A PROOF OF THE FIRST KAC–WEISFEILER CONJECTURE IN LARGE CHARACTERISTICS

BENJAMIN MARTIN, DAVID STEWART AND LEWIS TOPLEY

WITH AN APPENDIX BY AKAKI TIKARADZE

ABSTRACT. In 1971, Kac and Weisfeiler made two influential conjectures describing the dimensions of simple modules of a restricted Lie algebra $\mathfrak{g}$. The first predicts the maximal dimension of simple $\mathfrak{g}$-modules and in this paper we apply the Lefschetz Principle and classical techniques from Lie theory to prove this conjecture for all restricted Lie subalgebras of $\mathfrak{gl}_n(k)$ whenever k is an algebraically closed field of sufficiently large characteristic p (depending on n). As a consequence we deduce that the conjecture holds for the Lie algebra of an affine algebraic group scheme over any commutative ring, after specialising to an algebraically closed field of almost any characteristic.

In the appendix to this paper, written by Akaki Tikaradze, an alternative, short proof of the first Kac–Weisfeiler conjecture is given for the Lie algebra of group scheme over a finitely generated ring $R \subseteq \mathbb{C}$, after base change to a field of large positive characteristic.

1. INTRODUCTION

Since the pioneering work of Zassenhaus [Zas54], it has been known that the dimensions of simple modules of finite-dimensional Lie algebras over a field k of characteristic $p > 0$ are bounded, and that the maximal dimension, which we denote $M(\mathfrak{g})$, is a power of p. Jacobson introduced the notion of a restricted Lie algebra with a view to developing a Galois theory for purely inseparable field extensions [Jac37]. Very briefly, restricted Lie algebras are those that admit a p-power map $x \mapsto x^{[p]}$ satisfying axioms which are modelled on the properties of the map $\mathrm{Der}_k(A) \to \mathrm{Der}_k(A)$ given by $d \mapsto d^p$, where A is an associative k-algebra. Many of the modular Lie algebras arising in nature are restricted: for example, when $\mathfrak{g}$ is the Lie algebra of an algebraic group scheme G of finite type over k then there is a natural G-equivariant restricted structure on $\mathfrak{g}$ [Jan03, I.7.10].

Now let k be algebraically closed. In [VK71] Kac and Weisfeiler carried out the first intensive study of representations of restricted Lie algebras. The key property of the restricted structure on $\mathfrak{g}$ is that the elements $x^p - x^{[p]}$ are central in $U(\mathfrak{g})$ for $x \in \mathfrak{g}$, and the subalgebra $Z_p(\mathfrak{g}) \subseteq U(\mathfrak{g})$ generated by these elements is known as the *p-centre*. One of the fundamental insights of [VK71] is that the maximal ideals of $Z_p(\mathfrak{g})$ are parametrised by $\mathfrak{g}^*$. Since the universal enveloping algebra $U(\mathfrak{g})$ is finite over its p-centre it follows from Hilbert's Nullstellensatz that every simple $\mathfrak{g}$-module is annihilated by a unique maximal ideal of $Z_p(\mathfrak{g})$, and so to every simple $\mathfrak{g}$-module M we may assign

some linear form $\chi \in \mathfrak{g}^*$ known as the *p-character of M*. This situation is reminiscent of Kirillov's orbit method, and so it is natural to hope that global properties of the module category $\mathfrak{g}$-mod will be controlled by geometric properties of the module $\mathfrak{g}^*$. These aspirations were formalised by Kac–Weisfeiler in the form of two conjectures: the first of these predicts the maximal dimension of simple $\mathfrak{g}$-modules, and in the current paper we apply techniques from model theory to confirm that conjecture for all restricted Lie subalgebras of $\mathfrak{gl}_n(k)$ when the characteristic of the field k is large. The second conjecture proposes lower bounds on powers of p dividing the dimensions of $\mathfrak{g}$-modules with *p*-character χ; for more detail see [PS99] and the references therein.

The coadjoint stabiliser of $\chi \in \mathfrak{g}^*$ is denoted $\mathfrak{g}^\chi$ and the *index of* $\mathfrak{g}$ is defined by

$$\mathrm{ind}(\mathfrak{g}) := \min_{\chi \in \mathfrak{g}^*} \dim \mathfrak{g}^\chi. \tag{1.1}$$

The first Kac–Weisfeiler conjecture (KW1) predicts that when $\mathfrak{g}$ is any restricted Lie algebra the maximal dimension of simple $\mathfrak{g}$-modules is

$$M(\mathfrak{g}) = p^{\frac{1}{2}(\dim \mathfrak{g} - \mathrm{ind}\, \mathfrak{g})}. \tag{1.2}$$

Theorem 1.1. *For all $d \in \mathbb{N}$ there exists $p_0 \in \mathbb{N}$ depending only on n such that, if $k = \overline{k}$ is a field of characteristic $p > p_0$, and $\mathfrak{g} \subseteq \mathfrak{gl}_d(k)$ is a restricted Lie subalgebra, then the first Kac–Weisfeiler conjecture holds for $\mathfrak{g}$.*

In future work we hope to provide an explicit bound on p_0 in the theorem. We now outline the proof of the result stated. It was first demonstrated by Mil'ner in [Mil75, Theorem 2] (see also [PS99, Remark 5.4]) that $M(\mathfrak{g}) \geqslant p^{\frac{1}{2}(\dim \mathfrak{g} - \mathrm{ind}\, \mathfrak{g})}$ for any restricted Lie algebra $\mathfrak{g}$, and so it remains to prove the opposite inequality. Kirillov in his thesis introduced the notion of a *polarisation of a linear form χ*, which is a Lie subalgebra $\mathfrak{s} \subseteq \mathfrak{g}$ satisfying $\chi[\mathfrak{s}, \mathfrak{s}] = 0$ and $\dim \mathfrak{s} = \frac{1}{2}(\dim \mathfrak{g} + \dim \mathfrak{g}^\chi)$. These turn out to be central to the classification of primitive ideals in enveloping algebras of complex solvable Lie algebras [Dix96, Ch. 6], as well as the classification of simple modules over restricted solvable Lie algebras [VK71, §2]. We say that $\mathfrak{s}$ is a *weak polarisation of* $\chi \in \mathfrak{g}^*$ if $\mathfrak{s} \subseteq \mathfrak{g}$ is a Lie subalgebra of dimension $\frac{1}{2}(\dim \mathfrak{g} + \mathrm{ind}\, \mathfrak{g})$ satisfying $\chi[\mathfrak{s}, \mathfrak{s}] = 0$. Solvable weak polarisations are known to exist for every linear form on every finite-dimensional complex Lie algebra, and we deduce that the same holds for all modular Lie algebras in large characteristics. To do this we apply a first-order version of the Lefschetz Principle. The condition for a solvable weak polarisation to exist involves polynomials in the structure constants of $\mathfrak{g}$; we need to express this condition in terms of first-order sentences, and the key idea is to quantify over all Lie algebras of a fixed dimension simultaneously. The proof concludes by observing that every simple module is a quotient of a module induced from a restricted Lie subalgebra containing a solvable polarisation (Theorem 3.3). This places the required upper bound on the dimension of simple modules. After providing an elementary introduction to the Lefschetz Principle and the representation theory of restricted Lie algebras in §2, we give the proof of Theorem 1.1 in §3.

It is worth comparing the proof sketched above to the situation for Lie algebras of reductive groups. When $\mathfrak{g}$ is such a Lie algebra it is known that for every $\chi \in \mathfrak{g}^*$ there exists a Borel subalgebra $\mathfrak{b} \subseteq \mathfrak{g}$ such that $\chi([\mathfrak{b}, \mathfrak{b}]) = 0$, $\dim \mathfrak{b} = \frac{1}{2}(\dim \mathfrak{g} + \mathrm{ind}\, \mathfrak{g})$

and $[\mathfrak{b}, \mathfrak{b}]$ is unipotent (that is, $[\mathfrak{b}, \mathfrak{b}]$ is annihilated by a sufficiently high power of the p-map). It follows quickly that every simple $\mathfrak{g}$-module of p-character χ is a quotient of some baby Verma module. These are defined to be the $U_\chi(\mathfrak{g})$-modules induced from one-dimensional $U_\chi(\mathfrak{b})$-modules. Hence the Borel subalgebras play the role of solvable weak polarisations in the reductive case.

Let R be a commutative unital ring and say that k is an R-field if k is a field with an R-algebra structure. If G is an R-group scheme and k is an R-field then we write G_k for the base change of G from R to k. In our next theorem we describe a fruitful source of examples to which our main theorem can be applied; note that we do not need the group schemes G_k to be reduced.

Theorem 1.2. *Let G be an affine algebraic group scheme over R. There exists $p_0 \in \mathbb{N}$ such that when $p > p_0$ is prime and $k = \bar{k}$ is an R-field of characteristic p, the first Kac–Weisfeiler conjecture holds for the Lie algebra $\mathrm{Lie}(G_k)$.*

Thus for a fixed group scheme, the KW1 conjecture holds in *almost all* characteristics. The proof, which is presented in §3.1, demonstrates that the Lie algebra $\mathrm{Lie}(G_k)$ admits a faithful restricted representation of dimension d independent of the choice of characteristic $p > 0$ of the field k, which allows us to apply Theorem 1.1.

