Linear Algebra and its Applications 713 (2025) 1–17

Contents lists available at ScienceDirect

Linear Algebra and its Applications

journal homepage: www.elsevier.com/locate/laa

# Two-generation of traceless matrices over finite fields ☆

Omer Cantor [a], Urban Jezernik [b,*], Andoni Zozaya [c]

[a] *Department of Mathematics, University of Haifa, 199 Abba Khoushy Avenue, Haifa, Israel*
[b] *Faculty of Mathematics and Physics, University of Ljubljana and Institute of Mathematics, Physics, and Mechanics, Jadranska 19, 1000 Ljubljana, Slovenia*
[c] *Department of Statistics, Computer Science and Mathematics, Public University of Navarre (UPNA), Arrosadia Campus, 31006 Pamplona, Spain*

A R T I C L E I N F O

*Article history:*
Received 24 May 2024
Received in revised form 20 February 2025
Accepted 22 February 2025
Available online 28 February 2025
Submitted by R.A. Brualdi

*MSC:*
17B05
17A04

*Keywords:*
Generation
Simple Lie algebra
Finite field

A B S T R A C T

We prove that the Lie algebra $\mathfrak{sl}_n(\mathbf{F}_q)$ of traceless matrices over a finite field of characteristic $p$ can be generated by 2 elements with exceptions when $(n, p)$ is $(3, 3)$ or $(4, 2)$. In the latter cases, we establish curious identities that obstruct 2-generation.



☆ OC is supported by the Israel Science Foundation grant 721/24. UJ is supported by the Slovenian Research Agency program P1-0222 and grants J1-50001, J1-4351, J1-3004, N1-0217. AZ was supported by the Slovenian Research Agency programs P1-0222, P1-0294 and grants J1-50001, J1-4351, N1-0216 during his previous affiliation with the University of Ljubljana.

* Corresponding author.
*E-mail addresses:* ocantor@proton.me (O. Cantor), urban.jezernik@fmf.uni-lj.si (U. Jezernik), andoni.zozaya@unavarra.es (A. Zozaya).

https://doi.org/10.1016/j.laa.2025.02.023

## 1. Introduction

In the study of algebraic structures, the concept of generation – specifically, the ability of a small number of elements to generate an entire structure – plays a crucial role in understanding their complexities and capabilities. A particularly notable generation property observed across *simple* algebraic structures is their tendency to be generated by merely *two* elements.

This 2-generation phenomenon is well-established across various classical algebraic structures over *classical fields* such as the complex numbers. For simple associative algebras, this property is underscored by the classical Burnside irreducibility theorem, which posits that over algebraically closed fields, any two matrices without a common nontrivial invariant subspace generate the whole matrix algebra. Similarly, for simple algebraic groups, it is a result of Guralnick [8, Theorem 3.3] that over an algebraically closed field of any characteristic, a simple algebraic group $G$ is topologically 3/2-generated, meaning that for every nontrivial $x$ there exists $y$ so that $\langle x, y\rangle$ is dense in $G$. Furthermore, simple Lie algebras over any field of characteristic 0 have been shown to be 2-generated by Kuranishi [12] (see also [2] for a more generic approach), and explicit generating pairs were found by Grozman and Leites [13]. This was extended to 3/2-generation in characteristic 0 by Ionescu [10] and in infinite fields of positive characteristic $p > 3$ by Bois [3]. More recently, Chistopolskaya [4] has explored nilpotent pairs of generators in traceless matrices.

Within the context of *finite fields*, there are analogous results for simple associative algebras, such as explicit generating pairs for matrices over integers provided by Petrenko and Sidki [16, Example 2.6], which project to matrices over finite fields. Additionally, Neumann and Praeger [15] have demonstrated that random pairs of matrices over a finite field generate the whole algebra with high probability as the field's size increases. Similar advancements have been made for finite simple groups, with Steinberg [17] proving that finite simple Chevalley groups are 2-generated, and subsequently Aschbacher and Guralnick [1] establishing 2-generation for all finite simple groups. Research into 2-generation of Lie algebras over finite fields remains comparatively underexplored. This paper aims to address that gap.

**Theorem.** *Let $\mathbf{F}_q$ be a finite field of characteristic $p$. Then the simple Lie algebra $\mathfrak{psl}_n(\mathbf{F}_q)$ is 2-generated as long as $(n, p) \neq (3, 3), (4, 2)$.*

We show that both $\mathfrak{psl}_3(\mathbf{F})$ and $\mathfrak{psl}_4(\mathbf{F})$ are, intriguingly, *not* 2-generated when $\mathbf{F}$ is any field of characteristic 3 and 2 respectively. However, these Lie algebras do allow for 3-generation. These are, to the best of our knowledge, the first known examples of simple Lie algebras over infinite fields that are not generated by two elements, thus answering [6, Question 2.3] as well as [4, Problem 2].

The strategy of the proof is outlined as follows. Our argument rests on the concept of *consistent matrices* (Section 2) in $\mathfrak{sl}_n(\mathbf{F}_q)$. We explain what these matrices are, where they come from and how they can be used to prove 2-generation of $\mathfrak{sl}_n(\mathbf{F}_q)$, and consequently of $\mathfrak{psl}_n(\mathbf{F}_q)$, as long as they exist. When $n$ is fixed and the field $\mathbf{F}_q$ is large enough in terms of $n$ (this is the case of *bounded rank*, Section 3), we can produce these matrices from suitable subsets of integers related to distinct sum sets from additive combinatorics. On the other hand, when $n$ tends to infinity and the field is small (this is the case of *unbounded rank*, Section 4), we produce generating pairs from companion matrices of suitable elements in extensions of $\mathbf{F}_q$. In the simple case, when $p$ does not divide $n$, normal elements do the job. In the modular case, when $p$ divides $n$, we replace normal elements by developing their traceless version which we call sharply traceless elements. *Even characteristic* (Section 5) requires special care and a further step to reach 2-generation. The *exceptional cases* (Section 6) that our method does not cover are the Lie algebras $\mathfrak{psl}_3(\mathbf{F}_q)$ and $\mathfrak{psl}_4(\mathbf{F}_q)$ in characteristics 3 and 2 respectively. We demonstrate that these algebras are not 2-generated by establishing a curious identity between any two elements in these Lie algebras that obstructs 2-generation.

