 + 1 \leq i \leq f(l_1+l_2)$ and $d \geq 1$, from (3.3) it follows that

$$\sum_{i=1}^{f(l_1+l_2)} p^{fy_{i,1}} \geq fg(p^f). \tag{3.4}$$

Our strategy is to prove that

$$\sum_{i=1}^{f(l_1+l_2)} p^{fdy_{i,1}} \geq fg(p^{fd}). \tag{3.5}$$

Without loss of generality we assume that $y_{1,1} \geq \cdots \geq y_{f(l_1+l_2),1}$. Set $N := \deg(\hat{g})$. There are two cases to consider:

Case 1. $y_{i,1} \leq N$ for all i. We claim that $y_{i,1} = N$ for $1 \leq i \leq f\hat{g}_N$: otherwise since $p \geq 1 + l_1 + l_2$ and the coefficients of $\hat{g}(T)$ are non-negative, we have

$$\sum_{i=1}^{f(l_1+l_2)} p^{fy_{i,1}} \leq (f\hat{g}_N - 1)p^{fN} + f(l_1+l_2)p^{f(N-1)} < f\hat{g}_N p^{fN} \leq f\hat{g}(p^f) \leq fg(p^f),$$

which is a contradiction. It follows from above that $y_{i,1} = N$ for $1 \leq i \leq f\hat{g}_N$. If $y_{f\hat{g}_N+1,1} = N$ then from $p \geq l_2 + \sum_{i=0}^{N}\hat{g}_i$ it follows that

$$\begin{aligned} m_{\text{faithful}}(\mathscr{G}_R) &\geq \sum_{i=1}^{f(l_1+l_2)} x_{i,d} \geq \sum_{i=1}^{f(l_1+l_2)} x_{i,1}^d = \sum_{i=1}^{f(l_1+l_2)} p^{fdy_{i,1}} \geq (f\hat{g}_N + 1)p^{fdN} \\ &= f\hat{g}_N p^{fdN} + p^{fd(N-1)}p^{fd} \geq f\hat{g}_N p^{fdN} + p^{fd(N-1)} f\left(l_2 + \sum_{i=0}^{N-1}\hat{g}_i\right) \geq fg(p^{fd}). \end{aligned}$$

If $y_{f\hat{g}_N+1,1} < N$, then by cancelling out the summands p^{fN} from both sides of (3.4) we obtain a similar relation for a polynomial of lower degree on the right hand side of (3.5), and we can repeat the above argument (leading to either Case 1 above, or Case 2 below).

Case 2. $y_{1,1} \geq N+1$. Then from $p \geq l_2 + \sum_{i=0}^{N} \hat{g}_i$ it follows that

$$m_{\text{faithful}}(\mathscr{G}_R) \geq p^{fdy_{1,1}} \geq p^{fd(N+1)} \geq (1 + l_2 + \sum_{i=0}^{N} \hat{g}_i)^f p^{fdN} \tag{3.6}$$

$$\geq fl_2 + fp^{fdN} \sum_{i=0}^{N} \hat{g}_i \geq fg(p^{fd}). \qquad \square$$

4. Polynomiality over rings for pattern groups

In this section we prove Theorem 1.5, which in particular establishes Conjecture 1.2 for pattern groups. Throughout this section we set $\mathfrak{g} := \mathfrak{g}_{\prec}$. We begin with recalling some notation and general facts from [BMKS19] and [BMKS16]. For an abelian p-group Γ, set

$$\Omega_1(\Gamma) := \{g \in \Gamma : g^p = \mathbf{1}\}.$$

Note that $\Omega_1(\Gamma)$ is an $\mathbb{F}_p$-vector space. For an abelian group A we set $\widehat{A} := \mathrm{Hom}(A, \mathbb{C}^*)$. When A is an elementary abelian p-group, $\widehat{A}$ is canonically an $\mathbb{F}_p$-vector space and there exists an isomorphism $\widehat{A} \cong \mathrm{Hom}(A, \mathbb{Z}/p\mathbb{Z})$ obtained by identifying $\mathbb{Z}/p\mathbb{Z}$ with the subgroup of p-th roots of unity in $\mathbb{C}^*$.

Recall that $R \cong \mathcal{O}/\mathfrak{p}^d$ for $d \geq 1$. Fix a primitive character $\psi : R \to \mathbb{C}^*$ (for example the character described in the proof of Proposition 3.2), and also set $\psi_b(x) := \psi(bx)$ for $b \in R$ and $x \in R$, so that the map

$$R \to \widehat{R}\ ,\ b \mapsto \psi_b \tag{4.1}$$

is a group isomorphism. Now let $\mathfrak{a}$ be an ideal in R and set $\mathrm{Ann}(\mathfrak{a}) := \{r \in R : r\mathfrak{a} = 0\}$. From surjectivity of the restriction $\widehat{R} \to \widehat{\mathfrak{a}}$ it follows that the map

$$R/\operatorname{Ann}(\mathfrak{a}) \to \widehat{\mathfrak{a}}\ ,\ b + \operatorname{Ann}(\mathfrak{a}) \mapsto \psi_b\big|_{\mathfrak{a}}$$

is a group isomorphism. Notice that $\mathrm{Ann}(\mathfrak{p}^k/\mathfrak{p}^d) = \mathfrak{p}^{(d-k)}/\mathfrak{p}^d$ for $0 \leq k \leq d$, so that we obtain the following lemma.

Lemma 4.1. *Every additive character of the group $\mathfrak{p}^k/\mathfrak{p}^d$, where $0 \leq k \leq d$, is of the form*

$$\psi_b : \mathfrak{p}^k/\mathfrak{p}^d \to \mathbb{C}^*\ ,\ x \mapsto \psi(bx),$$

for a unique $b + \mathfrak{p}^{(d-k)}/\mathfrak{p}^d \in (\mathcal{O}/\mathfrak{p}^d)/(\mathfrak{p}^{(d-k)}/\mathfrak{p}^d) \cong \mathcal{O}/\mathfrak{p}^{d-k}$. In particular $\widehat{\mathfrak{p}^k/\mathfrak{p}^d} \cong \mathcal{O}/\mathfrak{p}^{(d-k)}$.

Hereafter, for a finite p-group G the $\mathbb{Z}/p\mathbb{Z}$-vector space $\mathrm{Hom}(\Omega_1(\mathrm{Z}(\mathrm{G})), \mathbb{C}^*)$ will be denoted by $\widehat{\Omega}_1(\mathrm{Z}(\mathrm{G}))$. By the central character of an irreducible representation (ρ, V) of G we mean the group homomorphism $\chi : \mathrm{Z}(\mathrm{G}) \to \mathbb{C}^*$ satisfying $\rho(g) = \chi(g)1_V$ for $g \in \mathrm{Z}(\mathrm{G})$.

Lemma 4.2. *Let G be a finite p-group.*

(i) *Let $(\rho_i, V_i)_{1 \leq i \leq k}$ be a family of irreducible representations of G with central characters χ_i. Suppose that $\{\chi_{i|_{\Omega_1(\mathrm{Z}(\mathrm{G}))}} : 1 \leq i \leq k\}$ spans $\widehat{\Omega}_1(\mathrm{Z}(\mathrm{G}))$. Then $\oplus_{1 \leq i \leq k}\rho_i$ is a faithful representation of G.*

(ii) *Let ρ be a faithful representation of G of dimension $m_{\mathrm{faithful}}(\mathrm{G})$. Then ρ decomposes as a direct sum of exactly $r := r_G$ irreducible representations, where r_G denotes the minimum number of generators of the abelian group $\mathrm{Z}(\mathrm{G})$. Furthermore, the restrictions to $\Omega_1(\mathrm{Z}(\mathrm{G}))$ of the central characters of these representations form a $\mathbb{Z}/p\mathbb{Z}$-basis for $\widehat{\Omega}_1(\mathrm{Z}(\mathrm{G}))$.*

Proof. For (i), see [BMKS19, Lem. 3.4] or [MR10]. For (ii), see [BMKS19, Lem. 3.5] □

Remark 4.3. For a finite abelian group A, the minimum number of generators is equal to the number of invariant factors of A (this is a consequence of elementary divisor theorem for finite abelian groups). By a similar argument, if A is a finite abelian p-group, then the minimum number of generators of A is equal to $\dim_{\mathbb{Z}/p\mathbb{Z}}(A \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z})$. In particular, the minimum number of generators of the abelian group $\mathcal{O}/\mathfrak{p}^d$ is equal to fe. This is because $\mathcal{O}/\mathfrak{p}^d \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z} \cong (\mathcal{O}/\mathfrak{p}^d)/(p(\mathcal{O}/\mathfrak{p}^d)) \cong \mathcal{O}/\mathfrak{p}^e$ and $\#\mathfrak{p}^i/\mathfrak{p}^{i+1} = p^f$ for $0 \le i \le e-1$.

Next we establish a general combinatorial lemma about bases of direct sums.