Until recently it was considered to be possible that (1.2) might hold for non-restricted Lie algebras; however, counterexamples to this hope were found by the third author, by presenting pairs of Lie algebras with isomorphic enveloping algebras and distinct indexes [Top17]. We give some new examples in §3.2. We produce a family of Lie algebras parameterised by the primes p with the property that $\mathfrak{g}_p$ is restricted if and only if (1.2) holds, which is the case if and only if $p \equiv 1$ modulo 4 (see Proposition 3.8).

2. Preliminaries

2.1. **Model theory and the Lefschetz Principle.** Since the main results and motivations of this paper come from representation theory, we expect that some of the readers will be unfamiliar with the model-theoretic methods which we use at several points. Hence we include here a short recap of some of the elements of model theory; a more detailed introduction to the theory may be found in [Mar02]. Since our goal is to explain the Lefschetz Principle, we work exclusively with the language of rings.

The *language of rings* $\mathcal{L}_{\mathrm{ring}}$ consists of the binary function symbols symbols $+, -, \times$ and the constant symbols $0, 1$ [Mar02, Example 1.2.8]. We consider the collection of first-order formulas in this language: these are the formulas that can be built from the symbols $\{\forall, \exists, \vee, \wedge, \neg, +, -, \times, 0, 1, =\}$ along with arbitrary choice of variables (see [Mar02, Section 1.1] for a precise definition of first-order formula). For example, for

$n > 0$ fixed the following are formulas in $\mathcal{L}_{\mathrm{ring}}$:

$$(\forall x)(\forall y)\neg(x^n + y^n = z^n); \tag{2.1}$$

$$(\forall x)(\exists y)\left((xy = 1)) \vee (x = 0)\right); \tag{2.2}$$

$$(\forall x_0)(\forall x_1)\cdots(\forall x_{n-1})(\exists y)(y^n + x_{n-1}y^{n-1} + \cdots + x_0 = 0). \tag{2.3}$$

We say that a formula is a *sentence* if every variable is bound to a quantifier; for example the formula (2.1) is not a sentence because z is a free variable, whilst (2.2) and (2.3) are both sentences in $\mathcal{L}_{\mathrm{ring}}$. If ϕ is a formula with free variables $x_1, ..., x_n$ then we might indicate this by writing $\phi = \phi(x_1, ..., x_n)$. In this case we can obtain a sentence from ϕ by binding the free variables to quantifiers. For example, if $\phi = \phi(z)$ is the formula from (2.1) then $(\forall z)\phi(z)$ is a sentence in the language of rings. In this way we may use formulas to build sentences.

For $p \geqslant 0$ we record one more first-order sentence ψ_p in $\mathcal{L}_{\mathrm{ring}}$:

$$\psi_p \ : \ \underbrace{1 + \cdots + 1}_{p \text{ times}} = 0. \tag{2.4}$$

An $\mathcal{L}_{\mathrm{ring}}$-*structure* is a set R together with elements $0_R, 1_R \in R$, binary operations $+_R, -_R, \times_R : R \times R \to R$, and the binary relation $=_R$ which is always taken to be the diagonal embedding $R \subseteq R \times R$. For example, every ring R gives rise to an $\mathcal{L}_{\mathrm{ring}}$-structure in the obvious way.

Later in this paper we will need to express some statements about elements of vector spaces as formulas and sentences in the language $\mathcal{L}_{\mathrm{ring}}$. To prepare for those arguments we now record a few examples which illustrate this procedure.

Example 2.1. Let k be a field and fix a positive integer $m \in \mathbb{N}$. The following statements can be formulated as sentences and formulas in $\mathcal{L}_{\mathrm{ring}}$ using appropriate variables:

(1) there exist elements $x_1, ..., x_m \in k^n$ which are linearly independent in k^n;
(2) a given bilinear map $f : k^n \times k^n \to k^n$ defines a Lie bracket $[\cdot, \cdot]_f$ on k^n;
(3) the Lie algebra $(k^n, [\cdot, \cdot]_f)$ is solvable.

Moreover, the sentences and formulas we obtain do not depend on the choice of k. To see this, we view k^n as the set of tuples $(a_1, ..., a_n)$ of elements of k. Then (1) is equivalent to the following first-order sentence

$$(\exists a_{i,j})_{i=1,...,n;j=1,...,m}(\forall b_1, ..., b_m)$$

$$((\sum_{j=1}^{m} b_j a_{1,j} = \sum_{j=1}^{m} b_j a_{2,j} = \cdots = \sum_{j=1}^{m} b_j a_{m,j} = 0) \Rightarrow (b_1 = b_2 = \cdots = b_m = 0)),$$

where we take $x_j = (a_{1,j}, ..., a_{n,j})$ for $1 \leqslant j \leqslant m$. This sentence does not depend on k.

Let $v_1, ..., v_n \in k^n$ denote the standard basis. A bilinear map $f : k^n \times k^n \to k^n$ is defined by $f(v_i, v_j) = \sum_{l=1}^{n} f_{i,j;l} v_l$ for some scalars $f_{i,j;l}$, and we identify f with the array $(f_{i,j;l})_{1 \leqslant i,j,l \leqslant n} \in k^{n^3}$. Now the claim that f *defines a Lie bracket* can be encoded as a collection of linear and quadratic polynomial relations not depending on k with integral coefficients in the variables

$$(f_{i,j;l})_{1 \leqslant i,j,l \leqslant n}. \tag{2.5}$$

These relations correspond to skew-symmetry and the Jacobi identity. Since every integer can be constructed using only the symbols $\{+, -, 1, 0\}$ it follows that *f defines a Lie bracket* is a first-order formula not depending on k in $\mathcal{L}_{\mathrm{ring}}$ with free variables (2.5). Similarly the statement *the Lie algebra $(k^n, [\cdot, \cdot]_f)$ is solvable* can be encoded in terms of the vanishing of all n-fold iterations of the Lie bracket, which is equivalent to the vanishing of a collection of homogeneous polynomials of degree $2^n - 1$ amongst the variables (2.5). Again this is a first-order formula not depending on k in $\mathcal{L}_{\mathrm{ring}}$ with free variables (2.5).

An $\mathcal{L}_{\mathrm{ring}}$-*theory* is a set T of first-order sentences in $\mathcal{L}_{\mathrm{ring}}$. If ϕ is a sentence and $M := (R, +_R, -_R, \times_R, 0_R, 1_R, =_R)$ is an $\mathcal{L}_{\mathrm{ring}}$-structure then we say that *M is a model of ϕ*, and write $M \vDash \phi$, if the sentence ϕ is true when interpreted in M. If T is an $\mathcal{L}_{\mathrm{ring}}$-theory then we say that *M is a model of T* and write $M \vDash T$ if $M \vDash \phi$ for all $\phi \in T$.

One way to obtain a theory is to take the collection of all sentences that are true for every model of a particular class of mathematical object. Since mathematical objects are usually determined by axioms, we shall briefly explain (by way of an example) how to pass from a set of axioms to a theory of this type. Consider the set A of axioms of commutative rings, which are clearly first-order sentences in $\mathcal{L}_{\mathrm{ring}}$. We may then consider the set $\mathsf{CR} \subseteq \mathcal{L}_{\mathrm{ring}}$ of sentences that are true for every model of A: i.e., those that are true in every commutative ring. Thus CR denotes the theory of commutative rings. To illustrate the notation introduced above, observe that $(R, +_R, -_R, \times_R, 0_R, 1_R, =_R) \vDash \mathsf{CR}$ is equivalent to the statement that $(R, +_R, -_R, \times_R, 0_R, 1_R)$ is a commutative ring. As such the class of models of CR is precisely the class of commutative rings.

In this paper we will be primarily interested in the theory of fields. The axioms of a field can obviously be written as first-order sentences in $\mathcal{L}_{\mathrm{ring}}$; for instance (2.2) expresses the existence of multiplicative inverses. The axioms of the algebraically closed fields are obtained by including the sentences (2.3) for all $n > 0$. If $p > 0$ is prime then we may include the sentence ψ_p, defined in (2.4), to obtain the axioms of the algebraically closed fields of characteristic $p > 0$; the corresponding theory is denoted ACF_p. Alternatively we may include the sentences $\{\neg \psi_p \mid p > 0\}$ to obtain the axioms of the algebraically closed fields of characteristic zero, and we denote their theory by ACF_0 (cf. [Mar02, Example 1.2.8]). As was the case for commutative rings, we see that the class of all models of ACF_p is precisely the class of all algebraically closed fields of characteristic p.

The following result is Gödel's completeness theorem in the context of $\mathcal{L}_{\mathrm{ring}}$ (cf. [Mar02, Theorem 2.1.2]).

Lemma 2.2. *Let ϕ be a first-order sentence and T let be any theory in $\mathcal{L}_{\mathrm{ring}}$. Then ϕ is true when interpreted in every model of T if and only if ϕ can be deduced from T by means of a formal proof in $\mathcal{L}_{\mathrm{ring}}$.*

We say that an $\mathcal{L}_{\mathrm{ring}}$-theory T is *complete* if, for every first-order sentence ϕ in $\mathcal{L}_{\mathrm{ring}}$, either ϕ is true when interpreted in every model of T, or $\neg \phi$ is true when interpreted in every model of T. By Lemma 2.2 this is equivalent to saying that for every sentence ϕ we can derive either ϕ or $\neg \phi$ from T by means of a formal proof. The following well-known result is proved by quantifier elimination [Mar02, Corollary 3.2.3].