## 2. Consistent matrices

An important ingredient of our proof of 2-generation consists of *consistent matrices*. These are traceless diagonal matrices

$$D = \mathrm{diag}(\lambda_1, \lambda_2, \dots, \lambda_n) \in \mathfrak{sl}_n(\mathbf{F})$$

over a field $\mathbf{F}$ satisfying the condition

$$\lambda_i - \lambda_j = \lambda_k - \lambda_l \quad \text{if and only if} \quad (i,j) = (k,l) \text{ or } (i,k) = (j,l). \tag{1}$$

The set of diagonal elements of a consistent matrix $D$ is called a *consistent set*. For example, over a field $\mathbf{F}$ of characteristic 0, the following is a consistent set for any $n \geq 2$:

$$\left\{1, 2, 2^2, 2^3, \dots, 2^{n-2}, 1 - 2^{n-1}\right\}. \tag{2}$$

Note that when $\mathrm{char}(\mathbf{F}) = 2$, one has $\lambda_i - \lambda_j = \lambda_j - \lambda_i$ for any $i, j$, so no consistent set exists. We will deal with even characteristic separately in Section 5.

Consistent matrices were implicitly used by Kuranishi [12] in the study of 2-generation of semisimple Lie algebras of characteristic 0, and were further inspected by Chistopolskaya [4] who was looking for pairs of nilpotent generators of Lie algebras over infinite fields. The relevance of consistent matrices to 2-generation is as follows. Let

$$\mathbf{1} = E - I \in \mathfrak{sl}_n(\mathbf{F}),$$

where $E$ is the matrix with all entries equal to 1 and $I$ is the identity matrix.

**Proposition 2.1** *([3, Theorem 2.2.3], [4, Lemma 1]). Let $D$ be a consistent matrix. Then $D$ and $\mathbf{1}$ generate the Lie algebra $\mathfrak{sl}_n(\mathbf{F})$.*

**Proof.** Let $D = \operatorname{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$ and observe that for every $k \geq 1$, we have

$$[\mathbf{1}, D, \overset{k}{\ldots}, D] = \left((\lambda_j - \lambda_i)^k\right)_{i,j}.$$

Thus the coefficients of the matrices $\mathbf{1}$, $[\mathbf{1}, D]$, ..., $[\mathbf{1}, D, \overset{n^2-n}{\ldots}, D]$ written in the standard basis $\{E_{ij} \mid i \neq j\}$ form a Vandermonde matrix with determinant

$$\prod_{\substack{i,j,k,l \\ i\neq j, k\neq l, (i,j)\neq(k,l)}} \left((\lambda_i - \lambda_j) - (\lambda_k - \lambda_l)\right),$$

which is nonzero as $D$ is consistent. Therefore the Lie algebra generated by $D$ and $\mathbf{1}$ contains the set $\{E_{ij} \mid i \neq j\}$, and as $[E_{ij}, E_{ji}] = E_{ii} - E_{jj}$, it thus contains all traceless matrices. □

## 3. Bounded rank

Using consistent matrices, we can easily find 2 generators for Lie algebras $\mathfrak{sl}_n(\mathbf{F}_q)$ of *bounded rank*, meaning that $n \geq 2$ is fixed and either the characteristic $p$ of the field $\mathbf{F}_q$ is large enough in terms of $n$, or $q$ is large enough in terms of $p$ and $n$.

Our argument here goes through the following remark. Suppose $S = \{s_1, s_2, \ldots, s_n\}$ is a subset of the vector space $\mathbf{F}_q$ over $\mathbf{F}_p$ consisting of $n$ elements. We call $S$ *sharply traceless* if

$$\textstyle\sum_{i=1}^n s_i = 0 \quad \text{and} \quad \dim_{\mathbf{F}_p}\langle S\rangle = n - 1.$$

In other words, the only linear relation up to a scalar between the vectors of $S$ is that their sum is 0.

**Lemma 3.1.** *A sharply traceless set of size $n$ is consistent if and only if $p \neq 2$ and $(n, p) \neq (3, 3)$.*

**Proof.** No consistent sets exist in even characteristic. Assume now that $p \neq 2$. A relation violating consistency $s_i - s_j = s_k - s_l$ involves at most 4 elements, so the set is consistent if $n \geq 5$. When $n = 4$, there are no linear relations involving at most 3 terms, so a violating relation can be a scalar multiple of the sum zero relation only when $p = 2$. Similarly, when $n = 3$, consistency can be violated only when $p = 2$ or $p = 3$ (for example in the form $s_1 - s_2 = s_2 - s_3$, a relation that is equivalent to sum zero). Conversely, in case $(n, p) = (3, 3)$, a sharply traceless set $\{s_1, s_2, s_3\}$ always satisfies $s_3 - s_2 = s_2 - s_1$, so it is not consistent. Finally, when $n = 2$, a sharply traceless set $\{s, -s\}$ with $s \neq 0$ is consistent provided $p \neq 2$. □

It is not difficult to construct sharply traceless sets as long as the field is large enough.

**Proposition 3.2.** *Let $p \neq 2$, $(n, p) \neq (3, 3)$, $q \geq p^{n-1}$. Then $\mathfrak{sl}_n(\mathbf{F}_q)$ is 2-generated.*

**Proof.** Let $k \geq n - 1$ and let $\mathbf{F}_{p^k}$ be an extension of $\mathbf{F}_p$ of degree $k$ with some vector space basis $B = \{\lambda_1, \lambda_2, \ldots, \lambda_k\}$. Let

$$S = \{\lambda_1, \lambda_2, \ldots, \lambda_{n-1}, -\textstyle\sum_{i=1}^{n-1} \lambda_i\} \subseteq \mathbf{F}_{p^k}.$$

Note that $S$ is sharply traceless, therefore it is consistent and so $\mathfrak{sl}_n(\mathbf{F}_q)$ can be generated by 2 elements. □

On the other hand, whenever we have a consistent set $\{\lambda_1, \lambda_2, \ldots, \lambda_n\}$ with entries in the integers, we can project it modulo $p$. The projected set is consistent as long as $p > 4\max\{|\lambda_1|, |\lambda_2|, \ldots, |\lambda_n|\}$, in which case the matrices $\mathrm{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$ and $\mathbf{1}$ generate $\mathfrak{sl}_n(\mathbf{F}_p)$ over $\mathbf{F}_p$, and therefore $\mathfrak{sl}_n(\mathbf{F}_q)$ over $\mathbf{F}_q$.