Lemma 4.4. *Let V_1 and V_2 be two vector spaces of dimensions d_1 and d_2 over an arbitrary field. Let $S = \{(v_i, v_i') : 1 \le i \le d_1 + d_2\}$ be a basis for $V_1 \oplus V_2$. Then S can be partitioned into two sets B_1 and B_2, of sizes d_1 and d_2 respectively, such that the V_i-components of the vectors in B_i form a basis of V_i for $i = 1, 2$.*

Proof. The following argument is communicated to us by I. Bogdanov. Let $\{e_1, \dots, e_{d_1}\}$ and $\{e_1', \dots, e_{d_2}'\}$ denote bases of V_1 and V_2, respectively. Then for $1 \le j \le d_1 + d_2$ we obtain

$$v_j = \sum_{i=1}^{d_1} a_{ij} e_i \quad \text{and} \quad v_j' = \sum_{i=1}^{d_2} b_{ij} e_j'.$$

Consider the square matrix A of size $d_1 + d_2$ whose i-th column, for $1 \le i \le d_1 + d_2$, is the transpose of the row vector

$$(a_{1i}, \cdots, a_{d_1 i}, b_{1i}, \dots, b_{d_2 i}).$$

Since S is a basis, A is invertible. Set $I := \{1, \dots, d_1\}$ and consider the generalized Laplace expansion

$$\det(A) = \sum_{\substack{J \subseteq \{1,\dots,d_1+d_2\} \\ |J| = d_1}} (-1)^{\sum_{i \in I} i + \sum_{j \in J} j} \det A_{I,J} \det A_{I',J'},$$

where $I' := \{d_1 + 1, \dots, d_1 + d_2\}$, J' is the complement of J in $\{1, \dots, d_1 + d_2\}$, and $A_{I,J}$ (respectively, $A_{I',J'}$) is the minor of A corresponding to rows and columns indexed by I and J (respectively, by I' and J'). Since $\det(A) \neq 0$, there exists J with $\det A_{I,J} \det A_{I',J'} \neq 0$. The desired sets are $B_1 := \{(v_j, v_j') : j \in J\}$ and $B_2 := \{(v_j, v_j') : j \in J'\}$. □

Lemma 4.4 and induction yield the following.

Lemma 4.5. *Let V be a finite dimensional vector space over an arbitrary field and let S be a basis for $V^{\oplus k}$ where $k \ge 1$. Then S can be partitioned into subsets $B_1, \dots, B_k$ such that each of the sets $\{\pi_\ell(w) : w \in B_\ell\}$ is a basis of V for $1 \le \ell \le k$, where $\pi_\ell(v_1, \dots, v_k) := v_\ell$.*

The following simple lemma was also used in [BMKS16].

Lemma 4.6. *Let $a_0, \dots, a_{m-1}$ be non-negative real numbers with $\sum_{\ell=0}^{m-1} a_\ell = m$. Assume that for any $0 \le \ell \le m-1$ we have $a_\ell + \cdots + a_{m-1} \le m - \ell$. Then for any decreasing sequence $x_0 \ge \cdots \ge x_{m-1}$, we have $\sum_{\ell=0}^{m-1} a_\ell x_\ell \ge \sum_{\ell=0}^{m-1} x_\ell$.*

Proof. Define $A_\ell := \sum_{j=\ell}^{m-1} a_j$ for $0 \le \ell \le m-1$ and set $A_m := 0$. Then $A_\ell \le m - \ell$ and $A_0 = m$. Set $\Delta A_\ell := A_\ell - A_{\ell+1}$ and $\Delta x_\ell := x_\ell - x_{\ell-1}$. Since $\Delta x_\ell \le 0$, we have

$$\sum_{\ell=0}^{m-1} a_\ell x_\ell = \sum_{\ell=0}^{m-1} \Delta A_\ell x_\ell = A_0 x_0 + \sum_{\ell=1}^{m-1} A_\ell \Delta x_\ell \ge m x_0 + \sum_{\ell=1}^{m-1} (m-\ell)\Delta x_\ell = \sum_{\ell=0}^{m-1} x_\ell. \qquad \square$$

For the proof of Theorem 1.5 we need some standard facts from the *orbit method* for describing irreducible representations of finite p-groups. The tools that we need from the orbit method can be found in various references, including [Kaz77], [How77], and [BS08]. For the reader's convenience, we briefly review the pertinent results from the orbit method (we follow [BS08] closely; see also [BMKS19, Sec. 3.2]). Let $\mathfrak{f}$ and $\exp(\mathfrak{f})$ be as in Section 1. Then we can define a coadjoint action of $\exp(\mathfrak{f})$ on $\widehat{\mathfrak{f}} := \mathrm{Hom}_{\mathbb{Z}}(\mathfrak{f}, \mathbb{C}^*)$ as follows. For $x \in \exp(\mathfrak{f}) = \mathfrak{f}$ and $\theta \in \widehat{\mathfrak{f}}$, we define $\theta^x \in \widehat{\mathfrak{f}}$ by

$$\theta^x(y) := \theta\left(\sum_{k\ge 0} \frac{\mathrm{ad}_x^k(y)}{k!}\right), \quad \text{for } y \in \mathfrak{f}.$$

Note that only finitely many summands are nonzero.

Theorem 4.7. *Assume that p is an odd prime that is strictly larger than the nilpotency class of $\mathfrak{f}$. Then there exists a bijection between the orbits of the coadjoint action on $\widehat{\mathfrak{f}}$ and characters of irreducible representations of $\exp(\mathfrak{f})$. Furthermore, if ρ_Θ denotes the irreducible representation corresponding to the coadjoint orbit $\Theta \subseteq \widehat{\mathfrak{f}}$, then the following statements hold.*

(a) *The character of ρ_Θ is given by $\chi_\Theta(x) := |\Theta|^{-1/2} \sum_{\theta\in\Theta} \theta(x)$ for $x \in \exp(\mathfrak{f}) = \mathfrak{f}$.*

(b) $\dim(\rho_\Theta) = \left(\dfrac{\#\mathfrak{f}}{\#\mathrm{Stab}_{\mathfrak{f}}(\theta_0)}\right)^{1/2}$ *for $\theta_0 \in \Theta$, where* $\mathrm{Stab}_{\mathfrak{f}}(\theta_0) := \{x \in \mathfrak{f} : \theta_0([x,\mathfrak{f}]) = 1\}$.

(c) *$\rho_\Theta(g)$ is multiplication by the scalar $\theta(g)$ for $g \in \mathrm{Z}(\exp(\mathfrak{f}))$ and $\theta \in \Theta$.*

Recall that in this section $\mathfrak{g} := \mathfrak{g}_\prec$. Our next goal is to use the orbit method to study irreducible representations of $\mathscr{G}_R := \exp(\mathfrak{g}_R)$.

Remark 4.8. The nilpotency class of $\mathfrak{g}$ is $\max\{\alpha(i,j) : i \prec j\} + 1$, where $\alpha(i,j)$ is defined as in (1.1). To see this, note that the l-th term in the lower central series of $\mathfrak{g}$ is the $\mathbb{Z}$-span of the e_{ij} where $\alpha(i,j) \ge l$. It is also straightforward to verify that $\mathrm{Z}(\mathfrak{g})$ is the $\mathbb{Z}$-span of the e_{ij} where $(i,j) \in I_{\mathrm{ex}}$ (see [BMKS19, Lemma 4.2]). The same argument proves that $\mathrm{Z}(\mathfrak{g}_R)$ is a free R-module generated by the e_{ij} for $(i,j) \in I_{\mathrm{ex}}$.

By the isomorphism (4.1), elements of $\widehat{\mathfrak{g}_R}$ are of the form $\psi_{\mathbf{b}}$ for a vector $\mathbf{b} := (b_{ij})_{i\prec j}$ with entries in R, where

$$\psi_{\mathbf{b}}\left(\sum_{i\prec j} x_{ij} e_{ij}\right) := \psi\left(\sum_{i\prec j} b_{ij} x_{ij}\right). \tag{4.2}$$

Definition 4.9. *We define the level of $b := \tilde{b} + \mathfrak{p}^d \in R$ to be the smallest k such that $\tilde{b} \notin \mathfrak{p}^{k+1}$, and we denote it by $\mathbf{lev}(b)$.*

Proposition 4.10. *Let $b_{ij} = \tilde{b}_{ij} + \mathfrak{p}^d$ for $i \prec j$ be elements of R. Set $\mathbf{b} := (b_{ij})_{i\prec j}$, and let $\rho_{\mathbf{b}}$ be the irreducible representation of $\mathscr{G}_R$ corresponding to the orbit of $\psi_{\mathbf{b}}$ under the coadjoint action. Then $\dim \rho_{\mathbf{b}} \ge p^{f(d-\mathbf{lev}(b_{i_1 j_1}))\alpha(i_1,j_1)}$ for all $(i_1,j_1) \in I_{\mathrm{ex}}$.*

Proof. We use Theorem 4.7(b). Let $x = \sum_{i \prec j} x_{ij} e_{ij} \in \mathfrak{g}_R$ be an element of $\mathrm{Stab}_{\mathfrak{g}_R}(\psi_{\mathbf{b}})$. Then for any $y = \sum_{i \prec j} y_{ij} e_{ij} \in \mathfrak{g}_R$ we have

$$1 = \psi_{\mathbf{b}}([x,y]) = \psi_{\mathbf{b}}\left(\sum_{i\prec j,\, k\prec l} x_{ij}y_{kl}[e_{ij}, e_{kl}]\right)$$
$$= \psi\left(\sum_{i\prec j}\sum_{i\prec k\prec j} b_{ij}(x_{ik}y_{kj} - x_{kj}y_{ik})\right) = \psi\left(\sum_{i\prec j}\left(\sum_{k\prec i} b_{kj}x_{ki} - \sum_{j\prec l} b_{il}x_{jl}\right) y_{ij}\right).$$

Since the $y_{ij} \in R$ are arbitrary and ψ is primitive, the stabilizer of $\psi_{\mathbf{b}}$ is equal to the solution set of the system of linear equations $\mathscr{L} := \{L_{ij}(x_{st}) = 0 \ : \ i,j \in [n] \text{ and } i \prec j\}$, where

$$L_{ij}(x_{st}) := \sum_{k\prec i} b_{kj}x_{ki} - \sum_{j\prec l} b_{il}x_{jl}. \tag{4.3}$$

In particular since $(i_1, j_1) \in I_{\mathrm{ex}}$, the linear forms $L_{i_1 i}(x_{st})$ and $L_{j j_1}(x_{st})$, for $i_1 \prec i \prec j_1$ and $i_1 \prec j \prec j_1$, yield $2\alpha(i_1, j_1)$ linear equations that can be written as

$$b_{i_1 j_1}x_{ij_1} = -\sum_{i\prec k\neq j_1} b_{i_1 k}x_{ik} \quad \text{and} \quad b_{i_1 j_1}x_{i_1 j} = -\sum_{i_1\neq l\prec j} b_{l j_1}x_{lj}. \tag{4.4}$$

The cardinality of the kernel of the map $R \to R$, $x \mapsto b_{i_1 j_1}x$, is $p^{f\mathbf{lev}(b_{i_1 j_1})}$. To see this, note that the ideal generated by $b_{i_1 j_1}$ is $\mathfrak{p}^{\ell}/\mathfrak{p}^d$, with $\ell = \mathbf{lev}(b_{i_1 j_1})$. The above fact now follows from $\mathrm{Ann}(\mathfrak{p}^{\ell}/\mathfrak{p}^d) = \mathfrak{p}^{(d-\ell)}/\mathfrak{p}^d$ in combination with $\#(\mathfrak{p}^i/\mathfrak{p}^{i+1}) = p^f$ for $0 \le i \le d-1$.