Theorem 2.3. *For $p = 0$ or p prime, the theory ACF_p is complete.*

As an immediate consequence we obtain a first-order version of the Lefschetz Principle from algebraic geometry [Mar02, Corollary 2.2.10]:

Corollary 2.4. *(Lefschetz Principle) If ϕ is a sentence in $\mathcal{L}_{\mathrm{ring}}$ then:*

(1) *If ϕ is true in some model of ACF_p where $p \geqslant 0$ then ϕ is true in every model of ACF_p.*

(2) *If ϕ is true in some model of ACF_0 then there exists $p_0 \in \mathbb{N}$ such that ϕ is true in every model of ACF_p for $p > p_0$.*

Proof. Part (1) is precisely Theorem 2.3. For part (2) suppose that ϕ is true over some field satisfying the axioms of ACF_0. Then by part (1) it is true for every such field, and by Lemma 2.2 we conclude that there exists a formal proof for ϕ in $\mathcal{L}_{\mathrm{ring}}$ using only the axioms of ACF_0. Since the proof of ϕ involves only finitely many sentences in $\mathcal{L}_{\mathrm{ring}}$, it follows that the set of primes

$$P_\phi := \{p \mid \neg\psi_p \text{ occurs in the proof of } \phi\}$$

is finite, where ψ_p is defined in (2.4). Hence for $p > \max(P_\phi)$ there is a formal proof of ϕ using the axioms of ACF_p. Using Lemma 2.2 once more we see that ϕ is true for every $\mathcal{L}_{\mathrm{ring}}$-structure satisfying the axioms of ACF_p. $\qquad\square$

2.2. **Restricted Lie algebras and reduced enveloping algebras.** Fix a field k of characteristic $p > 0$ and let $\mathfrak{g}$ be a Lie algebra over k. As usual we write $U(\mathfrak{g})$ for the enveloping algebra and $Z(\mathfrak{g})$ for the centre of $U(\mathfrak{g})$. Then $\mathfrak{g}$ is said to be a *restricted Lie algebra over k* if it comes equipped with a p-map $\mathfrak{g} \to \mathfrak{g}$, written $x \mapsto x^{[p]}$, which satisfies two axioms: if we write $\xi : \mathfrak{g} \to U(\mathfrak{g})$ for the map $x \mapsto x^p - x^{[p]}$, then $(-)^{[p]}$ must satisfy

(1) $\xi(\mathfrak{g}) \subseteq Z(\mathfrak{g})$;

(2) ξ is p-semilinear in the sense of [Jan98, Lemma 2.1].

We refer the reader to [SF88] for a comprehensive introduction to the theory of restricted Lie algebras. It follows from the PBW theorem that the vector space $\xi(\mathfrak{g})$ generates a polynomial algebra of rank equal to $\dim(\mathfrak{g})$ inside $U(\mathfrak{g})$. This algebra is referred to as the *p-centre* of $U(\mathfrak{g})$, and is denoted $Z_p(\mathfrak{g})$. If $\{x_i \mid i \in I\}$ is a basis for $\mathfrak{g}$ then the PBW theorem for $U(\mathfrak{g})$ implies that $Z_p(\mathfrak{g})$ is isomorphic to a polynomial ring generated by $\{\xi(x_i) \mid i \in I\}$. Hence $Z_p(\mathfrak{g})$ can be naturally identified with the coordinate ring $k[(\mathfrak{g}^*)^{(1)}]$ on the Frobenius twist of $\mathfrak{g}^*$.

When k is an algebraically closed field we have $\mathfrak{g}^* = (\mathfrak{g}^*)^{(1)}$ as sets and so for every $\chi \in \mathfrak{g}^*$ there is a maximal ideal $I_\chi \in \operatorname{Spec} Z_p(\mathfrak{g})$. Explicitly we have $I_\chi := (x^p - x^{[p]} - \chi(x)^p \mid x \in \mathfrak{g})$ and the *reduced enveloping algebra with p-character χ* is defined to be

$$U_\chi(\mathfrak{g}) := U(\mathfrak{g})/U(\mathfrak{g})I_\chi.$$

We have $\dim U_\chi(\mathfrak{g}) = p^{\dim \mathfrak{g}}$, so a simple module for $U_\chi(\mathfrak{g})$ can have dimension at most $p^{\frac{1}{2}\dim \mathfrak{g}}$. If $\mathfrak{g}_0 \subseteq \mathfrak{g}$ is a restricted subalgebra and $\chi \in \mathfrak{g}^*$ then we can abuse notation by identifying $U_{\chi|_{\mathfrak{g}_0}}(\mathfrak{g}_0)$ with the subalgebra of $U_\chi(\mathfrak{g})$ generated by $\mathfrak{g}_0$, and denote this subalgebra by $U_\chi(\mathfrak{g}_0)$. We say that a $\mathfrak{g}$-module M has p-character χ if the corresponding

representation $U(\mathfrak{g}) \to \mathrm{End}_k(M)$ factors through the quotient $U(\mathfrak{g}) \to U_\chi(\mathfrak{g})$. If $\mathfrak{g}_0 \subseteq \mathfrak{g}$ are restricted Lie algebras, $\chi \in \mathfrak{g}^*$ and M_0 is a $U_\chi(\mathfrak{g}_0)$-module then we may define the induced module

$$\mathrm{Ind}_{\mathfrak{g}_0}^{\mathfrak{g},\chi}(M_0) := U_\chi(\mathfrak{g}) \otimes_{U_\chi(\mathfrak{g}_0)} M_0. \tag{2.6}$$

We have

$$\dim \mathrm{Ind}_{\mathfrak{g}_0}^{\mathfrak{g},\chi}(M_0) = p^{\dim \mathfrak{g} - \dim \mathfrak{g}_0} \dim(M_0) \tag{2.7}$$

and this induced module is universal amongst $U_\chi(\mathfrak{g})$-modules M such that the restriction to $U_\chi(\mathfrak{g}_0)$ contains a submodule isomorphic to M_0: that is, any nonzero homomorphism of $U_\chi(\mathfrak{g}_0)$-modules $M_0 \to M$ induces a nonzero homomorphism $\mathrm{Ind}_{\mathfrak{g}_0}^{\mathfrak{g},\chi}(M_0) \to M$ of $U_\chi(\mathfrak{g})$-modules.

The coadjoint $\mathfrak{g}$-module is the vector space $\mathfrak{g}^*$ with module structure given by $(x \cdot \chi)(y) := \chi([y, x])$ where $x, y \in \mathfrak{g}$ and $\chi \in \mathfrak{g}^*$. The stabiliser of $\chi \in \mathfrak{g}^*$ is then defined to be

$$\mathfrak{g}^\chi := \{x \in \mathfrak{g} \mid x \cdot \chi = 0\} = \{x \in \mathfrak{g} \mid \chi([x, \mathfrak{g}]) = 0\}$$

and the index of $\mathfrak{g}$ — commonly denoted $\mathrm{ind}(\mathfrak{g})$ — is the minimal dimension of $\mathfrak{g}^\chi$ as χ varies over all elements of $\mathfrak{g}^*$.

3. The maximal dimensions of simple modules

In this section we prove Theorem 1.1. In order to do so we recall a few pieces of terminology. If $\mathfrak{g}$ is a Lie algebra over a field k and $\chi \in \mathfrak{g}^*$ we say that a Lie subalgebra $\mathfrak{s} \subseteq \mathfrak{g}$ is *subordinate to* χ if $\mathfrak{s}$ is an isotropic subspace with respect to the skew-symmetric form

$$\begin{array}{rcl} B_\chi : \mathfrak{g} \times \mathfrak{g} & \to & k \\ (x, y) & \mapsto & \chi([x, y]) : \end{array} \tag{3.1}$$

in other words, if $\chi([\mathfrak{s}, \mathfrak{s}]) = 0$. We say that a Lie subalgebra $\mathfrak{s} \subseteq \mathfrak{g}$ is a *polarisation of* χ if $\mathfrak{s}$ is a Lagrangian for B_χ, i.e., $\mathfrak{s}$ is a maximal isotropic subspace of $\mathfrak{g}$. Since the stabiliser $\mathfrak{g}^\chi$ coincides with the radical of B_χ it follows from [Dix96, 1.12.1] that

$$\dim(\mathfrak{s}) \leqslant \frac{1}{2}(\dim(\mathfrak{g}) + \dim(\mathfrak{g}^\chi)) \tag{3.2}$$

if $\mathfrak{s}$ is subordinate to χ. Furthermore equality holds if and only if $\mathfrak{s}$ is a polarisation of χ. Finally we say that a Lie subalgebra $\mathfrak{s} \subseteq \mathfrak{g}$ is a *weak polarisation of* χ if $\mathfrak{s}$ is isotropic for the form (3.1) and

$$\dim(\mathfrak{s}) = \frac{1}{2}(\dim(\mathfrak{g}) + \mathrm{ind}(\mathfrak{g})). \tag{3.3}$$

The proof of Theorem 1.1 rests on the existence of solvable weak polarisations for linear forms, and the following result is the key step.