Consistent sets with entries in positive integers are intimately related to the concept of *distinct sum sets* [7]. These are sets of integers $\{a_i\}_{i=0}^n$ with

$$0 = a_0 < a_1 < \cdots < a_n$$

and the property that the sums $a_i + a_j$ for $i < j$ represent each integer at most once. From such a set, one obtains the consistent set of integers

$$S = \{a_1, a_2, \ldots, a_n, -\textstyle\sum_{i=1}^{n} a_i\},$$

all of whose elements are of absolute value at most $n \cdot a_n$.

Much is known about existence of distinct sum sets. It is shown in [7, Theorem 1 (3)] that given $n$, one can construct such a set in which every element is of size at most $n^2 + O(n^{36/23})$, and therefore the associated consistent set consists of elements with absolute values bounded by $O(n^3)$. As a consequence, for $p = \Omega(n^3)$, the Lie algebra $\mathfrak{sl}_n(\mathbb{F}_q)$ is 2-generated.

## 4. Unbounded rank

We now construct generator matrices of $\mathfrak{sl}_n(\mathbf{F}_q)$ in *unbounded rank*, meaning that $n$ is arbitrarily large and both $p$ and $q$ might be small. Note that it follows from lower bounds on distinct sum sets in residue rings [7, Theorem 1 (4)] that no consistent sets exist over $\mathbf{F}_p$ when $p < n^2 - O(n)$, so the method we used in the previous section will have to be adapted.

### *4.1. Polynomials with consistent roots*

Our strategy in unbounded rank is to find an appropriate irreducible polynomial $f \in \mathbf{F}_q[x]$ whose roots form a consistent set, and thus its companion matrix $C$ belongs to $\mathfrak{sl}_n(\mathbf{F}_q)$ and diagonalizes in some finite extension $\mathbf{F}$ of $\mathbf{F}_q$ to a consistent matrix $D = PCP^{-1} \in \mathfrak{sl}_n(\mathbf{F})$. The matrices $D$ and $\mathbf{1}$ then generate the Lie algebra $\mathfrak{sl}_n(\mathbf{F})$.

**Example 4.1.** Let $n = 7$ and $q = 3$. Choose a representation of the finite field $\mathbf{F}_{3^7}$ as an extension of $\mathbf{F}_3$, say, as

$$\mathbf{F}_{3^7} = \mathbf{F}_3[\omega]/(\omega^7 - \omega^2 + 1).$$

Now consider the irreducible polynomial

$$x^7 - x^5 + x^3 - x^2 - x - 1 \in \mathbf{F}_3[x].$$

Its companion matrix $C \in \mathfrak{sl}_7(\mathbf{F}_3)$ diagonalizes over $\mathbf{F}_{3^7}$ as $D = PCP^{-1}$, where

$$D = \mathrm{diag}(\omega^{1766}, \omega^{1776}, \omega^{2046}, \omega^{592}, \omega^{682}, \omega^{926}, \omega^{956}).$$

The matrix $D$ is consistent over the field $\mathbf{F}_{3^7}$, so it generates $\mathfrak{sl}_7(\mathbf{F}_{3^7})$ together with the matrix $\mathbf{1}$. Observe that

$$P^{-1}\mathbf{1}P = \begin{pmatrix} \cdot & \cdot & 2 & \cdot & 1 & 2 & 2 \\ \cdot & 2 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 2 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 2 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 2 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 2 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 2 \end{pmatrix},$$

a matrix that surprisingly belongs to $\mathfrak{sl}_7(\mathbf{F}_3)$.

The following lemma shows that it is always possible to pull back the generating pair $D$ and $\mathbf{1}$ to the original $\mathfrak{sl}_n(\mathbf{F}_q)$, and moreover explains the peculiar form of the matrix $P^{-1}\mathbf{1}P$ as in the example. Recall the *Frobenius endomorphism*

$$\mathrm{Fr}\colon \mathbf{F}_{q^n} \to \mathbf{F}_{q^n}, \quad \lambda \mapsto \lambda^q.$$

The entries of $P$ and $P^{-1}\mathbf{1}P$ are related to the *field trace* of the extension $\mathbf{F}_{q^n}$ of $\mathbf{F}_q$, which computes, for a given $\alpha \in \mathbf{F}_{q^n}$, the sum of its Galois conjugates:

$$\mathrm{Tr}(\alpha) = \textstyle\sum_{i=0}^{n-1} \mathrm{Fr}^i(\alpha) = \sum_{i=0}^{n-1} \alpha^{q^i} \in \mathbf{F}_q.$$

**Lemma 4.2.** *Let $f \in \mathbf{F}_q[x]$ be an irreducible polynomial of degree $n$ and let $\alpha$ be a root of $f$ in a splitting field. Let $C$ be the companion matrix of $f$ with diagonal form*

$$D = PCP^{-1} = \operatorname{diag}\left(\alpha, \operatorname{Fr}(\alpha), \ldots, \operatorname{Fr}^{n-1}(\alpha)\right).$$

*Then*

$$P^{-1}\mathbf{1}P = \begin{pmatrix} n & \operatorname{Tr}(\alpha) & \cdots & \operatorname{Tr}(\alpha^{n-1}) \\ \cdot & \cdot & \cdots & \cdot \\ \vdots & \vdots & & \vdots \\ \cdot & \cdot & \cdots & \cdot \end{pmatrix} - I.$$