It follows that for any choice of values for the variables on the right hand side of (4.4), there exists at most $p^{f\mathbf{lev}(b_{i_1 j_1})}$ choices for each of the $2\alpha(i_1, j_1)$ variables $x_{i_1 i}$ and $x_{j j_1}$ such that the corresponding equation in (4.4) is satisfied. Therefore the number of solutions of the linear system $\mathscr{L}$ is at most

$$p^{fd(|I|-2\alpha(i_1,j_1))+2f\alpha(i_1,j_1)\mathbf{lev}(b_{i_1 j_1})}, \tag{4.5}$$

where $I := \{(i,j) : i \prec j\}$. Using Theorem 4.7(b) it is now straightforward to verify that $\dim \rho_{\mathbf{b}} \ge p^{f(d-\mathbf{lev}(b_{i_1 j_1}))\alpha(i_1,j_1)}$. □

Lemma 4.11. *Let $b = \tilde{b} + \mathfrak{p}^d \in R$. Fix $(i_1, j_1) \in I_{\mathrm{ex}}$ and let $\mathbf{b} := (b_{ij})_{i\prec j}$ where $b_{i_1 j_1} = b$ and $b_{ij} = 0$ for all other pairs (i,j). Then the dimension of the irreducible representation of $\mathscr{G}_R$ that corresponds to the coadjoint orbit of $\psi_{\mathbf{b}} \in \widehat{\mathfrak{g}_R}$ is equal to $q^{(n-\mathbf{lev}(b))\alpha(i_1,j_1)}$.*

Proof. We write the linear system in the proof of Proposition 4.10 explicitly, and determine the number of its solutions. In this case the only nonzero equations in the linear system $\mathscr{L}$ are the L_{ij_1} and the $L_{i_1 j}$ for $i_1 \prec i, j \prec j_1$, and they are of the form $b_{i_1 j_1}x_{i_1 j} = 0$ and $b_{i_1 j_1}x_{ij_1} = 0$. The values of the variables x_{ij_1} and $x_{i_1 j}$ can be chosen independently of each other, and the only restriction is that

$$\mathbf{lev}(x_{i_1 j}), \mathbf{lev}(x_{ij_1}) \ge d - \mathbf{lev}(b_{i_1 j_1}).$$

Thus, for each of these variables there are $p^{f\mathbf{lev}(b_{i_1 j_1})}$ possible values. There is no restriction on the values of the other variables of the linear system and each of them can be chosen arbitrarily, from p^{fd} possible values. Thus the number of solutions of the linear system is equal to (4.5). Since the number of solutions of the linear system is also equal to the cardinality of $\mathrm{Stab}_{\mathfrak{g}_R}(\psi_{\mathbf{b}})$, the assertion of the lemma follows from Theorem 4.7(b). □

In the next lemma we prove that $m_{\text{faithful}}(\mathscr{G}_R) \le \sum_{\ell=0}^{e-1}\sum_{(i,j)\in I_{\mathrm{ex}}} f p^{f(d-\ell)\alpha(i,j)}$.

Lemma 4.12. *The group $\mathscr{G}_R$ has a faithful representation of dimension*

$$\sum_{\ell=0}^{e-1} \sum_{(i,j)\in I_{\mathrm{ex}}} fp^{f(d-\ell)\alpha(i,j)}.$$

Proof. Let $\omega_1, \dots, \omega_f$ be units in $\mathcal{O}$ such that $\{\omega_1+\mathfrak{p}, \dots, \omega_f+\mathfrak{p}\}$ forms a basis for $\mathcal{O}/\mathfrak{p}$ over $\mathbb{F}_p$. Set $\tilde{b}_{k\ell} := \omega_k \varpi^\ell$ and $b_{k\ell} := \tilde{b}_{k\ell} + \mathfrak{p}^e$ for $1 \le k \le f$ and $0 \le \ell \le e-1$. The $b_{k\ell}$ form a basis of the $\mathbb{F}_p$-vector space $\mathcal{O}/\mathfrak{p}^e$. Since $\mathrm{Z}(\mathscr{G}_R) \cong \mathrm{Z}(\mathfrak{g}_{\mathrm{R}})$ as abelian groups, from Remark 4.8 it follows that

$$\widehat{\Omega}_1(\mathrm{Z}(\mathscr{G}_R)) \cong \widehat{\Omega}_1(\mathrm{Z}(\mathfrak{g}_{\mathrm{R}})) = \bigoplus_{(i,j)\in I_{\mathrm{ex}}} \widehat{\Omega}_1(\mathcal{O}/\mathfrak{p}^d). \tag{4.6}$$

Note that $\Omega_1(\mathcal{O}/\mathfrak{p}^d) = \mathfrak{p}^{d-e}/\mathfrak{p}^d$, so that Lemma 4.1 yields an isomorphism of abelian groups $\mathcal{O}/\mathfrak{p}^e \cong \widehat{\Omega}_1(\mathcal{O}/\mathfrak{p}^d)$. Given $i_\circ, j_\circ \in [n]$ such that $i_\circ \prec j_\circ$, we define $\mathbf{b}(i_\circ, j_\circ, k, \ell)$, for $1 \le k \le f$ and $0 \le \ell \le e-1$, to be the vector in $\bigoplus_{i\prec j} \mathcal{O}/\mathfrak{p}^d$ with exactly one nonzero component, at the $(i_\circ, j_\circ)$-position, equal to $\tilde{b}_{k\ell}$.

Since $\mathrm{Z}(\mathfrak{g}_R) \cong \bigoplus_{(i,j)\in I_{\mathrm{ex}}} \mathcal{O}/\mathfrak{p}^d$ (see Remark 4.8), from (4.6) it follows that the restrictions of the characters $\psi_{\mathbf{b}(i_\circ,j_\circ,k,l)}$ to $\mathrm{Z}(\mathscr{G}_R)$ form an $\mathbb{F}_p$-basis of $\widehat{\Omega}_1(\mathrm{Z}(\mathscr{G}_R))$. Let $\rho_{\mathbf{b}(i_\circ,j_\circ,k,\ell)}$ denote the irreducible representation of $\mathscr{G}_R$ that corresponds to the coadjoint orbit of $\psi_{\mathbf{b}(i_\circ,j_\circ,k,\ell)}$ (see Theorem 4.7). Then by Lemma 4.2, the representation

$$\rho := \bigoplus_{\substack{1\le k\le f\\ 0\le \ell\le e-1}} \bigoplus_{(i,j)\in I_{\mathrm{ex}}} \rho_{\mathbf{b}(i,j,k,\ell)}$$

is faithful. The set $\{b_{k\ell} : 1 \le k \le f,\ 0 \le \ell \le e-1\}$ contains exactly f elements of any given level ℓ where $0 \le \ell \le e-1$, and by Lemma 4.11 we have $\dim \rho_{\mathbf{b}(i,j,k,\ell)} = p^{f(d-\ell)\alpha(i,j)}$ for any $(i,j) \in I_{\mathrm{ex}}$. These imply that $\dim \rho = \sum_{\ell=0}^{e-1} \sum_{(i,j)\in I_{\mathrm{ex}}} fq^{(n-\ell)\alpha(i,j)}$. □

Proof of the Theorem 1.5. By Lemma 4.12 it suffices to prove that

$$m_{\mathrm{faithful}}(\mathscr{G}_R) \ge \sum_{\ell=0}^{e-1} \sum_{(i,j)\in I_{\mathrm{ex}}} fp^{f(d-\ell)\alpha(i,j)}.$$

Let ρ be a faithful representation of $\mathscr{G}_R$ of dimension $m_{\mathrm{faithful}}(\mathscr{G}_R)$. By Lemma 4.2(ii) and Remark 4.3, ρ is a direct sum of $N := ef(\#I_{\mathrm{ex}})$ irreducible representations. Thus we can express ρ as