Proposition 3.1. *For all $n, d \in \mathbb{N}$, there exists $p_1 = p_1(n, d) \in \mathbb{N}$ such that if:*
- (1) *k is an algebraically closed field of characteristic $p > p_1$;*
- (2) *$\mathfrak{g}$ is a Lie algebra of dimension n over k;*
- (3) *there exists a faithful representation $\rho : \mathfrak{g} \to \mathfrak{gl}_d(k)$;*

then for every $\chi \in \mathfrak{g}^*$ there is a solvable weak polarisation $\mathfrak{s} \subseteq \mathfrak{g}$ such that $\rho(\mathfrak{s})$ is upper-triangularisable in $\mathfrak{gl}_d(k)$.

Proof. Fix $n, d \in \mathbb{N}$, $r \in \{0, ..., n\}$ and let k be an algebraically closed field of characteristic $p \geqslant 0$. Let $\{v_1, ..., v_n\}$ denote the standard basis for k^n. If f is a bilinear map from $k^n \times k^n$ to k^n then $f(v_i, v_j) = \sum_{l=1}^{n} f_{i,j;l} v_l$ and so we identify the set of such bilinear maps with k^{n^3} and identify f with $(f_{i,j;l})_{1 \leqslant i,j,l \leqslant n} \in k^{n^3}$. For $i = 1, ..., n$ we write A_i for an element of $\mathrm{Mat}_d(k) \cong k^{d^2}$, so that the n-tuple $A = (A_1, ..., A_n)$ is an element of k^{nd^2}. Finally pick $\chi = (\chi_1, ..., \chi_n) \in k^n$ and identify k^n with $(k^n)^* = \mathrm{Hom}_k(k^n, k)$ by letting χ be the linear map determined by $v_i \mapsto \chi_i$.

Fix $r \in \{0, ..., n\}$ and for any $(f, A, \chi) \in k^{n^3 + nd^2 + n}$ we consider the following four statements:

(i) $f = (f_{i,j;l})$ are the structure constants of a Lie bracket $[\cdot, \cdot]_f$ on k^n;
(ii) the Lie algebra $(k^n, [\cdot, \cdot]_f)$ has index equal to r;
(iii) the linear map $k^n \to \mathrm{Mat}_d(k)$ given by $v_i \mapsto A_i$ is a faithful Lie algebra representation $\rho : k^n \to \mathfrak{gl}_d(k)$;
(iv) there exist elements $x_1, ..., x_s \in k^n$ where $s = \frac{1}{2}(n+r)$ which are linearly independent and span a solvable Lie subalgebra $\mathfrak{s}$ of $(k^n, [\cdot, \cdot]_f)$ such that $\chi([\mathfrak{s}, \mathfrak{s}]_f) = 0$ and $\rho(\mathfrak{s})$ is upper-triangularisable inside $\mathfrak{gl}_d(k)$.

Now consider the following statements indexed by r:

$$\Phi_r \quad : \quad \forall (f, A, \chi) \in k^{n^3 + d^2 n + n}((\text{i}) \wedge (\text{ii}) \wedge (\text{iii})) \Rightarrow (\text{iv})) \tag{3.4}$$

Claim: Each statement Φ_r can be formulated as a first-order sentence in the language $\mathcal{L}_{\mathrm{ring}}$ of rings (in the notation of §2.1). Moreover, the resulting sentences do not depend on the choice of k.

In Example 2.1(2) we showed that (i) is given by a formula independent of k in the language $\mathcal{L}_{\mathrm{ring}}$ with free variables $(f_{i,j;l})$. If $(f_{i,j;l})$ are the structure constants of a Lie bracket $[\cdot, \cdot]_f$ then the structure constants of the coadjoint representation $\mathrm{ad}_f^* : k^n \to \mathrm{Mat}_n(k)$ are $(-f_{i,l;j})_{1 \leqslant i,j,l \leqslant n}$. It follows that for $x = (a_1, ..., a_n) \in k^n$ the statement $\mathrm{ad}_f^*(x)\chi = 0$ can be expressed by the vanishing of certain polynomial functions, with integral coefficients, in the variables $(f_{i,j;l})$ and $a_1, ..., a_n, \chi_1, ..., \chi_n$. The statement (ii) can be phrased in the following way: *there exists $\psi = (\psi_1, ..., \psi_n) \in k^n \cong \mathrm{Hom}_k(k^n, k)$ and linearly independent elements $x_1, ..., x_r \in k^n$ that satisfy $\mathrm{ad}_f^*(x_i)\psi = 0$, and there does not exist $\varphi \in \mathrm{Hom}_k(k^n, k)$ such that if $x_1, ..., x_r \in k^n$ satisfy $\mathrm{ad}_f^*(x_i)\varphi = 0$ then $x_1, ..., x_r$ must be linearly dependent.* This is a first-order formula which does not depend on the choice of k in $\mathcal{L}_{\mathrm{ring}}$ with free variables $(f_{i,j;l})$ thanks to part (1) of Example 2.1 and the previous remarks. The fact that (iii) is a first-order formula which does not depend on the choice of k in $\mathcal{L}_{\mathrm{ring}}$ with free variables (f, A) follows similarly. Statement (iv) asserts the existence of linearly independent $x_1, ..., x_s$ spanning a solvable Lie subalgebra of $(k^n, [\cdot, \cdot]_f)$. The existence of linearly independent elements $x_1, ..., x_s$ that satisfy $\chi([x_i, x_j]_f) = 0$ and span a solvable Lie algebra is a first-order formula not depending on k—indeed this follows quickly from Example 2.1. The fact that the solvable subalgebra can be upper-triangularised in $\mathfrak{gl}_d(k)$ can be expressed by the existence of a basis of

k^d satisfying special properties which can also be expressed as first-order formulas not depending on k in $\mathcal{L}_{\mathrm{ring}}$. Since the last remark is proved in a manner almost identical to the previous parts, we leave the details to the reader. The only free variables in (iv) are (f, A, χ) and so we have shown that all of the variables in the formulas (i), (ii), (iii), (iv) are bound to quantifiers in Φ_r. Hence Φ_r is a first-order sentence in $\mathcal{L}_{\mathrm{ring}}$ which is independent of the choice of k, and this proves the claim.

Keep $n, d \in \mathbb{N}$, let $r \in \{0, ..., n\}$ fixed, and now suppose that k is algebraically closed of characteristic zero. By Lie's theorem [Dix96, Theorem 1.3.12] we know that every solvable Lie subalgebra of $\mathfrak{gl}_d(k)$ is upper-triangularisable, and thanks to [Dix96, Corollary 1.12.17] we know that when $\mathfrak{g}$ is a Lie algebra over k of dimension n and index r, then for all $\chi \in \mathfrak{g}^*$ there exists a weak polarisation of χ. Hence every algebraically closed field of characteristic zero is a model for Φ_r. It follows by the Lefschetz Principle (Corollary 2.4) that there is a number $p_1^r = p_1^r(n, d) \in \mathbb{N}$ such that Φ_r is also true when interpreted in any algebraically closed field of characteristic $p > p_1^r$. If we set $p_1 := \max\{p_1^0, p_1^1, ..., p_1^n\}$ then it follows from the above remarks that for all $r = 0, ..., n$, Φ_r is true for every algebraically closed field of characteristic $p > p_1$. This completes the proof of the current Proposition. $\qquad\square$

The next result follows from [VK71, Corollary 2.6].

Lemma 3.2. *Let $\mathfrak{s}$ be a restricted solvable Lie algebra over k with a faithful restricted representation $\mathfrak{s} \to \mathfrak{gl}_d(k)$. If $\mathfrak{s}$ is upper-triangularisable in $\mathfrak{gl}_d(k)$ and $\chi \in \mathfrak{s}^*$, then all irreducible $U_\chi(\mathfrak{s})$-modules have the same dimension.*

Theorem 3.3. *For all $d \in \mathbb{N}$ there exists $p_0 = p_0(d) \in \mathbb{N}$ such that if $k = \bar{k}$ is a field of characteristic $p > p_0$, if $\mathfrak{g} \subseteq \mathfrak{gl}_d(k)$ and M is a simple $\mathfrak{g}$-module with p-character χ then M is a quotient of a module of the form $\mathrm{Ind}_{\bar{\mathfrak{s}}}^{\mathfrak{g},\chi}(M_0)$, where $\bar{\mathfrak{s}}$ is a restricted Lie subalgebra of $\mathfrak{g}$ which contains a solvable weak polarisation of χ, and M_0 is a one-dimensional $U_\chi(\bar{\mathfrak{s}})$-module.*