*In particular, $P^{-1}\mathbf{1}P$ belongs to $\mathfrak{sl}_n(\mathbf{F}_q)$.*

**Proof.** The polynomial $f$ splits completely in $\mathbf{F}_{q^n}$. Its roots are the Galois conjugates of $\alpha$, namely $\{\alpha, \operatorname{Fr}(\alpha), \ldots, \operatorname{Fr}^{n-1}(\alpha)\}$. These are in turn the eigenvalues of $C$. Let $e_1, e_2, \ldots, e_n$ be the standard basis of the vector space $(\mathbf{F}_{q^n})^n$. The *left* eigenvector of $C$ corresponding to $\alpha$ is

$$v_0 = \left(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\right),$$

and the eigenvector corresponding to $\operatorname{Fr}^i(\alpha)$ is $v_i = \operatorname{Fr}^i(v_0)$, where the Frobenius endomorphism is applied componentwise. The rows of $P$ consist precisely of the vectors $v_0, v_1, \ldots, v_{n-1}$. Setting $e = e_1 + e_2 + \cdots + e_n$, we thus have $Pe_1 = e$, hence $P^{-1}e = e_1$. This gives

$$e_i^{\mathrm{T}} P^{-1} e = \begin{cases} 1 & i = 1 \\ 0 & i \neq 1 \end{cases} \quad \text{and therefore} \quad e_i^{\mathrm{T}} P^{-1} E = \begin{cases} e^{\mathrm{T}} & i = 1 \\ 0 & i \neq 1, \end{cases}$$

as $E$ is the matrix with all columns equal to $e$. Now, since

$$e^{\mathrm{T}} P = v_0 + v_1 + \cdots + v_{n-1} = \left(\operatorname{Tr}(1), \operatorname{Tr}(\alpha), \operatorname{Tr}(\alpha^2), \ldots, \operatorname{Tr}(\alpha^{n-1})\right),$$

we obtain

$$P^{-1}EP = \begin{pmatrix} n & \operatorname{Tr}(\alpha) & \cdots & \operatorname{Tr}(\alpha^{n-1}) \\ \cdot & \cdot & \cdots & \cdot \\ \vdots & \vdots & & \vdots \\ \cdot & \cdot & \cdots & \cdot \end{pmatrix}.$$

The lemma follows as $\mathbf{1} = E - I$. □

**Corollary 4.3.** *Let $f \in \mathbf{F}_q[x]$ be an irreducible polynomial of degree $n$ whose roots in a splitting field form a consistent set. Then $\mathfrak{sl}_n(\mathbf{F}_q)$ is 2-generated.*

**Proof.** Let $\mathbf{F}$ be a splitting field for $f$. Let $C$ be the companion matrix of $f$. Since the roots of $f$ form a consistent set, we have $C \in \mathfrak{sl}_n(\mathbf{F}_q)$ and the eigenvalues of $C$, being the roots of $f$, are all distinct in $\mathbf{F}$. Therefore $C$ diagonalizes to a consistent matrix $D = PCP^{-1}$ for some $P \in \mathrm{GL}_n(\mathbf{F})$, which generates $\mathfrak{sl}_n(\mathbf{F})$ together with the matrix $\mathbf{1}$. Thus, according to [3, Proposition 1.1.3], there exist $n^2 - 1$ Lie monomials $\{g_i(X, Y)\}_i$ in two variables whose evaluations in $(D, \mathbf{1})$ span the vector space $\mathfrak{sl}_n(\mathbf{F})$ over $\mathbf{F}$. Since Lie polynomials are equivariant (meaning that if $g(X, Y)$ is a Lie polynomial, then $P^{-1}g(X, Y)P = g(P^{-1}XP, P^{-1}YP)$) the matrices $g_i(C, P^{-1}\mathbf{1}P) = P^{-1}g_i(D, \mathbf{1})P$ also span $\mathfrak{sl}_n(\mathbf{F})$ over $\mathbf{F}$. Now, both $C$ and $P^{-1}\mathbf{1}P$ belong to $\mathfrak{sl}_n(\mathbf{F}_q)$, and as each $g_i$ is a Lie monomial, its evaluation $g_i(C, P^{-1}\mathbf{1}P)$ is in $\mathfrak{sl}_n(\mathbf{F}_q)$. Therefore $C$ and $P^{-1}\mathbf{1}P$ generate $\mathfrak{sl}_n(\mathbf{F}_q)$ as a Lie algebra over $\mathbf{F}_q$. □

### *4.2. Normal elements*

We proceed by exhibiting an irreducible polynomial $f \in \mathbf{F}_q[x]$ of degree $n$ whose roots form a consistent set in the case when $\mathfrak{sl}_n(\mathbf{F}_q)$ is *simple*, *i.e.* the characteristic $p$ and degree $n$ are coprime.

In order to do so, we make use of the concept of a *normal element*, which is an element $\alpha \in \mathbf{F}_{q^n}$ whose Galois conjugates $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ form a basis of $\mathbf{F}_{q^n}$ as a vector space over $\mathbf{F}_q$. It is well-known that normal elements exist in any finite field [9].

Given a normal element $\alpha$, consider $\beta = \alpha - \mathrm{Tr}(\alpha)/n$. One can indeed construct this element since $n$ is invertible in $\mathbf{F}_q$. Note that $\beta$ is a traceless element and as $\alpha$ is normal, the Galois conjugates of $\beta$ form a consistent set.[1] Taking $f$ to be the minimal polynomial of $\beta$ then does the job.

**Corollary 4.4.** *Let $p \neq 2$ and $n$ coprime to $p$. Then $\mathfrak{sl}_n(\mathbf{F}_q)$ is 2-generated.*

### *4.3. Sharply traceless elements*

In case $p$ divides $n$, normal elements still exist, but there is no evident way of producing a *traceless* matrix from them.

In order to proceed, we will replace normal elements with their traceless version. To be more precise, we call an element $\alpha \in \mathbf{F}_{q^n}$ *sharply traceless* if its Galois conjugates over $\mathbf{F}_q$ form a sharply traceless set. In other words, $\alpha$ is traceless, meaning that the sum of its Galois conjugates is zero, and this is the only linear relation up to a scalar between the Galois conjugates.

**Theorem 4.5.** *Sharply traceless elements exist in any extension $\mathbf{F}_{q^n}/\mathbf{F}_q$.*

Generation of $\mathfrak{sl}_n(\mathbf{F}_q)$ now follows as in the previous section.

[1] The Galois conjugates of $\beta$ are $\alpha^{p^i} - \mathrm{Tr}(\alpha)/n$, so their pairwise differences are the same as the pairwise differences of Galois conjugates of $\alpha$.