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

where each $\rho_{\psi_{\mathbf{a}_k}}$ is the irreducible representation of $\mathscr{G}_R$ corresponding (according to Theorem 4.7) to the coadjoint orbit of the character $\psi_{\mathbf{a}_k}$ of $\mathfrak{g}_R$ (and $\mathbf{a}_k$ is a vector in $\bigoplus_{i\prec j} \mathcal{O}/\mathfrak{p}^d$). Furthermore, by Theorem 4.7(c) and Lemma 4.2(ii) the restrictions of the $\psi_{\mathbf{a}_k}$ to $\Omega_1(\mathrm{Z}(\mathscr{G}_R))$ form a $\mathbb{Z}/p\mathbb{Z}$-basis of $\widehat{\Omega}_1(\mathrm{Z}(\mathscr{G}_R))$. Since $\Omega_1(\mathcal{O}/\mathfrak{p}^d) = \mathfrak{p}^{d-e}/\mathfrak{p}^d$, Lemma 4.1 implies that $\widehat{\Omega}_1(\mathcal{O}/\mathfrak{p}^d) \cong \mathcal{O}/\mathfrak{p}^e$ as $\mathbb{Z}/p\mathbb{Z}$-vector spaces, from which it follows that the projections of the vectors $\mathbf{a}_k$ onto $\bigoplus_{(i,j)\in I_{\mathrm{ex}}} \mathcal{O}/\mathfrak{p}^e$ form a $\mathbb{Z}/p\mathbb{Z}$-basis. Using Lemma 4.5 we can partition the set $\{\mathbf{a}_k\}_{k=1}^N$ into $\#I_{\mathrm{ex}}$ sets of cadinality ef, say $\{\mathscr{A}_{(r,s)} : (r,s) \in I_{\mathrm{ex}}\}$, such

that the (r,s)-components of the elements of $\mathscr{A}_{(r,s)}$ form a basis of $\mathcal{O}/\mathfrak{p}^e$. To complete the proof, it suffices to verify that

$$\sum_{\mathbf{a}\in\mathscr{A}_{(r,s)}} \dim(\rho_{\psi_{\mathbf{a}}}) \geq f\sum_{\ell=0}^{e-1} p^{f(d-\ell)\alpha(r,s)} \quad \text{for } (r,s)\in I_{\mathrm{ex}}. \tag{4.7}$$

Fix $(r,s)\in I_{\mathrm{ex}}$, and denote the (r,s)-component of any $\mathbf{a}\in\mathscr{A}_{(r,s)}$ by $\mathbf{a}_{(r,s)}$. For $0\leq\ell\leq e-1$ set

$$N_\ell := \#\{\mathbf{a}\in\mathscr{A}_{(r,s)} \,:\, \mathbf{lev}(\mathbf{a}_{(r,s)})=\ell\},$$

where $\mathbf{lev}(\cdot)$ is the level as in Definition 4.9. From Proposition 4.10 it follows that if $\mathbf{lev}(\mathbf{a}_{(r,s)})=\ell$ then $\dim(\rho_{\psi_{\mathbf{a}}})\geq p^{f(d-\ell)\alpha(r,s)}$. This implies that

$$\sum_{\mathbf{a}\in\mathscr{A}_{(r,s)}} \dim(\rho_{\psi_{\mathbf{a}}}) \geq \sum_{\ell=0}^{e-1} N_\ell p^{f(d-\ell)\alpha(r,s)}. \tag{4.8}$$

Note that $\sum_{\ell=0}^{e-1} N_\ell = ef$, and

$$\sum_{k=\ell}^{e-1} N_k \leq \dim_{\mathbb{Z}/p\mathbb{Z}}(\mathfrak{p}^\ell/\mathfrak{p}^e) = (e-\ell)f.$$

Thus by Lemma 4.6 for $m:=e$, $a_\ell := N_\ell/f$ and $x_\ell := p^{f(d-\ell)\alpha(r,s)}$ we obtain

$$\sum_{\ell=0}^{e-1} N_\ell p^{f(d-\ell)\alpha(r,s)} \geq f\sum_{\ell=0}^{e-1} p^{f(d-\ell)\alpha(r,s)}. \tag{4.9}$$

Inequality (4.7) now follows from (4.8) and (4.9). □

5. The faithful dimension in the case $\mathfrak{g} := \mathfrak{m}_{n,c}$

In this section we prove Theorem 1.6. We begin by introducing some notation. Recall that $[n] := \{1,\dots,n\}$ for $n\in\mathbb{N}$. For $k\geq 1$, the set of sequences

$$\mathbf{i} = (i_1,\dots,i_k), \quad i_1,\dots,i_k\in[n]$$

is denoted by $\mathscr{A}(n,k)$. We say that $\mathbf{i}$ is *decreasing* if $i_1\geq\cdots\geq i_k$. The set of decreasing sequences in $\mathscr{A}(n,k)$ is denoted by $\mathscr{D}(n,k)$. There is an obvious sorting map

$$^-\colon \mathscr{A}(n,k)\to\mathscr{D}(n,k).$$

For example $\overline{(5,4,4,2,3,1)} = (5,4,4,3,2,1)$. We say that $\mathbf{i}\in\mathscr{A}(n,k)$ is a *Hall sequence* if the initial sequence $(i_1,\dots,i_{k-1})$ is decreasing and $i_{k-1}<i_k$ (by convention, every element of $\mathscr{A}(n,1)$ is a Hall sequence). The subset of Hall sequences in $\mathscr{A}(n,k)$ is denoted by $\mathscr{H}(n,k)$.

Lemma 5.1. (a) *For $n,k\geq 1$ we have* $\#\mathscr{D}(n,k) = \binom{n+k-1}{k}$.

(b) *For $n\geq 2$ and $k\geq 2$ we have*

$$\#\mathscr{H}(n,k) = \sum_{m=1}^{n-1} m\binom{k+m-2}{k-2} = (k-1)\binom{k+n-2}{k}.$$

Proof. For part (a), note that cardinality of $\mathscr{D}(n,k)$ is equal to the number of solutions of the equation $t_1+\cdots+t_n=k$ in non-negative integers, where $t_j=\#\{\ell\in[k]:i_\ell=j\}$.

For part (b), fix $n,k\geq 2$ and for $m\in[n-1]$ denote by A_m the subset of $\mathscr{H}(n,k)$ consisting of those sequences $(i_1,\dots,i_k)\in\mathscr{H}(n,k)$ such that $i_{k-1}=m$. Note that since $i_{k-1}<i_k\leq n$, we must have $i_{k-1}\in[n-1]$. Once m is fixed, there are $n-m$ options left for i_k. Moreover, the sequence $(i_1,\dots,i_{k-1})$ can be any decreasing sequence in $[n]$ for which $i_{k-1}=m$. Using the map $(i_1,\dots,i_{k-2})\mapsto(i_1-m+1,\dots,i_{k-2}-m+1)$ these sequences stand in one-to-one correspondence with elements of the set $\mathscr{D}(n-m+1,k-2)$, whose cardinality by part (a) is equal to $\binom{n-m+k-2}{k-2}$. Since the two choices can be made independently of each other we have

$$\#\mathscr{H}(n,k)=\sum_{m=1}^{n-1}(n-m)\binom{n-m+k-2}{k-2}.$$

Replacing m by $n-m$ in this expression yields the first equality in part (b). For the second equality note that

$$\sum_{m=1}^{n-1}m\binom{k+m-2}{k-2}=\sum_{m=1}^{n-1}(k-1)\binom{k+m-2}{k-1}=(k-1)\sum_{m=1}^{n-1}\binom{k+m-2}{k-1},$$

and $\sum_{m=1}^{n-1}\binom{k+m-2}{k-1}$ counts the number of subsets of size k of $[k+n-2]$, where the summand $\binom{k+m-2}{k-1}$ corresponds to subsets of $[k+n-2]$ with maximum equal to $k+m-1$. □

Since $\mathfrak{f}_{n,2}=\mathfrak{m}_{n,2}$, the case $c=2$ of Theorem 1.6 follows from [BMKS16, Theorem 2.13]. Thus from now on we assume that $c\geq 3$. We denote the standard generators of $\mathfrak{m}_{n,c}$ by $X_n:=\{\mathsf{v}_i:i\in[n]\}$. For each k-tuple $\mathbf{i}=(i_1,\dots,i_k)\in\mathscr{A}(n,k)$, write

$$\mathsf{v}_{\mathbf{i}}:=[\mathsf{v}_{i_1},[\mathsf{v}_{i_2},\dots,[\mathsf{v}_{i_{k-1}},\mathsf{v}_{i_k}]\dots].$$

Set $\mathscr{H}^{\leq c-1}:=\bigcup_{j=1}^{c-1}\mathscr{H}(n,j)$ and $\mathscr{H}^{\geq 2}:=\bigcup_{j=2}^{c}\mathscr{H}(n,j)$.