Proof. Fix $d \in \mathbb{N}$, let $p_0 := \max\{d, p_1(1, d), p_1(2, d), ..., p_1(d^2, d)\}$ where $p_1(n, d)$ was defined in Proposition 3.1, and let k be an algebraically closed field of characteristic $p > p_0$. Let $\mathfrak{g} \subseteq \mathfrak{gl}_d(k)$ be restricted and let $\chi \in \mathfrak{g}^*$. Thanks to Proposition 3.1 we know there exists a solvable weak polarisation $\mathfrak{s} \subseteq \mathfrak{g}$ of χ with $\mathfrak{s}$ upper-triangularisable. Let $\bar{\mathfrak{s}}$ denote the restricted closure of $\mathfrak{s}$ in $\mathfrak{gl}_d(k)$, which is the smallest restricted Lie subalgebra of $\mathfrak{gl}_d(k)$ containing $\mathfrak{s}$. Evidently we have $\mathfrak{s} \subseteq \bar{\mathfrak{s}} \subseteq \mathfrak{g}$. Since the upper-triangular matrices form a restricted Lie subalgebra of $\mathfrak{gl}_d(k)$ it follows that $\bar{\mathfrak{s}}$ is upper-triangularisable and solvable. Since $[\bar{\mathfrak{s}}, \bar{\mathfrak{s}}]$ consists of strictly upper-triangularisable matrices, our assumption $p > d$ ensures that the p-power map vanishes identically on $[\bar{\mathfrak{s}}, \bar{\mathfrak{s}}]$ and so this derived ideal is restricted. By [SF88, Proposition 2.1.3(1)], $\bar{\mathfrak{s}}$ is spanned by elements of the form $x^{[p]^m}$ where $x \in \mathfrak{s}$ and $m \geqslant 0$. Since $[x^{[p]}, y] = \mathrm{ad}(x^{[p]})(y) = \mathrm{ad}(x)^p(y)$ for all $x, y \in \mathfrak{g}$, we see that $[\bar{\mathfrak{s}}, \bar{\mathfrak{s}}] = [\mathfrak{s}, \mathfrak{s}]$.

Now $[\bar{\mathfrak{s}}, \bar{\mathfrak{s}}]$ is a proper restricted ideal of $\bar{\mathfrak{s}}$, so $[\bar{\mathfrak{s}}, \bar{\mathfrak{s}}]$ generates a proper ideal of $U_\chi(\bar{\mathfrak{s}})$. The quotient is a nonzero finite-dimensional abelian k-algebra and therefore all of its simple modules are one-dimensional. This shows that $U_\chi(\bar{\mathfrak{s}})$ has at least one one-dimensional module. We deduce from Lemma 3.2 that every simple $U_\chi(\bar{\mathfrak{s}})$-module is one-dimensional. Now let M be a simple $\mathfrak{g}$-module with p-character χ. According to

our previous deductions there is a one-dimensional $U_\chi(\bar{\mathfrak{s}})$-submodule, which we call M_0. Now the existence of a surjection $\mathrm{Ind}_{\bar{\mathfrak{s}}}^{\mathfrak{g},\chi}(M_0) \twoheadrightarrow M$ follows from the universal property of induced modules, along with the fact that M is simple. $\qquad\square$

Now the proof of Theorem 1.1 follows from the previous theorem, combined with (2.7).

Remark 3.4. It has been conjectured that for a restricted Lie algebra $\mathfrak{g}$ the following are equivalent:

(i) $\mathfrak{g}$ is Frobenius, meaning $\mathrm{ind}(\mathfrak{g}) = 0$;
(ii) there exists a non-empty open subset $\mathcal{O} \subseteq \mathfrak{g}^*$ such that $U_\chi(\mathfrak{g})$ is simple for all $\chi \in \mathcal{O}$.

Our main theorem implies that the conjecture holds for Lie subalgebras of $\mathfrak{gl}_d(k)$ provided $\mathrm{char}(k) > p_0(d)$. In fact (i) $\Rightarrow$ (ii) holds in general thanks to [PS99, Theorem 4.4]. Conversely, supposing $U_\chi(\mathfrak{g})$ is simple, there is a simple $\mathfrak{g}$-module of the maximal possible dimension $\sqrt{\dim U_\chi(\mathfrak{g})} = p^{\frac{1}{2}\dim \mathfrak{g}}$. If the KW1 conjecture holds for $\mathfrak{g}$ then $M(\mathfrak{g}) = p^{\frac{1}{2}\dim \mathfrak{g}} = p^{\frac{1}{2}(\dim \mathfrak{g} - \mathrm{ind}\,\mathfrak{g})}$ and so $\mathfrak{g}$ is Frobenius.

3.1. **Example: the Lie algebras of group schemes.** In this final subsection we draw attention to families of important Lie algebras to which Theorem 1.1 can be applied, proving Theorem 1.2 from the introduction. We recall some of the elements of the theory of affine algebraic group schemes, following [DG70], [Jan03]. Throughout the subsection we fix a commutative unital ring R, we write R-alg for the category of R-algebras, and we say that k is an *R-field* if k is both a field and an object of R-alg. An affine group scheme G over R is a functor from R-algebras to groups, naturally equivalent to one of the form $\mathrm{Spec}_R R[G] := \mathrm{Hom}_{R\text{-alg}}(R[G], -)$ where $R[G]$ is some R-algebra. We call $R[G]$ the co-ordinate ring of G. We say that G is *algebraic* if $R[G]$ is a finitely generated R-algebra. The archetypal example of an affine algebraic group scheme is GL_d. Endowing an R-algebra $R[G]$ with the structure of an affine algebraic group scheme is equivalent to endowing a finitely generated R-algebra $R[G]$ with a Hopf algebra structure $(R[G], \Delta, \sigma, \epsilon)$. Associated to G we have the Lie algebra $\mathfrak{g} = \mathrm{Lie}(G)$ over R [DG70, II.4.1.2]; we may identify $\mathfrak{g}$ with the kernel of the homomorphism $G(R[\epsilon]/(\epsilon^2)) \to G(R)$ induced by the R-algebra homomorphism $R[\epsilon]/(\epsilon^2) \to R, \epsilon \mapsto 0$.

When G is an affine group scheme over R and k is any R-algebra then we can consider the base change G_k, which is an affine group scheme over k obtained by viewing k-algebras as R-algebras. The co-ordinate ring $k[G_k]$ of G_k is given by $k[G_k] = R[G] \otimes_R k$. We write $\mathfrak{g}_k = \mathrm{Lie}(G_k)$. If G is affine algebraic then we can write $R[G] \cong R[x_1, ..., x_n]/I$ for some n and some ideal I of the polynomial ring $R[x_1, ..., x_n]$; we obtain a map $\omega : R[x_1, ..., x_n] \to k[x_1, ..., x_n]$ and we have

$$G_k \cong \mathrm{Spec}_k k[x_1, ..., x_n]/I_k \tag{3.5}$$

for some ideal I_k of $k[x_1, ..., x_n]$.

Lemma 3.5. *Let G be an affine algebraic group scheme over R. There exists $d \in \mathbb{N}$ depending only on G such that for each R-field k there exists a representation $\rho : G_k \to (\mathrm{GL}_d)_k$, with $d\rho : \mathfrak{g}_k \to (\mathfrak{gl}_d)_k$ faithful.*

Proof. Suppose that G corresponds to the Hopf algebra $(R[G], \Delta, \sigma, \epsilon)$, with $R[G] = R[x_1, ..., x_n]/I$. Fix $i \in \{1, ..., n\}$, write $\Delta(x_i) = \sum_{j=1}^{r(i)} f_{i,j}^{(1)} \otimes f_{i,j}^{(2)}$ and define $d := \sum_{i=1}^{n} r(i)$. Choose any R-field k and let M be the R-submodule of $R[G]$ generated by the elements $\{f_{i,j}^{(1)} \mid i = 1, ..., n, j = 1, ..., r(i)\}$. Write $\omega : R[G] \to k[G_k]$ for the natural homomorphism.

Thanks to (3.5) there is a surjection $M \otimes_R k \twoheadrightarrow \omega(M)$ and so $\omega(M)$ identifies with a subspace of $k[G_k]$ of dimension $\leqslant d$. We observe that the coproduct $\Delta(\omega(x_i)) = \sum_{i=1}^{r(i)} \omega(f_{i,j}^{(1)}) \otimes \omega(f_{i,j}^{(2)})$ can be rewritten in the form $\Delta(\omega(x_i)) = \sum_{i=1}^{r_k(i)} h_{i,j} \otimes \omega(f_{i,j}^{(2)})$ for some $r_k(i) \leqslant r(i)$ and certain elements $h_{i,j} \in \omega(M)$, such that $\omega(f_{i,1}^{(2)}), ..., \omega(f_{i,r_k(i)}^{(2)})$ are k-linearly independent. According to [Jan03, I.2.13(4)] the space $N_i := \sum_{j=1}^{r_k(i)} k h_{i,j}$ is a G_k-submodule of $\omega(M)$ containing x_i. Furthermore it follows from [Mil17, Proof of Prop. 4.7] that $N = \sum_{i=1}^{n} N_i$ is a faithful G_k-submodule of $k[G_k]$ of dimension $\leqslant d$. Therefore $N \oplus k^{\oplus(d-\dim N)}$ is a faithful G_k-module of dimension d. Finally observe that $N \oplus k^{\oplus(d-\dim N)}$ is a faithful $\mathfrak{g}_k$-module. To see this note, for example, that by faithfulness $1 \to G(k[\epsilon]/(\epsilon^2)) \to \mathrm{GL}_d(k[\epsilon]/(\epsilon^2))$ is exact; also $\mathrm{Lie}(G_k) \cong \ker(G(k[\epsilon]/(\epsilon^2)) \to G(k))$ for the map $\epsilon \mapsto 0$, and similarly for GL_d. Hence the claim follows from the commutativity of the following diagram [DG70, II.4.1.3]:

$$
\begin{array}{ccc}
0 \longrightarrow \mathfrak{g}_k \longrightarrow & G_k(k[\epsilon]/(\epsilon^2)) \\
\downarrow & \downarrow \\
0 \longrightarrow \mathfrak{gl}_d \longrightarrow & \mathrm{GL}_d(k[\epsilon]/(\epsilon^2))
\end{array}
\qquad \square
$$