**Corollary 4.6.** *Let $p \neq 2$ and $(n,p) \neq (3,3)$. Then $\mathfrak{sl}_n(\mathbf{F}_q)$ is 2-generated.*

**Proof.** A sharply traceless element gives a sharply traceless set of its Galois conjugates. The result follows from Lemma 3.1. □

Our proof of Theorem 4.5 relies on viewing the finite field $\mathbf{F}_{q^n}$ as a module over the modular group algebra of the Galois group $G = \mathrm{Gal}(\mathbf{F}_{q^n}/\mathbf{F}_q)$, generated by the Frobenius endomorphism Fr. More precisely, we consider the ring $\mathbf{F}_q[G] = \mathbf{F}_q[x]/(m(x))$, where $m(x) = x^n - 1$ is the minimal and at the same time characteristic polynomial of Fr (see [14, proof of Theorem 2.35]). We can express the trace in terms of the polynomial

$$\Phi(x) = \frac{m(x)}{x-1} = x^{n-1} + x^{n-2} + \cdots + 1,$$

since, for an element $\alpha \in \mathbf{F}_{q^n}$, we have $\mathrm{Tr}(\alpha) = \Phi(\mathrm{Fr})\alpha$. Consider now the module homomorphism

$$\eta\colon \mathbf{F}_q[G] \to \mathbf{F}_{q^n}, \quad t \mapsto t \cdot \alpha.$$

Note that $\eta$ is an isomorphism precisely when $\alpha$ is a normal element in $\mathbf{F}_{q^n}$. Write $t = \sum_{i=0}^{n-1} t_i \,\mathrm{Fr}^i$ and let $\epsilon(t) = \sum_{i=0}^{n-1} t_i$ be the augmentation of $t$. Then

$$\mathrm{Tr}(t \cdot \alpha) = \textstyle\sum_{i=0}^{n-1} t_i \,\mathrm{Tr}(\mathrm{Fr}^i(\alpha)) = \epsilon(t) \cdot \mathrm{Tr}(\alpha).$$

For a normal $\alpha$, we have $\mathrm{Tr}(\alpha) \neq 0$, and so elements of trace 0 in $\mathbf{F}_{q^n}$ correspond precisely to the image of the augmentation ideal under $\eta$. This ideal is generated by $\mathrm{Fr} - 1$, so traceless elements in $\mathbf{F}_{q^n}$ are generated by $(\mathrm{Fr}-1)(\alpha) = \alpha^q - \alpha$ as a module over $\mathbf{F}_q[G]$. The sharply traceless ones among these can be understood as follows.

**Lemma 4.7.** *Let $\alpha$ be a normal element in $\mathbf{F}_{q^n}$ and $\pi$ a polynomial in $\mathbf{F}_q[x]$. Then $\beta = \pi(\mathrm{Fr})(\mathrm{Fr}-1)(\alpha)$ is sharply traceless if and only if $\pi$ is coprime to $\Phi$.*

**Proof.** Suppose first that $\pi$ is coprime to $\Phi$. By Bézout, there are polynomials $a, b$ in $\mathbf{F}_q[x]$ so that $a\pi + b\Phi = 1$. Evaluating in Fr and applying to $(\mathrm{Fr}-1)(\alpha)$, we obtain $a(\mathrm{Fr})(\beta) = (\mathrm{Fr}-1)(\alpha)$. Hence if some polynomial $c$ in $\mathbf{F}_q[x]$ satisfies $c(\mathrm{Fr})(\beta) = 0$, then also $c(\mathrm{Fr})(\mathrm{Fr}-1)(\alpha) = 0$, and since $\alpha$ is normal, it follows that $\Phi$ divides $c$. Thus $\beta$ is sharply traceless.

Conversely, suppose that $\beta = \pi(\mathrm{Fr})(\mathrm{Fr}-1)(\alpha)$ is sharply traceless element. Note

$$\frac{\Phi}{\gcd(\pi,\Phi)}(\mathrm{Fr})(\beta) = m(\mathrm{Fr})\frac{\pi}{\gcd(\pi,\Phi)}(\mathrm{Fr})(\alpha) = 0.$$

As $\beta$ is sharply traceless, it follows that $\gcd(\pi,\Phi) = 1$. □

Note that two polynomials $\pi$, $\pi'$ in $\mathbf{F}_q[x]$ determine the same sharply traceless element $\beta$ if and only if $(\mathrm{Fr}-1)(\pi-\pi')(\mathrm{Fr})\alpha = 0$, which is equivalent to saying that $\Phi$ divides $\pi - \pi'$.

**Corollary 4.8.** *Sharply traceless elements in* $\mathbf{F}_{q^n}$ *are in bijective correspondence with the group of units of* $\mathbf{F}_q[x]/(\Phi(x))$.[2]

The number of these elements can be computed as follows. Let $\mathrm{Div}(\Phi)$ be the set of prime factors of $\Phi$. For a given $\pi \in \mathrm{Div}(\Phi)$, let $\mathrm{mult}(\pi)$ be the multiplicity of $\pi$ in $\Phi$. Then

$$\frac{\mathbf{F}_q[x]}{(\Phi(x))} \cong \prod_{\pi\in\mathrm{Div}(\Phi)} \frac{\mathbf{F}_q[x]}{(\pi(x)^{\mathrm{mult}(\pi)})}.$$

The invertible elements in each factor are polynomials that are coprime to $\pi$, so their number is

$$q^{\deg(\pi)\,\mathrm{mult}(\pi)} - q^{\deg(\pi)(\mathrm{mult}(\pi)-1)} = q^{\deg(\pi)\,\mathrm{mult}(\pi)}(1-q^{-\deg(\pi)}).$$

Note that $n-1 = \deg(\Phi) = \sum_{\pi\in\mathrm{Div}(\Phi)} \deg(\pi)\,\mathrm{mult}(\pi)$, implying the following.

**Corollary 4.9.** *The number of sharply traceless elements in* $\mathbf{F}_{q^n}$ *is*

$$q^{n-1} \prod_{\pi\in\mathrm{Div}(\Phi)} (1-q^{-\deg(\pi)}).$$

For example, when $n = 2$, we have $\Phi(x) = x + 1$, so we have $q - 1$ sharply traceless elements in $\mathbf{F}_{q^2}$, and this is precisely the same as the number of nonzero traceless elements. On the other hand, when $n = q = p$, we have $\Phi(x) = (x-1)^{p-1}$, so the number of sharply traceless elements in $\mathbf{F}_{p^p}$ is $p^{p-2}(p-1) = p^{p-1} - p^{p-2}$, whereas the number of nonzero traceless elements equals $p^{p-1} - 1$. In general, for a fixed $n$, the number given in the corollary is a polynomial in $q$ of degree $n - 1$, implying the following.