Lemma 5.2. *Let n and c be as above. For each $1\leq j\leq c$, the set $\{\mathsf{v}_{\mathbf{i}}:\mathbf{i}\in\mathscr{H}(n,j)\}$ is a basis for the vector space $\mathfrak{m}_{n,c}^j/\mathfrak{m}_{n,c}^{j+1}$. In particular,*

(a) *$\{\mathsf{v}_{\mathbf{i}}:\mathbf{i}\in\mathscr{H}(n,c)\}$ forms a basis for $\mathrm{Z}(\mathfrak{m}_{n,c})$.*
(b) *Elements in $\left\{\mathsf{v}_{\mathbf{i}}:\mathbf{i}\in\mathscr{H}^{\leq c-1}\right\}$ represent a basis of $\mathfrak{m}_{n,c}/\mathrm{Z}(\mathfrak{m}_{n,c})$.*
(c) *Elements in $\left\{\mathsf{v}_{\mathbf{i}}:\mathbf{i}\in\mathscr{H}^{\geq 2}\right\}$ form a basis for $[\mathfrak{m}_{n,c},\mathfrak{m}_{n,c}]$.*

Proof. This is well known. See [ABRdS18] for a proof. □

In the sequel, we will carry out a close study of the commutator matrix of $\mathfrak{m}_{n,c}$ with respect to the bases for $\mathfrak{m}_{n,c}/\mathrm{Z}(\mathfrak{m}_{n,c})$ and $[\mathfrak{m}_{n,c},\mathfrak{m}_{n,c}]$ described in Lemma 5.2. For $\mathbf{i},\mathbf{j}\in\mathscr{H}^{\leq c-1}$ let $\lambda_{\mathbf{ij}}^{\mathbf{k}}\in\mathbb{Z}$ be the structural constants defined by

$$[\mathsf{v}_{\mathbf{i}},\mathsf{v}_{\mathbf{j}}]=\sum_{\mathbf{k}\in\mathscr{H}^{\geq 2}}\lambda_{\mathbf{ij}}^{\mathbf{k}}\mathsf{v}_{\mathbf{k}}.$$

Let $\mathbf{T}:=(T_{\mathbf{i}})_{\mathbf{i}\in\mathscr{H}^{\geq 2}}$ be a vector of variables, and for $\mathbf{i},\mathbf{j}\in\mathscr{H}^{\leq c-1}$, define the linear forms

$$\Lambda_{\mathbf{ij}}(\mathbf{T}):=\sum_{\mathbf{k}\in\mathscr{H}^{\geq 2}}\lambda_{\mathbf{ij}}^{\mathbf{k}}T_{\mathbf{k}}.$$

The commutator matrix of $\mathfrak{g}$ relative to the chosen bases is the $N \times N$ skew-symmetric matrix of linear forms given by

$$F_{\mathfrak{g}}(\mathbf{T}) := [\Lambda_{\mathbf{ij}}(\mathbf{T})]_{\mathbf{i},\mathbf{j}\in\mathscr{H}^{\leq c-1}}, \quad \text{where } N := \#\mathscr{H}^{\leq c-1}.$$

For any $(i_1,\dots,i_c) \in \mathscr{H}(n,c)$, set $\mathbf{i} := (i_1)$ and $\mathbf{j} := (i_2,\dots,i_c) \in \mathscr{H}(n,c-1)$. Then the $(\mathbf{i},\mathbf{j})$ entry of $F_{\mathfrak{g}}(\mathbf{T})$ is equal to $T_{(i_1,\dots,i_c)}$. Further, for any $\mathbf{i} := (i_1,\dots,i_k)$ and $\mathbf{j} := (j_1,\dots,j_l)$, we have $\Lambda_{\mathbf{ij}} = 0$ unless $\min(k,l) = 1$.

Lemma 5.3. *Let $\mathbf{i} := (i_1) \in \mathscr{H}(n,1)$ and $\mathbf{j} := (i_2,\dots,i_c) \in \mathscr{H}(n,c-1)$. Then*

$$\Lambda_{\mathbf{ij}}(\mathbf{T}) = \begin{cases} T_{\overline{(i_1,\dots,i_{c-1}},i_c)} & \text{if } i_1 \geq i_{c-1}, \\ T_{(i_2,\dots,i_{c-1},i_1,i_c)} - T_{\overline{(i_2,\dots,i_{c-2},i_c}},i_1,i_{c-1)} & \text{if } i_1 < i_{c-1}. \end{cases}$$

Proof. First observe that for $a, a' \in \mathfrak{m}_{n,c}$ and $a'' \in [\mathfrak{m}_{n,c}, \mathfrak{m}_{n,c}]$ we have

$$[a,[a',a'']] = [a',[a,a'']], \tag{5.1}$$

because $[a,[a',a'']] = -[a',[a'',a]] - [a'',[a,a']] = [a',[a,a'']]$, where the second equality follows from the fact that $\mathfrak{m}_{n,c}$ is metabelian and a'' is a commutator.

Suppose that $i_1 \geq i_{c-1}$, and let $2 \leq r \leq c-1$ be the smallest integer with $i_1 \geq i_r$. By the assumption such an r exists. If $c = 3$, then we must have $r = 2$, hence $i_1 \geq i_2$. Thus $(i_1,i_2,i_3) \in \mathscr{H}(n,3)$, hence $[\mathsf{v}_{i_1}, \mathsf{v}_{(i_2,i_3)}] = [\mathsf{v}_{i_1},[\mathsf{v}_{i_2},\mathsf{v}_{i_3}]] = \mathsf{v}_{(i_1,i_2,i_3)}$, from which it follows that $\Lambda_{\mathbf{ij}}(\mathbf{T}) = \Lambda_{(i_1),(i_2,i_3)}(\mathbf{T}) = T_{(i_1,i_2,i_3)}$.

For $c > 3$, set $\eta_k := [\mathsf{v}_{i_k},[\mathsf{v}_{i_{k+1}},\dots,[\mathsf{v}_{i_{c-1}},\mathsf{v}_{i_c}]\dots]$. It follows from (5.1) that

$$[\mathsf{v}_{i_1},[\mathsf{v}_{i_2},\dots,[\mathsf{v}_{i_{c-1}},\mathsf{v}_{i_k}]\dots] = [\mathsf{v}_{i_1},[\mathsf{v}_{i_2},\eta_3]] = [\mathsf{v}_{i_2},[\mathsf{v}_{i_1},\eta_3]].$$

By repeating this process, we can keep swapping v_{i_1} with subsequent terms $\mathsf{v}_{i_3},\dots$ until we arrive at v_{i_r} where the process is terminated. Note that

$$(i_2,\dots,i_{r-1},i_1,i_r,\dots,i_{c-1}) = \overline{(i_1,\dots,i_c)}.$$

This proves the lemma for the case $i_1 \geq i_{c-1}$.

Let us now consider the case $i_1 < i_{c-1}$. In this case, the process described above can be continued all the way until v_{i_1} arrives in the innermost commutator, that is,

$$[\mathsf{v}_{i_1},[\mathsf{v}_{i_2},\dots,[\mathsf{v}_{i_{c-1}},\mathsf{v}_{i_k}]\dots] = [\mathsf{v}_{i_2},[\mathsf{v}_{i_3},\dots,[\mathsf{v}_{i_{c-2}},[\mathsf{v}_{i_1},[\mathsf{v}_{i_{c-1}},\mathsf{v}_{i_c}]]\dots].$$

We can now use the Jacobi identity to write $[\mathsf{v}_{i_1},[\mathsf{v}_{i_{c-1}},\mathsf{v}_{i_c}]] = [\mathsf{v}_{i_{c-1}},[\mathsf{v}_{i_1},\mathsf{v}_{i_c}]] - [\mathsf{v}_{i_c},[\mathsf{v}_{i_1},\mathsf{v}_{i_{c-1}}]]$. Similar to the previous case, by a repeated application of (5.1) we can move v_{i_c} inside to the location so that the resulting sequence is decreasing. This proves the claim. □

From now on we set $\widetilde{F}_{\mathfrak{g}}(\mathbf{T})$ to be equal to the submatrix of $F_{\mathfrak{g}}(\mathbf{T})$ that lies in the intersection of rows $\mathbf{i} \in \mathscr{H}(n,1)$ and columns $\mathbf{j} \in \mathscr{H}(n,c-1)$. We remark that the only variables that appear in the entries of $\widetilde{F}_{\mathfrak{g}}(\mathbf{T})$ are the $T_{\mathbf{i}}$ for $\mathbf{i} \in \mathscr{H}(n,c)$.

Lemma 5.4. *Let K be any field and fix scalars $\alpha_i, \lambda_j \in K$ for $1 \leq i \leq n$ and $0 \leq j \leq n-1$. For each $\mathbf{i} := (i_1,\dots,i_c) \in \mathscr{H}(n,c)$ set*

$$T_{\mathbf{i}} := \left(\prod_{k=1}^{c-2} \alpha_{i_k}\right) \begin{vmatrix} \alpha_{i_{c-1}} & \alpha_{i_c} \\ \lambda_{i_{c-1}-1} & \lambda_{i_c-1} \end{vmatrix}. \tag{5.2}$$

Set $\mathbf{T} := (T_{\mathbf{i}})_{\mathbf{i}\in\mathscr{H}(n,c)}$. Then the matrix $\widetilde{F}_{\mathfrak{g}}(\mathbf{T})$ has rank at most 1.

Proof. First we show that for every $\mathbf{i} := (i_1) \in \mathscr{H}(n,1)$ and $\mathbf{j} := (i_2, \dots, i_c) \in \mathscr{H}(n, c-1)$,

$$\widetilde{F}_{\mathfrak{g}}(\mathbf{T})_{\mathbf{ij}} = \left(\prod_{k=1}^{c-2} \alpha_{i_k}\right) \begin{vmatrix} \alpha_{i_{c-1}} & \alpha_{i_c} \\ \lambda_{i_{c-1}-1} & \lambda_{i_c-1} \end{vmatrix}. \tag{5.3}$$

We consider two different cases. If $i_1 \geq i_{c-1}$, then it follows from Lemma 5.3 that

$$\Lambda_{\mathbf{ij}}(\mathbf{T}) = T_{(\overline{i_1,\dots,i_{c-1}},i_c)}.$$

Since the sequence $(i_2, \dots, i_{c-1})$ is decreasing, and $i_1 \geq i_{c-1}$, it follows that i_{c-1} is also the least element of $(\overline{i_1, \dots, i_{c-1}}, i_c)$ and hence the first $c-2$ terms of $(\overline{i_1, \dots, i_{c-1}}, i_c)$ are precisely $i_1, \dots, i_{c-2}$, perhaps in a different order. Thus (5.3) follows from the fact that the last two terms of the sequence are i_{c-1} and i_c, in the same order.