Remark 3.6. Given a faithful representation $\sigma \colon G \to \mathrm{GL}_d$, we obtain by base change for any R-field k a representation $\sigma_k \colon G_k \to (\mathrm{GL}_d)_k$ such that $d\sigma_k$ is faithful. The question, however, of when such σ exists is rather subtle—this is not known even when R is the ring of dual numbers over a field k and G is flat and of finite type over R. On the other hand, the existence of such a representation is known when G is flat and of finite type over a Dedekind domain R, such as $\mathbb{Z}$, or indeed if R is any field. Fortunately we do not need such a σ: any family of representations $\rho \colon G_k \to (\mathrm{GL}_d)_{k_p}$ for p prime will do because we quantify over all representations simultaneously. (Here k_p denotes the algebraic closure of the finite field $\mathbb{F}_p$.)

Proof of Theorem 1.2. This follows immediately from Theorem 1.1 and Lemma 3.5. $\square$

Example 3.7. Fix a Dynkin type and a non-negative integer r. There exists a prime p_0 depending only on r and the Dynkin type with the following property. Suppose G is a connected reductive algebraic group over an algebraically closed field k of characteristic $p > 0$ such that $[G, G]$ has the given Dynkin type and $Z := Z(G)^0$ has dimension r. If $p > p_0$ then for any restricted Lie subalgebra $\mathfrak{h}$ of $\mathfrak{g} := \mathrm{Lie}\, G$, the first Kac-Weisfeiler conjecture holds for $\mathfrak{h}$. To see this, note first that if p is very good then $\mathrm{Lie}[G, G]$ has trivial centre, so any isogeny of connected reductive groups with domain or codomain equal to G is separable and therefore gives rise to an isomorphism of restricted Lie algebras. Hence without loss we can take G to be of the form $[G, G] \times Z$, where Z is a torus of dimension r and $[G, G]$ is adjoint. Then G admits a faithful representation of dimension $\dim G + r$ (just take the direct sum of the adjoint representation of $[G, G]$

and a faithful r-dimensional representation of Z). This yields a faithful restricted representation of $\mathfrak{g}$, and hence of $\mathfrak{h}$. The assertion now follows from Theorem 1.1.

In particular, the result applies when $\mathfrak{h}$ is a parabolic subalgebra of $\mathfrak{g}$, or when $\mathfrak{h}$ is the Lie algebra centraliser of some (possibly nonsmooth) subgroup scheme K of G — note that in the latter case, $\mathfrak{h}$ is the Lie algebra of the scheme-theoretic centraliser $C_G(K)$, so $\mathfrak{h}$ is restricted. In the special case $\mathfrak{h} = \mathfrak{g}$, it has been known for some time that the first Kac-Weisfeiler conjecture holds, at least when $p > 2$ (see [PS99, Section 4.1]).

3.2. **Example: families of non-algebraic Lie algebras.** Let $\mathfrak{g}$ be a Lie algebra over a commutative unital ring R such that $\mathfrak{g}$ is finitely generated as an R-module. If k is an algebraically closed R-field then base change yields a finite-dimensional Lie algebra $\mathfrak{g}_k$ over k. It is natural to ask whether the equality (1.2) from the first Kac-Weisfeiler conjecture holds when $\mathrm{char}(k) \gg 0$. In this final subsection we show that the answer is no; to see this we construct a Lie algebra $\mathfrak{g}$ over the Gaussian integers $\mathbb{Z}[i]$ such that the Lie algebras $\mathfrak{g}_p$ obtained by base change from $\mathbb{Z}[i]$ to k_p exhibit some striking behaviour, quite different from the situation for Lie algebras of group schemes. The underlying reason is that for infinitely many p, $\mathfrak{g}_p$ does not admit a restricted structure. This cannot happen in the setting of Theorem 1.2 because the Lie algebra of the affine group scheme G_k is automatically restricted.

Let $\mathfrak{g}$ be the free $\mathbb{Z}[i]$-module with basis $\{h, x, y\}$ and equip it with a $\mathbb{Z}[i]$-linear Lie algebra structure by defining brackets $[h, x] = x, [h, y] = iy, [x, y] = 0$. Since $\mathbb{Z} \subseteq \mathbb{Z}[i]$ is an integral extension, the going-up theorem implies that for every prime number $p \in \mathbb{N}$ there is a prime ideal $\mathfrak{p}_p \in \mathrm{Spec}(\mathbb{Z}[i])$ such that $\mathbb{Z}[i]/\mathfrak{p}_p$ has characteristic p. Since $\mathbb{Z}[i]$ is a principal ideal domain it follows that these quotients are fields, and we may write k_p for the algebraic closure of $\mathbb{Z}[i]/\mathfrak{p}_p$. Now define $\mathfrak{g}_p := \mathfrak{g} \otimes_{\mathbb{Z}[i]} k_p$. Note that $\mathfrak{g}$ has a faithful representation in $\mathrm{GL}_3(\mathbb{Z}[i])$ given by the adjoint, and this gives rise by base change to a faithful representation of $\mathfrak{g}_p$ in $\mathfrak{gl}_3(k_p)$ for every prime p. Since the example is elementary enough we can actually describe the representation theory explicitly.

Proposition 3.8. *Suppose that $p > 2$. The following are equivalent:*

(1) $M(\mathfrak{g}_p) = p^{\frac{1}{2}(\dim(\mathfrak{g}_p) - \mathrm{ind}(\mathfrak{g}_p))}$;
(2) $\mathfrak{g}_p$ *is a restricted Lie algebra;*
(3) $p \equiv 1$ *modulo 4.*

Proof. By Jacobson's theorem [SF88, Theorem 2.2.3] we know that $\mathfrak{g}_p$ is restricted if and only if there exist elements $\{h_0, x_0, y_0\}$ such that $\mathrm{ad}(h)^p = \mathrm{ad}(h_0)$, $\mathrm{ad}(x)^p = \mathrm{ad}(x_0)$, $\mathrm{ad}(y)^p = \mathrm{ad}(y_0)$. Elementary considerations in linear algebra confirm that this is the case if and only if $\mathrm{ad}(h)^p = \mathrm{ad}(h)$ which is equivalent to $(-1)^{\frac{p-1}{2}} iy = iy$. This is the case precisely when $p \equiv 1 \bmod 4$. Thus we see that $(2) \Leftrightarrow (3)$.

We now show that $(1) \Leftrightarrow (2)$. Observe that $\dim \mathfrak{g}_p^\chi = 1$ whenever $\chi(x) \neq 0$, and so $\mathrm{ind}(\mathfrak{g}_p) = 1$. Thanks to [PS99, Remark 5.4,(1)] we know that (1) holds if and only if $M(\mathfrak{g}_p) \leqslant p$. First suppose that $\mathfrak{g}_p$ is not restricted: $\mathfrak{g}_p \neq \bar{\mathfrak{g}}_p$, where we write $\bar{\mathfrak{g}}_p$ for the restricted hull of $\mathfrak{g}_p$. Since $\mathrm{ad}(h)^{p^2} = \mathrm{ad}(h)$ it follows that $\bar{\mathfrak{g}}_p$ is isomorphic to $\mathfrak{g}_p \ltimes k_p d$ where $d = \mathrm{ad}(h)^p \in \mathrm{Der}_k(\mathfrak{g}_p)$. Any linear form on $\bar{\mathfrak{g}}_p$ satisfying $\chi(x) \neq 0 \neq \chi(y)$ has $\bar{\mathfrak{g}}_p^\chi = 0$ and so $\mathrm{ind}\,\bar{\mathfrak{g}}_p = 0$. Thanks to the universal property of $\bar{\mathfrak{g}}_p$, simple $\mathfrak{g}$-modules are precisely the same as simple $\bar{\mathfrak{g}}$-modules. Now we have $M(\mathfrak{g}_p) = M(\bar{\mathfrak{g}}_p) \geqslant p^2$, which

shows that (1) $\Rightarrow$ (2). Finally we show (2) $\Rightarrow$ (1). Suppose $\mathfrak{g}_p$ is restricted and so $\mathfrak{s}_p = kx \oplus ky$ is a unipotent abelian restricted Lie subalgebra. This implies that every simple module is one-dimensional. The argument in the last paragraph of the proof of Theorem 3.3 shows that every simple $\mathfrak{g}_p$-module is a quotient of a module induced from a one-dimensional $\mathfrak{s}_p$-module. Such induced modules have dimension p by (2.7) and so $M(\mathfrak{g}_p) \leqslant p$, implying (1). This concludes the proof.