**Corollary 4.10.** *For any fixed* $n$*, a uniformly random traceless element of* $\mathbf{F}_{q^n}$ *is sharply traceless with probability tending to* 1 *as* $q$ *tends to infinity.*

An alternative (but longer) route[3] to proving Theorem 4.5 is by mimicking the usual approach for finding a normal element, compare with [18] or [14] and the closely related notion of a cyclic element from [15].

[2] The same argument gives that normal elements in $\mathbf{F}_{q^n}$ are in bijective correspondence with the group of units of $\mathbf{F}_q[x]/(m(x))$.

[3] We thank the referee for pointing out the simpler argument using group algebras.

## 5. Even characteristic

Our method for proving 2-generation in the previous sections used consistent matrices. These do not exist when the field is of characteristic 2. In this situation, we instead rely on *semiconsistent* matrices. These are traceless diagonal matrices

$$D = \operatorname{diag}(\lambda_1, \dots, \lambda_n) \in \mathfrak{sl}_n(\mathbf{F}_q)$$

that satisfy the condition

$$\lambda_i + \lambda_j = \lambda_k + \lambda_l \text{ if and only if } \{i, j\} = \{k, l\} \text{ or } (i, k) = (j, l).$$

(Compare with (1).) For instance, if $\alpha \in \mathbf{F}_{q^n}$ is a sharply traceless element, the diagonal matrix $\operatorname{diag}(\alpha, \operatorname{Fr}(\alpha), \dots, \operatorname{Fr}^{n-1}(\alpha))$ is semiconsistent in $\mathfrak{sl}_n(\mathbf{F}_{q^n})$ as long as $n \neq 4$.

**Proposition 5.1.** *Let $p = 2$ and $n \neq 2, 4$. Then $\mathfrak{sl}_n(\mathbf{F}_q)$ is 2-generated.*

**Proof.** It suffices to prove that $\mathfrak{sl}_n(\mathbf{F}_2)$ is 2-generated. Let $\alpha \in \mathbf{F}_{2^n}$ be a sharply traceless element with minimal polynomial $f \in \mathbf{F}_2[x]$ of degree $n$. Let $C \in \mathfrak{sl}_n(\mathbf{F}_2)$ be the companion matrix of $f$ with diagonal form

$$D = PCP^{-1} = \operatorname{diag}\left(\alpha, \operatorname{Fr}(\alpha), \dots, \operatorname{Fr}^{n-1}(\alpha)\right) \in \mathfrak{sl}_n(\mathbf{F}_{2^n}).$$

Since $\alpha$ is sharply traceless, $D$ is semiconsistent.

Now let $X = (x_{ij})_{i,j}$ be an arbitrary matrix in $\mathfrak{sl}_n(\mathbf{F}_{2^n})$. We have

$$[X, D, \overset{k}{\dots}, D] = \sum_{i<j} (\lambda_i + \lambda_j)^k \left(x_{ij} E_{ij} + x_{ji} E_{ji}\right),$$

so arguing as in the proof of Proposition 2.1, the matrix $A_{ij} = x_{ij} E_{ij} + x_{ji} E_{ji}$ for $i \neq j$ is contained in the Lie algebra generated by $X$ and $D$.

Let us consider $X = P(E_{21} + E_{13})P^T$. Recall from Lemma 4.2 that the rows of $P$ are $v_0, v_1, \dots, v_{n-1}$, where $v_0 = (1, \alpha, \alpha^2, \dots, \alpha^{n-1})$ and $v_i = \operatorname{Fr}^i(v_0)$. Thus

$$e_k^{\mathrm{T}} P E_{ij} P^T e_l = (e_k^{\mathrm{T}} P e_i)(e_j^{\mathrm{T}} P^T e_l) = \operatorname{Fr}^{k-1}(\alpha^{i-1}) \operatorname{Fr}^{l-1}(\alpha^{j-1})$$

and so

$$x_{kl} = \operatorname{Fr}^{k-1}(\alpha) \operatorname{Fr}^{l-1}(1) + \operatorname{Fr}^{k-1}(1) \operatorname{Fr}^{l-1}(\alpha^2) = \operatorname{Fr}^{k-1}(\alpha) + \operatorname{Fr}^{l}(\alpha).$$

Since we are in even characteristic and $\alpha$ is sharply traceless, $x_{kl} = 0$ if and only if $l \equiv k - 1 \pmod{n}$. In particular, $E_{n1} = x_{n1}^{-1} A_{n1}$ and $E_{i,i+1} = x_{i,i+1}^{-1} A_{i,i+1}$ for $1 \leq i \leq n-1$ are in the Lie algebra generated by $D$ and $X$. Since the matrices $E_{n1}$ and $E_{i,i+1}$ for

$1 \le i \le n-1$ generate $\mathfrak{sl}_n(\mathbf{F}_{2^n})$, the matrices $D$ and $X$ generate it as well, and so the matrices $C = P^{-1}DP$ and $P^{-1}XP = (E_{21} + E_{13})P^{\mathrm{T}}P$ also generate it.

Note, however, that both $C$ and $(E_{21} + E_{13})P^{\mathrm{T}}P$ belong to $\mathfrak{sl}_n(\mathbf{F}_2)$, since

$$e_k^{\mathrm{T}} P^{\mathrm{T}} P e_l = (Pe_k)^{\mathrm{T}}(Pe_l) = \sum_{i=0}^{n-1} \mathrm{Fr}^i(\alpha^{k-1})\,\mathrm{Fr}^i(\alpha^{l-1}) = \mathrm{Tr}(\alpha^{k+l-2})$$

for any $k, l$. Therefore, as in the proof of Corollary 4.3, the matrices $C$ and $(E_{21} + E_{13})P^{\mathrm{T}}P$ generate the Lie algebra $\mathfrak{sl}_n(\mathbf{F}_2)$. $\square$

We still have to take care of the Lie algebras of rank $n = 2$ and $n = 4$. Clearly $\mathfrak{sl}_2(\mathbf{F}_2)$ is 2-generated, for instance by $E_{12}$ and $E_{21}$. We deal with $\mathfrak{sl}_4(\mathbf{F})$ in Section 6.