If $i_1 < i_{c-1}$, then it follows from Lemma 5.3 that

$$\Lambda_{\mathbf{ij}}(\mathbf{T}) = T_{(i_2,\dots,i_{c-1},i_1,i_c)} - T_{(\overline{i_2,\dots,i_{c-2},i_c},i_1,i_{c-1})}.$$

Since both $(i_2, \dots, i_{c-1}, i_1, i_c)$ and $(\overline{i_2, \dots, i_{c-2}, i_c}, i_1, i_{c-1})$ are Hall sequences, we have

$$\begin{aligned} \Lambda_{\mathbf{ij}}(\mathbf{T}) &= \alpha_{i_{c-1}} \cdot \left(\prod_{k=2}^{c-2} \alpha_{i_k}\right) \cdot \begin{vmatrix} \alpha_{i_1} & \alpha_{i_c} \\ \lambda_{i_1-1} & \lambda_{i_c-1} \end{vmatrix} - \alpha_{i_c} \cdot \left(\prod_{k=2}^{c-2} \alpha_{i_k}\right) \cdot \begin{vmatrix} \alpha_{i_1} & \alpha_{i_{c-1}} \\ \lambda_{i_1-1} & \lambda_{i_{c-1}-1} \end{vmatrix} \\ &= \left(\prod_{k=2}^{c-2} \alpha_{i_k}\right) \cdot \left(\alpha_{i_{c-1}} \cdot \begin{vmatrix} \alpha_{i_1} & \alpha_{i_c} \\ \lambda_{i_1-1} & \lambda_{i_c-1} \end{vmatrix} - \alpha_{i_c} \cdot \begin{vmatrix} \alpha_{i_1} & \alpha_{i_{c-1}} \\ \lambda_{i_1-1} & \lambda_{i_{c-1}-1} \end{vmatrix}\right) \end{aligned} \tag{5.4}$$

After applying the elementary identity

$$r' \begin{vmatrix} q & r \\ s & t \end{vmatrix} - r \begin{vmatrix} q & r' \\ s & t' \end{vmatrix} = q \begin{vmatrix} r' & r \\ t' & t \end{vmatrix}$$

to the expression on the right hand side and merging the prefactor $q := \alpha_{i_1}$ with the product $\prod_{k=2}^{c-2} \alpha_{i_k}$ we obtain (5.3). From (5.3) it follows that for $\mathbf{i} := (i_1) \in \mathscr{H}(n,1)$ and $\mathbf{j} := (i_2, \dots, i_c) \in \mathscr{H}(n, c-1)$, we have $\widetilde{F}_{\mathfrak{g}}(\mathbf{T})_{\mathbf{ij}} = \alpha_{i_1}\beta_{\mathbf{j}}$ for some $\beta_{\mathbf{j}} \in K$. Thus $\widetilde{F}_{\mathfrak{g}}(\mathbf{T})$ is expressible as the product of the column vector $(\alpha_i)_{i \in \mathscr{H}(n,1)}$ and the row vector $(\beta_{\mathbf{j}})_{\mathbf{j} \in \mathscr{H}(n,c-1)}$, so that $\mathrm{rk}(\widetilde{F}_{\mathfrak{g}}(\mathbf{T})) \leq 1$. □

Example 5.5. *We compute $\widetilde{F}_{\mathfrak{g}}(\mathbf{T})$ for $\mathfrak{g} := \mathfrak{m}_{3,3}$ using Lemma 5.3. The rows are indexed by $(1), (2), (3) \in \mathscr{H}(3,1)$ and the columns are indexed by $(1,2), (1,3), (2,3) \in \mathscr{H}(3,2)$. Thus*

$$\widetilde{F}_{\mathfrak{g}}(\mathbf{T}) = \begin{pmatrix} T_{(112)} & T_{(113)} & T_{(213)} - T_{(312)} \\ T_{(212)} & T_{(213)} & T_{(223)} \\ T_{(312)} & T_{(313)} & T_{(323)} \end{pmatrix}.$$

Lemma 5.6. *Suppose $r, m, \delta \geq 1$. Let K be any field.*

(a) *Suppose $f \in K[x_1, \dots, x_m]$ is a polynomial in m variables over K such that the degree of f as a polynomial in x_i is at most δ_i for all $1 \leq i \leq m$. Assume that $\#K \geq 1 + \max(\delta_1, \dots, \delta_m)$, and $f(x_1, \dots, x_m) = 0$ for all $(x_1, \dots, x_m) \in K^m$. Then f is the zero polynomial.*

(b) *Suppose $f_1, \dots, f_r \in K[x_1, \dots, x_m]$, and the degree of each one of $f_1, \dots, f_r$ in the variable x_i is at most δ_i for $1 \leq i \leq m$. Let $f : K^m \to K^r$ be the polynomial map defined by $f = (f_1, \dots, f_r)$. Assume that the K-subspace of $K[x_1, \dots, x_m]$ spanned by $f_1, \dots, f_r$ has dimension at least δ. If $\#K \geq 1 + \max(\delta_1, \dots, \delta_m)$, then there exist $u_1, \dots, u_\delta \in K^m$ for which $f(u_1), \dots, f(u_\delta)$ are linearly independent vectors in K^r.*

Proof. Part (a) follows by induction on m. For $m = 1$, the statement is clear. Assuming that (a) holds for $m-1$, write $f(x_1, \dots, x_m) := \sum_{i=0}^{\delta_m} c_i x_m^i$ where the $c_i \in K[x_1, \dots, x_{m-1}]$. Fix $(x_1, \dots, x_{m-1}) \in K^{m-1}$ and consider the one-variable polynomial

$$g(x_m) := f(x_1, \dots, x_{m-1}, x_m).$$

Since $g(x_m) = 0$ for all $x_m \in K$, and $\#K > \deg g$, it follows that all the coefficients of g vanish. The claim follows by the induction hypothesis applied to the c_i.

For (b) by choosing a maximal linearly independent subset of $f_1, \dots, f_r$, we can assume that $\delta = r$. Thus the goal is to find $u_1, \dots, u_r \in K^m$ for which $f(u_1), \dots, f(u_r)$ are linearly independent vectors in K^r. If this is not the case, then the image of f must lie in a proper subspace of K^r. This implies that there exists a non-zero vector $(c_1, \dots, c_r) \in K^r$ such that $c_1 f_1(u) + \cdots + c_r f_r(u) = 0$ for all $u \in K^m$. By part (a), this implies that the polynomial $c_1 f_1 + \cdots + c_r f_r$ is the zero polynomial, which is a contradiction. □

We are now ready to prove Theorem 1.6 in the case where R is a finite field. In this case, we need to show that for p sufficiently large we have

$$m_{\text{faithful}}(\mathscr{G}_{\mathbb{F}_q}) = (c-1)\binom{n+c-2}{c} fq \qquad \text{for all } f \geq 1, \tag{5.5}$$

where $q := p^f$. Recall that T_i is chosen as in (5.2). We set $\lambda_0 := 0$ and $\lambda_1 := 1$. Then the entries of $\widetilde{F}_{\mathfrak{g}}$ are polynomials in variables $\alpha_1, \dots, \alpha_n$ and $\lambda_2, \dots, \lambda_{n-1}$. Thus $\widetilde{F}_{\mathfrak{g}}$ takes values in the vector space of matrices of size $n \times \#\mathscr{H}(n, c-1)$ with entries in the ring $\mathbb{F}_q[\alpha_1, \dots, \alpha_n, \lambda_2, \dots, \lambda_{n-1}]$. First we prove the following claim:

The set $\{T_{\mathbf{i}}\}_{\mathbf{i} \in \mathscr{H}(n,c)}$ is linearly independent in $\mathbb{F}_q[\alpha_1, \dots, \alpha_n, \lambda_2, \dots, \lambda_{n-1}]$.

To prove this claim suppose that

$$\sum_{\mathbf{i} \in \mathscr{H}(n,c)} c_{\mathbf{i}} \cdot \left(\prod_{k=1}^{c-2} \alpha_{i_k} \right) \cdot \begin{vmatrix} \alpha_{i_{c-1}} & \alpha_{i_c} \\ \lambda_{i_{c-1}-1} & \lambda_{i_c-1} \end{vmatrix} = 0,$$

for some coefficients $c_{\mathbf{i}} \in \mathbb{F}_q$. We will show that all the coefficients must be zero. For each such linear dependence, define r to be the largest value of i_c for which there exists $\mathbf{i} = (i_1, \dots, i_c) \in \mathscr{H}(n, c)$ such that $c_{\mathbf{i}} \neq 0$. Note that clearly $r \geq 2$. First suppose that $r = 2$. This implies that $i_{c-1} = 1$ and hence the linear dependence equation simplifies to

$$\sum_{(i_1, \dots, i_{c-2}) \in \mathscr{D}(n, c-2)} c_{(i_1, \dots, i_{c-2}, 1, 2)} \prod_{k=1}^{c-1} \alpha_{i_k} = 0.$$

Consider a monomial $g := \alpha_{i_1} \cdots \alpha_{i_{c-1}}$ that appears in the above linear combination. Then $\deg_{\alpha_i}(g) = \#\{j : 1 \leq j \leq c-1 \text{ and } i_j = i\}$. Since the sequence $(i_1, \dots, i_{c-1})$ is decreasing, the sequence $(\deg_{\alpha_1}(g), \dots, \deg_{\alpha_n}(g))$ uniquely determines the values $i_1, \dots, i_{c-2}$, hence uniquely determines g as well. Thus the monomials in the above linear combination have distinct degree sequences and therefore there is no possibility of cancellation between them. Next suppose that $r \geq 3$. This implies that there are some monomials involving λ_{r-1} and that there are no terms involving λ_j for $j > r-1$. It is also clear that the only terms involving λ_{r-1} correspond to those sequences $(i_1, \dots, i_c)$ for which $i_c = r$ and hence these terms are of the form

$$\prod_{k=1}^{c-2} \alpha_{i_k} (\alpha_{i_{c-1}} \lambda_{r-1} - \alpha_r \lambda_{i_{c-1}-1}).$$

By considering only the terms involving λ_{r-1} we obtain

$$\sum_{(i_1,\dots,i_{c-1})\in\mathscr{D}(n-1,c-1),i_{c-1}<r} c_{\mathbf{i}}\prod_{k=1}^{c-1}\alpha_{i_k}=0.$$

As in the previous case the monomials corresponding to different $\mathbf{i}$ are distinct, and hence this can only happen if $c_{\mathbf{i}}=0$ for all such terms. This contradicts the choice of r. This completes the proof of linear independence of the $\{T_{\mathbf{i}}\}_{\mathbf{i}\in\mathscr{H}(n,c)}$.