$\square$

Appendix A. Appendix by Akaki Tikaradze

In this appendix a short, alternative proof of Theorem 1.2 is presented, which applies to group schemes defined over a finitely generated ring $R \subseteq \mathbb{C}$. As was noted previously, in order to prove the KW1 conjecture for a restricted Lie algebra $\mathfrak{g}$ it suffices to demonstrate that $M(\mathfrak{g}) \leqslant p^{\frac{1}{2}(\dim \mathfrak{g} - \operatorname{ind} \mathfrak{g})}$. Thanks to the work of Zassenhaus this is equivalent to showing that the dimension of the skew division ring $D(\mathfrak{g})$ of fractions of $U(\mathfrak{g})$ is a field extension of rank $\leqslant p^{\dim \mathfrak{g} - \operatorname{ind} \mathfrak{g}}$ over its centre (see Lemma A.5 for more detail); this shall be proven by combining Rosenlicht's theorem with reduction modulo p and deformation arguments. As a by-product of the proof, a description of the centre of $D(\mathfrak{g})$ is obtained which confirms a slight modification of a conjecture of Kac [Kac95].

Given a commutative (noncommutative Noetherian) domain R, denote by $\operatorname{Frac}(R)$ its quotient field (skew field) of fractions. If R is commutative and M is any R-module and S is an R-algebra write $M_S := M \otimes_R S$ and, when R is also an integral domain and M is finitely generated, we refer to $\dim_{\operatorname{Frac}(R)} M_{\operatorname{Frac}(R)}$ as *the rank of M*.

Continue to write k for a field of characteristic $p > 0$. Given a restricted Lie algebra $\mathfrak{g}$ over k recall that $Z_p(\mathfrak{g})$ denotes the p-centre of $\mathfrak{g}$. Furthermore, whenever G is an R-group scheme and k is an R-field write $\mathfrak{g}_k$ for the Lie algebra of the scheme G_k obtained by base change.

Theorem A.1. *Let $R \subset \mathbb{C}$ be a finitely generated ring, let G be an R-group scheme and $R \to k$ a base change to an algebraically closed field. Then provided $\operatorname{char}(k) = p \gg 0$ the KW1 conjecture holds for $\mathfrak{g}_k$.*

As a consequence of the proof of Theorem A.1, we also show the following.

Theorem A.2. *Let G be a group scheme over a finitely generated ring $R \subseteq \mathbb{C}$. Then provided $\operatorname{char}(k) = p \gg 0$ the center of $D(\mathfrak{g}_k)$ is generated as a field by $Z_p(\mathfrak{g}_k)$ along with central elements obtained by reduction modulo p.*

For the proof we will need to recall couple of simple lemmas from commutative algebra.

Lemma A.3. *Let $R \subset \mathbb{C}$ be a finitely generated ring. Let A be a finitely generated commutative algebra over R such that $A_{\mathbb{C}}$ is a domain. Let $B \subset A$ be a finitely generated R-subalgebra. Then for all $p \gg 0$ and any base change $R \to k$ to an algebraically closed field of characteristic p the rank of A_k over $B_k A_k^p$ is $p^{\dim(A) - \dim(B)}$, where $\dim(A)$ and $\dim(B)$ denote the Krull dimension of A and B respectively.*

Proof. By localizing B if necessary, we may assume by the Noether normalization lemma that A is a finite module over $B[x_1, ..., x_n]$, where $x_1, ...x_n \in A$ are algebraically independent over B. Let m be a number of generators of A as a module over $B[x_1, ..., x_n]$. Since A is a finite extension of $B[x_1, ..., x_n]$ we have $n = \dim(A) - \dim(B)$. Now let $S \to k$ be a base change to an algebraically closed field of characteristic $p \gg 0$ (in particular $p > m$.) So A_k is a finite module with at most m generators over $B_k[x_1, \cdots, x_n]$. Clearly the rank of A_k over $B_k[x_1^p, ..., x_n^p] \subset B_k A_k^p$ is $p^n l$, where $l \leqslant m$ is the rank of A_k over $B_k[x_1, \cdots, x_n]$. On the other hand, it can easily be seen that if K is a field of characteristic $p > 0$ which is finitely generated over a perfect subfield, then K/K^p is a finite extension and $[K : K^p]$ is a power of p (by picking a transcendence basis over the perfect subfield we can reduce to the case of finite field extensions, and then use the fact that every finite extension of a perfect field is perfect). It follows that the rank A_k over A_k^p is a power of p. So, the rank of A_k over $B_k A_k^p$ is a power of p and divides $p^n l$, hence it must divide p^n. However, the rank of $B_k A_k^p$ over $B_k[x_1^p, ..., x_n^p]$ is at most m. Thus the rank of A_k over $B_k A_k^p$ is $p^{\dim(A) - \dim(B)}$. $\qquad\square$

Lemma A.4. *Let R be a nonnegatively filtered commutative algebra over a field k such that $\mathrm{gr}(R)$ is a finitely generated k-domain. Let M be a filtered R-module such that $\mathrm{gr}(M)$ is a finitely generated $\mathrm{gr}(R)$-module. Then the rank of M over R equals the rank of $\mathrm{gr}(M)$ over $\mathrm{gr}(R)$.*

For a proof of Lemma A.4 see for example [Tik11, Lemma 2.3]. For a more general result covering noncommutative algebras see [Gor07, Lemma 6.2]. We record one final useful lemma which is needed to complete the proof of Theorems A.1 and A.2.

Lemma A.5. *If $\mathfrak{g}$ is a restricted Lie algebra over an algebraically closed field k, then the following are equivalent:*

  (i) *the first Kac–Weisfeiler conjecture holds for $\mathfrak{g}$;*
  (ii) *the rank of $U(\mathfrak{g})$ over $Z(\mathfrak{g})$ is at most $p^{\dim \mathfrak{g} - \mathrm{ind}\,\mathfrak{g}}$;*
  (iii) *the rank of $Z(\mathfrak{g})$ over $Z_p(\mathfrak{g})$ is at least $p^{\mathrm{ind}(\mathfrak{g})}$.*

Proof. It was demonstrated in [Zas54, Theorem 6] that $M(\mathfrak{g})^2$ equals the rank of $U(\mathfrak{g})$ over $\mathrm{Frac}\,Z(\mathfrak{g})$, hence (i) holds if and only if we have equality in (ii). The inequality $M(\mathfrak{g})^2 \geqslant p^{\dim \mathfrak{g} - \mathrm{ind}\,\mathfrak{g}}$ was deduced in [PS99, Remark 5.4] and so (i) $\Leftrightarrow$ (ii). The equivalence (ii) $\Leftrightarrow$ (iii) follows from the fact that the rank of $U(\mathfrak{g})$ over $Z_p(\mathfrak{g})$ is $p^{\dim \mathfrak{g}}$. $\qquad\square$

Proof of Theorems A.1 and A.2. Let G be the connected complex algebraic group corresponding to $\mathfrak{g}_{\mathbb{C}}$. Let m be the index of $\mathfrak{g}_{\mathbb{C}}$. By Rosenlicht's theorem $\mathbb{C}(\mathfrak{g}_{\mathbb{C}}^*)^G$ has transcendence degree m over $\mathbb{C}$. Let $f_i, g_i \in \mathbb{C}[\mathfrak{g}_{\mathbb{C}}^*]$ be elements such that

$$\left\{ \frac{f_i}{g_i} \in \mathbb{C}(\mathfrak{g}_{\mathbb{C}}^*)^G \mid 1 \leqslant i \leqslant m \right\}$$

are algebraically independent elements, written as reduced fractions. We write $S_R(\mathfrak{g})$ for the symmetric R-algebra generated by the R-module $\mathfrak{g}$, and identify $\mathbb{C}(\mathfrak{g}_{\mathbb{C}}^*)$ with $\mathrm{Frac}\,S(\mathfrak{g}_{\mathbb{C}})$. By localizing R if necessary, we may assume that $f_i, g_i \in S_R(\mathfrak{g}), 1 \leqslant i \leqslant m$. Denote by ϕ_i (respectively ψ_i) the image of f_i (respectively g_i) under the symmetrization map $S(\mathfrak{g}_{\mathbb{C}}) \to U(\mathfrak{g}_{\mathbb{C}})$. Localizing R further if necessary we can assume that ϕ_i, ψ_i are

elements of the enveloping R-algebra $U_R(\mathfrak{g})$ (the R-tensor algebra of $\mathfrak{g}$ modulo the usual relations). It is well-known that ϕ_i, ψ_i are semi-invariants for the action of $\mathfrak{g}_\mathbb{C}$ of the same weight. After localising R further we deduce that there is an R-linear map $\chi_i : \mathfrak{g} \to R$ such that $\mathrm{ad}(x)\phi_i = \chi_i(x)\phi_i$ and $\mathrm{ad}(x)\psi_i = \chi_i(x)\psi_i$ for all $x \in \mathfrak{g}$. Now if $R \to k$ is a base change to any algebraically closed field then it follows that the quotient $\frac{\phi_i \otimes 1}{\psi_i \otimes 1} \in \mathrm{Frac}\, U(\mathfrak{g}_k)$ is central. Furthermore it follows from elementary linear algebra that $m = \mathrm{ind}(\mathfrak{g}_k)$ provided $\mathrm{char}(k) = p \gg 0$.