## 6. Exceptional cases

There are two exceptions that our methods with sharply traceless elements do not cover, namely the families $\mathfrak{sl}_3(\mathbf{F}_q)$ with $\mathbf{F}_q$ of characteristic 3 and $\mathfrak{sl}_4(\mathbf{F}_q)$ with $\mathbf{F}_q$ of characteristic 2. We will prove that these algebras are in fact *not* 2-generated, even over *infinite* fields of corresponding characteristic. This failure of 2-generation comes as a surprise, since this is a property enjoyed throughout simple algebraic structures over finite and infinite fields as pointed out in Section 1. We will show that this is a phenomenon that heavily relies both on the modularity of the situation and on smallness of the rank.

### *6.1.* $(n, p) = (3, 3)$

**Theorem 6.1.** *Let* $\mathbf{F}$ *be a field of characteristic* 3*. Then any two elements of* $\mathfrak{sl}_3(\mathbf{F})$ *generate a Lie algebra of dimension at most* 4*. In particular,* $\mathfrak{sl}_3(\mathbf{F})$ *is not* 2*-generated. It is, however,* 3*-generated.*

Note that our result diverges from [4, Theorem 1], whose argument appears to hinge on the existence of a consistent matrix, but these do not exist in $\mathfrak{sl}_3(\mathbf{F})$ when $\mathbf{F}$ is of characteristic 3, see Lemma 3.1.

The claim that $\mathfrak{sl}_3(\mathbf{F})$ is 3-generated follows immediately from the fact that over the prime field $\mathbf{F}_3$ of $\mathbf{F}$, the matrices

$$A = \begin{pmatrix} 1 & \cdot & \cdot \\ \cdot & -1 & \cdot \\ \cdot & \cdot & \cdot \end{pmatrix}, \quad B = \begin{pmatrix} \cdot & \cdot & 1 \\ \cdot & \cdot & 1 \\ \cdot & \cdot & \cdot \end{pmatrix}, \quad B^{\mathrm{T}} = \begin{pmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ 1 & 1 & \cdot \end{pmatrix} \tag{3}$$

generate $\mathfrak{sl}_3(\mathbf{F}_3)$, and so they also generate $\mathfrak{sl}_3(\mathbf{F})$ over $\mathbf{F}$. Indeed, $[A, B] - B = E_{23}$ and $[A, B^{\mathrm{T}}] - B^{\mathrm{T}} = E_{31}$. Thus the Lie algebra generated by $A, B, B^{\mathrm{T}}$ contains $E_{13} = B - E_{23}$, $E_{32} = B^{\mathrm{T}} - E_{31}$, and therefore $[E_{23}, E_{31}] = E_{21}$ and $[E_{13}, E_{32}] = E_{12}$.

We shall derive Theorem 6.1 from the following curious identity in the quotient $\mathfrak{psl}_3(\mathbf{F})$ of the Lie algebra $\mathfrak{sl}_3(\mathbf{F})$ by the central ideal consisting of scalar multiples of the identity.

**Proposition 6.2.** *For any $x, y \in \mathfrak{sl}_3(\mathbf{F})$, the following identity holds in $\mathfrak{psl}_3(\mathbf{F})$:*

$$[x, y, y] = -\operatorname{Tr}(y^2)x + \operatorname{Tr}(xy)y.$$

This identity implies that for any $x, y \in \mathfrak{psl}_3(\mathbf{F})$, the vector space spanned by $x, y, [x, y]$ is closed with respect to Lie bracketing with $x$ and $y$. In other words, the Lie algebra generated by $x$ and $y$ is of dimension at most 3. Thus $\mathfrak{psl}_3(\mathbf{F})$ is not 2-generated. Furthermore, it follows from the same identity that any two elements in $\mathfrak{sl}_3(\mathbf{F})$ generate a Lie algebra of dimension at most 4. Note that this bound is sharp, for example the Lie algebra generated by the matrices $A$ and $B$ from (3) is of dimension 4.

**Proof of Proposition 6.2.** Let $x \in \mathfrak{sl}_3(\mathbf{F})$. The characteristic polynomial of $x$ is $t^3 + \alpha(x)t - \det(x)$, where $\alpha(x)$ is a form in $x$, computable as the elementary symmetric polynomial $e_2$ in the eigenvalues of $x$. By Newton's identities, $e_2$ can be expressed as $(p_1^2 - p_2)/2$, where $p_i$ are power sums. As $\operatorname{Tr}(x) = 0$ and $\mathbf{F}$ is of characteristic 3, it follows that $\alpha(x) = p_2(x) = \operatorname{Tr}(x^2)$. Therefore we have

$$x^3 + \operatorname{Tr}(x^2)x = 0 \tag{4}$$

in $\mathfrak{psl}_3(\mathbf{F})$. This identity holds over any field of characteristic 3, as well as any subquotient of such a field. We can thus multilinearize this identity by using it in the Lie algebra $\mathfrak{psl}_3(\mathbf{F}) \otimes_{\mathbf{F}} \mathbf{F}[T]/(T^2)$ with the element $Tx + y$ for any $x, y \in \mathfrak{sl}_3(\mathbf{F})$.[4] Note that, by Jacobson's formula [11],

$$(Tx + y)^3 = T^3x^3 + y^3 + [Tx, y, y] - [Tx, y, Tx] = y^3 + T[x, y, y]$$

since $T^2 = 0$, and similarly

$$\operatorname{Tr}((Tx + y)^2) = -T\operatorname{Tr}(xy) + \operatorname{Tr}(y^2).$$

By inserting $Tx + y$ into (4), we thus obtain $[x, y, y] - \operatorname{Tr}(xy)y + \operatorname{Tr}(y^2)x = 0$. □

In fact, when the *u-invariant*[5] of $\mathbf{F}$ is at most 2, the identity in Proposition 6.2 further implies that for generic choices of $x$ and $y$, the Lie algebra they generate is isomorphic to $\mathfrak{sl}_2(\mathbf{F})$. This occurs, for example, when $\mathbf{F}$ is finite or algebraically closed (see [5, Example 36.2]).