Next set $f:=\widetilde{F}_{\mathfrak{g}}(\mathbf{T}')$ in Lemma 5.6(b), where $\mathbf{T}':=(T_{\mathbf{i}})_{\mathbf{i}\in\mathscr{H}(n,c)}$. Note that the components of f are the entries of $\widetilde{F}_{\mathfrak{g}}(\mathbf{T}')$ which are polynomials in the α_i and the λ_i. Furthermore, for every $\mathbf{i}:=(i_1,\dots,i_c)\in\mathscr{H}(n,c)$ if we set $\mathbf{i}':=(i_1)$ and $\mathbf{j}':=(i_2,\dots,i_c)$ then by Lemma 5.3 we have $\widetilde{F}_{\mathfrak{g}}(\mathbf{T})_{\mathbf{i}'\mathbf{j}'}=T_{\mathbf{i}}$. From linear independence of the set $\{T_{\mathbf{i}}\}_{\mathbf{i}\in\mathscr{H}(n,c)}$ and Lemma 5.6(b) it follows that for $q\geq c$ one can find $\#\mathscr{H}(n,c)$ linearly independent vectors $\mathbf{T}':=(T_{\mathbf{i}})_{\mathbf{i}\in\mathscr{H}(n,c)}$ with entries in $\mathbb{F}_q$ for which the values $\widetilde{F}_{\mathfrak{g}}(\mathbf{T}')$ are linearly independent. By Lemma 5.4 it follows that $\mathrm{rk}(\widetilde{F}_{\mathfrak{g}}(\mathbf{T}'))=1$ for all such $\mathbf{T}'$. We can extend each such vector $\mathbf{T}'$ to a vector $\mathbf{T}:=(T_{\mathbf{i}})_{\mathbf{i}\in\mathscr{H}^{\geq 2}}$ by setting $T_{\mathbf{i}}=0$ for $\mathbf{i}\in\mathscr{H}(n,k)$, where $2\leq k\leq c-1$. For the latter vectors $\mathbf{T}$ we have $\mathrm{rk}_{\mathbb{F}_q}(F_{\mathfrak{g}}(\mathbf{T}))=2$. Since $F_{\mathfrak{g}}$ is skew symmetric and each variable $T_{\mathbf{i}}$ where $\mathbf{i}:=(i_1,\dots,i_k)$ appears in the $(\mathbf{i}',\mathbf{j})$-entry of $F_{\mathfrak{g}}(\mathbf{T})$, where $\mathbf{i}':=(i_1)$ and $\mathbf{j}:=(i_2,\dots,i_k)$, we have $\mathrm{rk}_{\mathbb{F}_q}(F_{\mathfrak{g}}(\mathbf{T}))\geq 2$ whenever $\mathbf{T}\neq 0$. In view of Theorem 2.6 this proves the assertion in the case that R is a finite field.

Let us now consider the case where $R=\mathcal{O}/\mathfrak{p}^d$. Using Theorem 1.3 and equality (5.5) which was just proved, the upper bound follows immediately. Let us now turn to establishing the lower bound. We start with the following lemma. Recall the notion of level of an element of $\mathcal{O}/\mathfrak{p}^d$ from Definition 4.9.

Lemma 5.7. *Let B be an $r\times r$ skew-symmetric matrix with entries in $\mathcal{O}/\mathfrak{p}^d$. Suppose B has an entry of level ℓ. Then*

$$\#\ker B\leq p^{fd(r-2)+2f\ell}.$$

Proof. Write $B=(B_{ij})_{1\leq i,j\leq r}$. If $\ell=d$, there is nothing to prove. Next assume that the entry in question is non-zero, and hence non-diagonal. After possibly permuting rows and columns, we can assume that $\mathbf{lev}(B_{12})=\ell$. Consider a vector $(x_1,\dots,x_r)\in(\mathcal{O}/\mathfrak{p}^d)^{\oplus r}$ in $\ker B$. Then the following equations hold:

$$B_{12}x_2=-\sum_{j=3}^{r}B_{1j}x_j\quad\text{and}\quad B_{21}x_1=-\sum_{j=3}^{r}B_{2j}x_j.$$

Once the values of the x_j for $3\leq j\leq r$ are set, the number of choices for each one of x_1 and x_2 is $p^{f\ell}$. Since the number of choices for $(x_3,\dots,x_r)$ is $p^{fd(r-2)}$, the claim follows immediately. □

In order to avoid confusion with parameters n and c of $\mathfrak{m}_{n,c}$, henceforth we will denote the parameters l_1,l_2,n,m that were associated to $\mathfrak{g}$ in Section 2 by $\underline{l}_1,\underline{l}_2,\underline{n},\underline{m}$. Thus in particular we have

$$\underline{m}=\#\mathscr{H}^{\geq 2}\quad,\quad \underline{l}_1=\#\mathscr{H}(n,c)=(c-1)\binom{n+c-2}{c}\quad\text{and}\quad \underline{l}_2=0.$$

Moreover, the commutator matrix $F_{\mathfrak{g}}(\mathbf{T})$ is an $\underline{n}\times\underline{n}$ matrix with $\underline{n}=\mathrm{rk}_{\mathbb{Z}}(\mathfrak{m}_{n,c})-\underline{l}_1$.

Lemma 5.8. *Let* $\mathbf{a} := (\mathbf{a}(\mathbf{i}))_{\mathbf{i}\in\mathscr{H}^{\geq 2}} \in (\mathcal{O}/\mathfrak{p}^d)^{\oplus \underline{m}}$. *Then*

$$\#\ker_{\mathcal{O}/\mathfrak{p}^d} F_{\mathfrak{g}}(\mathbf{a}) \leq \min_{\mathbf{i}\in\mathscr{H}(n,c)} p^{fd(\underline{n}-2)+2f\mathbf{lev}(\mathbf{a}(\mathbf{i}))}.$$

Proof. By Lemma 5.2 we have $\underline{n} = \sum_{j=1}^{c-1} \#\mathscr{H}(n,j)$ and the rows and columns of $F_{\mathfrak{g}}(\mathbf{a})$ are indexed by elements of $\mathscr{H}^{\leq c-1} = \bigcup_{j=1}^{c-1} \mathscr{H}(n,j)$. Now fix any $\mathbf{i}', \mathbf{j}' \in \mathscr{H}^{\leq c-1}$. By Lemma 5.7 for $B := F_{\mathfrak{g}}(\mathbf{a})$, $r := \underline{n}$, and $\ell := \mathbf{lev}(F_{\mathfrak{g}}(\mathbf{a})_{\mathbf{i}'\mathbf{j}'})$ we have

$$\#\ker_{\mathcal{O}/\mathfrak{p}^d} F_{\mathfrak{g}}(\mathbf{a}) \leq p^{fd(\underline{n}-2)+2f\mathbf{lev}(F_{\mathfrak{g}}(\mathbf{a})_{\mathbf{i}'\mathbf{j}'})}.$$

In particular, if for any $\mathbf{i} \in \mathscr{H}(n,c)$ we set $\mathbf{i}' := (i_1)$ and $\mathbf{j}' := (i_2, \dots, i_c)$ then by Lemma 5.3 we obtain $\#\ker_{\mathcal{O}/\mathfrak{p}^d} F_{\mathfrak{g}}(\mathbf{a}) \leq p^{fd(\underline{n}-2)+2f\mathbf{lev}(\mathbf{a}(\mathbf{i}))}$. Finally, by taking the minimum over all $\mathbf{i} \in \mathscr{H}(n,c)$ we obtain the assertion of the lemma. □

Let $S = \{\mathbf{a}_1, \dots, \mathbf{a}_{fel_1}\} \subseteq (\mathcal{O}/\mathfrak{p}^d)^{\oplus \underline{m}}$ be a set of vectors that corresponds to $m_{\text{faithful}}(\mathscr{G}_R)$ in Proposition 3.2 (thus we assume that p is sufficiently large accordingly). Let $\pi_{\mathbf{i}}$ for $\mathbf{i} \in \mathscr{H}(n,c)$ denote the natural projection

$$\bigoplus_{\mathbf{i}\in\mathscr{H}(n,c)} (\mathcal{O}/\mathfrak{p}^e) \to \mathcal{O}/\mathfrak{p}^e,$$

that maps $\mathbf{a}$ to $\mathbf{a}(\mathbf{i})$. Using Lemma 4.5, we partition S into sets $S_{\mathbf{i}}$, each of cardinality ef, such that $\pi_{\mathbf{i}}(\mathsf{proj}(S_{\mathbf{i}}))$ is a basis for the $\mathbb{F}_p$-vector space $\mathcal{O}/\mathfrak{p}^e$. By Lemma 5.8 we have

$$\begin{aligned} m_{\text{faithful}}(\mathscr{G}_R) &= \sum_{i=1}^{fel_1} \left(\frac{p^{fd\underline{n}}}{\#\ker_{\mathcal{O}/\mathfrak{p}^d}(F_{\mathfrak{g}}(\mathbf{a}_i))}\right)^{\frac{1}{2}} \\ &= \sum_{\mathbf{i}\in\mathscr{H}(n,c)} \sum_{\mathbf{a}\in S_{\mathbf{i}}} \left(\frac{p^{fd\underline{n}}}{\#\ker_{\mathcal{O}/\mathfrak{p}^d}(F_{\mathfrak{g}}(\mathbf{a}))}\right)^{\frac{1}{2}} \geq \sum_{\mathbf{i}\in\mathscr{H}(n,c)} \sum_{\mathbf{a}\in S_{\mathbf{i}}} p^{f(d-\mathbf{lev}(\mathbf{a}(\mathbf{i})))}. \end{aligned} \tag{5.6}$$