Thanks to Lemma A.5, to establish the KW1 conjecture for $\mathfrak{g}_k$ we need to show that the rank of $U(\mathfrak{g}_k)$ over $Z(U(\mathfrak{g}_k))$ is at most $p^{\dim \mathfrak{g}_k - m}$. For this purpose, it is enough to show that the rank of $S(\mathfrak{g}_k)$ as a $\mathrm{gr}(Z(U(\mathfrak{g}_k)))$-module is at most $p^{\dim \mathfrak{g}_k - m}$ thanks to Lemma A.4. Let $z_i \in U(\mathfrak{g}_k)$ be such that $\psi_i z_i \in Z(U(\mathfrak{g}_k))$. So $\phi_i z_i \in Z(U(\mathfrak{g}_k))$. Now since

$$\mathrm{gr}(\phi_i)\,\mathrm{gr}(z_i), \mathrm{gr}(\psi_i)\,\mathrm{gr}(z_i) \in \mathrm{gr}\, Z(U(\mathfrak{g}_k)),$$

it follows that

$$\frac{f_i \otimes 1}{g_i \otimes 1} \in \mathrm{Frac}(\mathrm{gr}\, Z(U(\mathfrak{g}_k))), 1 \leqslant i \leqslant m. \tag{A.1}$$

If we put $A = S_R(\mathfrak{g})[g_1^{-1}, ..., g_m^{-1}]$ and $B = R[\frac{f_1}{g_1}, \cdots, \frac{f_m}{g_m}]$, then for any base change $R \to k$ we may view A_k and B_k as subalgebras of $\mathrm{Frac}\, S(\mathfrak{g}_k)$. Since $\psi_i \otimes 1$ is a semi-invariant for $\mathrm{ad}(\mathfrak{g}_k)$ it follows that $\psi_i^p \otimes 1 \in U(\mathfrak{g}) \otimes_R k \cong U(\mathfrak{g}_k)$ is actually central for $i = 1, ..., p$. Therefore $g_i^p \otimes 1 = \mathrm{gr}\, \psi_i^p \otimes 1 \in \mathrm{gr}\, Z(U(\mathfrak{g}_k))$. Combining this with (A.1) it follows that $\mathrm{Frac}(\mathrm{gr}\, Z(U(\mathfrak{g}_k)))$ contains $A_k^p B_k$, and so it suffices to show that the rank of A_k over $A_k^p B_k$ is at most $p^{\dim \mathfrak{g}_k - m}$, which follows from Lemma A.3. This completes the proof of Theorem A.1.

Applying Lemma A.5, we see that the rank of $Z(\mathfrak{g}_k)$ over $Z_p(\mathfrak{g}_k)$ is p^m for $\mathrm{char}\,k \gg 0$. Let Q denote the subfield of $\mathrm{Frac}\, Z(\mathfrak{g}_k)$ generated by $\mathrm{Frac}\, Z_p(\mathfrak{g}_k)$ and the elements

$$\frac{\phi_i \otimes 1}{\psi_i \otimes 1} \text{ for } i = 1, ..., m.$$

The above argument actually shows that $[D(\mathfrak{g}) : Q] = p^{\dim \mathfrak{g} - m}$, which implies $[Q : \mathrm{Frac}\, Z_p(\mathfrak{g})] = p^m$. It follows that the inclusion $Q \subseteq \mathrm{Frac}\, Z(\mathfrak{g}_k)$ must be an equality. This completes the proof of Theorem A.2.

$\square$

Remark A.6. Let $\mathfrak{g}$ be a Lie algebra of a $\mathbb{Z}$-group scheme and k be a field of large characteristic $p > 0$. Then it is natural to ask whether the center of $U(\mathfrak{g}_k)$ is generated by $Z_p(\mathfrak{g}_k)$ and the mod p reduction of the center of $U(\mathfrak{g})$ (this was conjectured by Kac in [Kac95]). Unfortunately this is not always true: let $\mathfrak{g}$ be a three-dimensional free $\mathbb{Z}$-module spanned by h, x, y with Lie brackets given by

$$[h, x] = nx, [h, y] = my, [x, y] = 0, n, m \in \mathbb{Z}_{>0}, (n, m) = 1.$$

Then the center of $U(\mathfrak{g}_k)$ is generated by $h^p - h, x^p, y^p, x^i y^j$ where $ni + mj = 0 \mod p$ and $0 < i, j < p$. On the other hand the center of $U(\mathfrak{g})$ is trivial, hence $Z(U(\mathfrak{g}_k)) \neq Z_p(\mathfrak{g}_k)$. Meanwhile, the center of $D(\mathfrak{g}_\mathbb{C})$ is generated by the elements $x^m y^{-n}$ which are also generators for the centre of $D(\mathfrak{g}_k)$ over $Z_p(\mathfrak{g}_k)$.

References

[DG70] M. Demazure and P. Gabriel, *Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs*, Masson & Cie, Éditeur, Paris, 1970, Avec un appendice *Corps de classes local* par M. Hazewinkel.

[Dix96] J. Dixmier, *Enveloping algebras*, Graduate Studies in Mathematics, vol. 11, American Mathematical Society, Providence, RI, 1996, Revised reprint of the 1977 translation. MR 1393197 (97c:17010)

[Gor07] I. Gordon, *Gelfand-Kirillov conjecture for symplectic reflection algebras*, arxiv:0710.1419v2.pdf (2007).

[Jac37] Nathan Jacobson, *Abstract derivation and Lie algebras*, Trans. Amer. Math. Soc. **42** (1937), no. 2, 206–224. MR 1501922

[Jan98] Jens Carsten Jantzen, *Representations of Lie algebras in prime characteristic*, Representation theories and algebraic geometry (Montreal, PQ, 1997), NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., vol. 514, Kluwer Acad. Publ., Dordrecht, 1998, Notes by Iain Gordon, pp. 185–235. MR 1649627

[Jan03] J. C. Jantzen, *Representations of algebraic groups*, second ed., Mathematical Surveys and Monographs, vol. 107, American Mathematical Society, Providence, RI, 2003. MR MR2015057 (2004h:20061)

[Kac95] V. Kac, *Featured Math. review of* Irreducible representations of reductive Lie algebras of reductive groups and the Kac–Weisfeiler conjecture *by A. Premet.*, Invent. Math. **121** (1995), no. 1, 79–117.

[Mar02] David Marker, *Model theory*, Graduate Texts in Mathematics, vol. 217, Springer-Verlag, New York, 2002, An introduction. MR 1924282

[Mil75] A. A. Mil'ner, *Irreducible representations of modular Lie algebras*, Izv. Akad. Nauk SSSR Ser. Mat. **39** (1975), no. 6, 1240–1259, 1437.

[Mil17] J. S. Milne, *Algebraic groups*, Cambridge Studies in Advanced Mathematics, vol. 170, Cambridge University Press, Cambridge, 2017, The theory of group schemes of finite type over a field. MR 3729270

[PS99] Alexander Premet and Serge Skryabin, *Representations of restricted Lie algebras and families of associative $\mathcal{L}$-algebras*, J. Reine Angew. Math. **507** (1999), 189–218. MR 1670211

[SF88] H. Strade and R. Farnsteiner, *Modular Lie algebras and their representations*, Monographs and Textbooks in Pure and Applied Mathematics, vol. 116, Marcel Dekker Inc., New York, 1988. MR 929682 (89h:17021)

[Tik11] Akaki Tikaradze, *On the Azumaya locus of almost commutative algebras*, Proc. Amer. Math. Soc. **139** (2011), no. 6, 1955–1960. MR 2775371

[Top17] Lewis Topley, *A non-restricted counterexample to the first Kac-Weisfeiler conjecture*, Proc. Amer. Math. Soc. **145** (2017), no. 5, 1937–1942. MR 3611310

[VK71] B. Ju. Veĭsfeĭler and V. G. Kac, *The irreducible representations of Lie p-algebras*, Funkcional. Anal. i Priložen. **5** (1971), no. 2, 28–36. MR 0285575

[Zas54] Hans Zassenhaus, *The representations of Lie algebras of prime characteristic*, Proc. Glasgow Math. Assoc. **2** (1954), 1–36. MR 0063359

Benjamin Martin

Department of Mathematics, University of Aberdeen, King's College, Fraser Noble Building, Aberdeen AB24 3UE, United Kingdom

B.Martin@abdn.ac.uk

David I. Stewart

School of Mathematics and Statistics, Herschel Building, Newcastle, NE1 7RU, UK

`david.stewart@ncl.ac.uk`

Lewis Topley

School of Mathematics, Statistics and Actuarial Science, University of Kent, Canterbury, United Kingdom CT2 7FS

`L.Topley@kent.ac.uk`

Akaki Tikaradze

Department of Mathematics, Mail Stop 942, University of Toledo, 2801 W. Bancroft Street, Toledo, OH 43606-3390, USA

`Akaki.Tikaradze@utoledo.edu`