Recall that for every $0 \leq \ell \leq e-1$, the set of $x \in (\mathcal{O}/\mathfrak{p}^e)$ with $\mathbf{lev}(x) \geq \ell$ is an $\mathbb{F}_p$-subspace of dimension $f(e-\ell)$. Let us call this subspace $\mathcal{W}_\ell$. Fix $\mathbf{i} \in \mathscr{H}(n,c)$, and set $a_\ell = \frac{1}{f}\#\{\mathbf{a} \in S_{\mathbf{i}} : \mathbf{lev}(\mathbf{a}(\mathbf{i})) = \ell\}$. Since $\{\pi_{\mathbf{i}}(\mathsf{proj}(\mathbf{a})) : \mathbf{a} \in S_{\mathbf{i}}\}$ is a basis for $\mathcal{O}/\mathfrak{p}^e$, it follows that for every $0 \leq \ell \leq e-1$, the set of $\mathbf{a} \in S_{\mathbf{i}}$ with $\mathbf{lev}(\mathbf{a}(\mathbf{i})) \geq \ell$ is a linearly independent subset of $\mathcal{W}_\ell$. Thus, the cardinality of the latter set of vectors is at most $\dim \mathcal{W}_\ell = f(e-\ell)$. Hence $a_\ell + \cdots + a_{e-1} \leq e - \ell$ for all $0 \leq \ell \leq e-1$. Using Lemma 4.6 for $m = e$ and $x_\ell = p^{f(d-\ell)}$, where $0 \leq \ell \leq e-1$, we deduce

$$\frac{1}{f}\sum_{\mathbf{a}\in S_{\mathbf{i}}} p^{f(d-\mathbf{lev}(\mathbf{a}(\mathbf{i})))} = \sum_{\ell=0}^{e-1} a_\ell x_\ell \geq \sum_{\ell=0}^{e-1} x_\ell = \sum_{\ell=0}^{e-1} p^{f(d-\ell)}. \tag{5.7}$$

Equivalently, $\sum_{\mathbf{a}\in S_{\mathbf{i}}} p^{f(d-\mathbf{lev}(\mathbf{a}(\mathbf{i})))} \geq f\sum_{\ell=0}^{e-1} p^{f(d-\ell)}$. The assertion of Theorem 1.6 follows immediately from combining (5.6) and (5.7).

References

[ABRdS18] Menny Aka, Emmanuel Breuillard, Lior Rosenzweig, and Nicolas de Saxcé, *Diophantine approximation on matrices and Lie groups*, Geom. Funct. Anal. **28** (2018), no. 1, 1–57. MR 3777412

[AK65] James Ax and Simon Kochen, *Diophantine problems over local fields. I*, Amer. J. Math. **87** (1965), 605–630. MR 184930

[AKOV13] Nir Avni, Benjamin Klopsch, Uri Onn, and Christopher Voll, *Representation zeta functions of compact p-adic analytic groups and arithmetic groups*, Duke Math. J. **162** (2013), no. 1, 111–197. MR 3011874

[Ax67] James Ax, *Solving diophantine problems modulo every prime*, Ann. of Math. (2) **85** (1967), 161–183. MR 0209224

[Ax68] _____, *The elementary theory of finite fields*, Ann. of Math. (2) **88** (1968), 239–271. MR 229613

[BF03] Grégory Berhuy and Giordano Favi, *Essential dimension: a functorial point of view (after A. Merkurjev)*, Doc. Math. **8** (2003), 279–330. MR 2029168

[BMKS16] Mohammad Bardestani, Keivan Mallahi-Karai, and Hadi Salmasian, *Minimal dimension of faithful representations for p-groups*, J. Group Theory **19** (2016), no. 4, 589–608. MR 3518394

[BMKS19] _____, *Kirillov's orbit method and polynomiality of the faithful dimension of p-groups*, Compos. Math. **155** (2019), no. 8, 1618–1654. MR 4043356

[BR97] J. Buhler and Z. Reichstein, *On the essential dimension of a finite group*, Compositio Math. **106** (1997), no. 2, 159–179. MR 1457337

[BS08] Mitya Boyarchenko and Maria Sabitova, *The orbit method for profinite groups and a p-adic analogue of Brown's theorem*, Israel J. Math. **165** (2008), 67–91. MR 2403615

[Del84] P. Deligne, *Les corps locaux de caractéristique p, limites de corps locaux de caractéristique 0*, Representations of reductive groups over a local field, Travaux en Cours, Hermann, Paris, 1984, pp. 119–157. MR 771673

[Gre65] Newcomb Greenleaf, *Irreducible subvarieties and rational points*, Amer. J. Math. **87** (1965), 25–31. MR 182625

[Gre74] Marvin J. Greenberg, *Strictly local solutions of Diophantine equations*, Pacific J. Math. **51** (1974), 143–153. MR 351994

[GS84] Fritz Grunewald and Dan Segal, *Reflections on the classification of torsion-free nilpotent groups*, Group theory, Academic Press, London, 1984, pp. 121–158. MR 780569

[How77] Roger E. Howe, *Kirillov theory for compact p-adic groups*, Pacific J. Math. **73** (1977), no. 2, 365–381. MR 0579176

[Jac85] Nathan Jacobson, *Basic algebra. I*, second ed., W. H. Freeman and Company, New York, 1985. MR 780184

[Kaz77] D. Kazhdan, *Proof of Springer's hypothesis*, Israel J. Math. **28** (1977), no. 4, 272–286. MR 0486181

[Khu98] E. I. Khukhro, *p-automorphisms of finite p-groups*, London Mathematical Society Lecture Note Series, vol. 246, Cambridge University Press, Cambridge, 1998. MR 1615819

[KM08] Nikita A. Karpenko and Alexander S. Merkurjev, *Essential dimension of finite p-groups*, Invent. Math. **172** (2008), no. 3, 491–508. MR 2393078

[Kne78] Martin Kneser, *Konstruktive Lösung p-adischer Gleichungssysteme*, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II (1978), no. 5, 67–69. MR 523328

[Lag83] J. C. Lagarias, *Sets of primes determined by systems of polynomial congruences*, Illinois J. Math. **27** (1983), no. 2, 224–239. MR 694641

[Mar18] Daniel A. Marcus, *Number fields*, Universitext, Springer, Cham, 2018, Second edition of [MR0457396], With a foreword by Barry Mazur. MR 3822326

[McL73] K. R. McLean, *Commutative artinian principal ideal rings*, Proc. London Math. Soc. (3) **26** (1973), 249–272. MR 319981

[Mer17] Alexander S. Merkurjev, *Essential dimension*, Bull. Amer. Math. Soc. (N.S.) **54** (2017), no. 4, 635–661. MR 3683628

[MR10] Aurel Meyer and Zinovy Reichstein, *Some consequences of the Karpenko-Merkurjev theorem*, Doc. Math. (2010), no. Extra vol.: Andrei A. Suslin sixtieth birthday, 445–457. MR 2804261

[OV15] E. A. O'Brien and C. Voll, *Enumerating classes and characters of p-groups*, Trans. Amer. Math. Soc. **367** (2015), no. 11, 7775–7796. MR 3391899

[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), no. 2, 501–550. MR 3188068

[Tie18] Elena Tielker, *Topics in the representation theory of finite p-groups*, Masters thesis, 2018.

[vdD91] Lou van den Dries, *A remark on Ax's theorem on solvability modulo primes*, Math. Z. **208** (1991), no. 1, 65–70. MR 1125733

[Vol04] Christopher Voll, *Zeta functions of groups and enumeration in Bruhat-Tits buildings*, Amer. J. Math. **126** (2004), no. 5, 1005–1032. MR 2089080

[Vol05] ———, *Functional equations for local normal zeta functions of nilpotent groups*, Geom. Funct. Anal. **15** (2005), no. 1, 274–295, With an appendix by A. Beauville. MR 2140633

JOHN ABBOTT COLLEGE, 21 275 RUE LAKESHORE ROAD, SAINTE-ANNE-DE-BELLEVUE, QC, H9X 3L9, CANADA.
Email address: mohammad.bardestani@gmail.com

CONSTRUCTOR UNIVERSITY, CAMPUS RING I, BREMEN 28759 GERMANY
Email address: kmallahikarai@constructor.university

CONSTRUCTOR UNIVERSITY, CAMPUS RING I, BREMEN 28759 GERMANY
Email address: drumiantsau@constructor.university

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF OTTAWA, STEM COMPLEX, 150 LOUIS-PASTEUR PVT, OTTAWA, ON, CANADA K1N 6N5
Email address: hadi.salmasian@uottawa.ca