[4] We thank Alexander Premet who showed us this trick. It substantially shortens our previous argument.
[5] The largest integer $u(\mathbf{F}) \geq 0$ such that there exists an anisotropic quadratic form of dimension $u(\mathbf{F})$ over $\mathbf{F}$, or infinity if no such largest integer exists.

**Corollary 6.3.** *Let* $\mathbf{F}$ *be a field of characteristic* 3 *such that* $u(\mathbf{F}) \leq 2$*. Let* $x, y \in \mathfrak{sl}_3(\mathbf{F})$*. Let* $G \in \mathrm{M}_3(\mathbf{F})$ *be the Gram matrix of* $x, y, [x, y]$ *under the trace form. Then the Lie algebra generated by the images of* $x$ *and* $y$ *in* $\mathfrak{psl}_3(\mathbf{F})$ *is isomorphic to* $\mathfrak{sl}_2(\mathbf{F})$ *if and only if* $\det G \neq 0$.[6]

**Proof.** Suppose first that $G$ is nondegenerate. Hence $x, y, [x, y]$ are linearly independent. The restriction of the trace form to the span of $x, y, [x, y]$ is thus a nondegenerate quadratic form of dimension 3. This form is isotropic, so by the Witt decomposition theorem, it contains a hyperbolic plane spanned by some $e, f$. Thus $\mathrm{Tr}(e^2) = \mathrm{Tr}(f^2) = 0$ and $\mathrm{Tr}(ef) = 1$. Let $h = [e, f]$. Using Proposition 6.2, we then compute $[h, e] = 2e$ and $[h, f] = -2f$ in $\mathfrak{psl}_3(\mathbf{F})$. These formulas further imply that $e, f, h$ are linearly independent. After passing to $\mathfrak{psl}_3(\mathbf{F})$, the Lie algebra generated by $x$ and $y$ is thus isomorphic to $\mathfrak{sl}_2(\mathbf{F})$.

Assume now that $G$ is degenerate. We can assume that the Lie algebra generated by the images of $x, y$ in $\mathfrak{psl}_3(\mathbf{F})$ is of dimension 3. Hence $x, y, [x, y]$ are linearly independent and the restriction of the trace form to their span $L = \langle x, y, [x, y]\rangle$ is degenerate. Thus there is a nonzero $z \in L$ with $\mathrm{Tr}(zx) = \mathrm{Tr}(zy) = \mathrm{Tr}(z[x, y]) = 0$. Using Proposition 6.2, we conclude that $\mathrm{ad}_z$ is nilpotent of degree 2 on $\mathfrak{psl}_3(\mathbf{F})$. The Lie algebra $\mathfrak{sl}_2(\mathbf{F})$, however, does not contain nonzero nilpotent elements of degree 2 when $\mathbf{F}$ is of odd characteristic. This completes the proof. □

In particular, when $\mathbf{F}$ is finite the probability that a uniformly random tuple $x, y \in \mathfrak{sl}_3(\mathbf{F})$ belongs to the variety $\det G = 0$ is at most $8/|\mathbf{F}|$ by the Schwartz-Zippel lemma, which tends to 0 as $|\mathbf{F}|$ tends to infinity.

### *6.2.* $(n, p) = (4, 2)$

This case is handled using the same method.

**Theorem 6.4.** *Let* $\mathbf{F}$ *be a field of characteristic* 2*. Then any two elements of* $\mathfrak{sl}_4(\mathbf{F})$ *generate a Lie algebra of dimension at most* 9*. In particular,* $\mathfrak{sl}_4(\mathbf{F})$ *is not* 2*-generated. It is, however,* 3*-generated.*

It is not difficult to find 3 matrices in $\mathfrak{sl}_4(\mathbf{F})$ that generate the whole Lie algebra. One can take, for example,

$$A = \begin{pmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix}, \quad B = \begin{pmatrix} \cdot & \cdot & 1 & 1 \\ 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ 1 & 1 & \cdot & \cdot \end{pmatrix}, \quad B^{\mathrm{T}} = \begin{pmatrix} \cdot & 1 & \cdot & 1 \\ \cdot & \cdot & \cdot & 1 \\ 1 & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot \end{pmatrix}. \tag{5}$$

[6] It is not difficult to see that $\det G = (\mathrm{Tr}(x^2)\,\mathrm{Tr}(y^2) - (\mathrm{Tr}(xy))^2)(\mathrm{Tr}(x^2y^2) - \mathrm{Tr}((xy)^2))$.

Indeed, the Lie algebra $L$ generated by these elements contains $[A, B] + B = E_{21}$ and thus also $[E_{21}, B^{\mathrm{T}}] + A = E_{24} \in L$. Symmetrically, we obtain $E_{12}, E_{42} \in L$. Therefore $[E_{42}, E_{21}] = E_{41} \in L$ and symmetrically $E_{14} \in L$. It follows that $[E_{41}, E_{14} + B] = E_{43} \in L$ and thus $[E_{24}, E_{43}] = E_{23} \in L$. Symmetrically we obtain $E_{32} \in L$ and hence $[E_{32}, E_{21}] = E_{31} \in L$. This means that $L$ contains all nondiagonal elementary matrices, therefore $L = \mathfrak{sl}_4(\mathbf{F})$.

The difficult part of the proof of Theorem 6.4 again follows from an incidental identity that relies on just the right smallness of the rank and even characteristic.

**Proposition 6.5.** *There are forms $a, b, c, d$ on $\mathfrak{sl}_4(\mathbf{F})$ so that for any $x, y \in \mathfrak{sl}_4(\mathbf{F})$, the following identity holds in $\mathfrak{psl}_4(\mathbf{F})$:*

$$[x, y, y, y] = a(x, y)x + b(x, y)y + c(x, y)[x, y] + d(x, y)y^2.$$

For any $x, y \in \mathfrak{psl}_4(\mathbf{F})$, the Lie algebra generated by $x$ and $y$ contains the following elements:

$$x, y, [x, y], [x, y, y], [y, x, x], [x, y, y, y], [y, x, x, x], [x, y, x, y]. \tag{6}$$

Since the Lie algebra $\mathfrak{psl}_4(\mathbf{F})$ is 2-restricted, we have $\mathrm{ad}_{z^2} = (\mathrm{ad}_z)^2$ for any $z$. This implies that $[x, y, y, y] = [x, y, y^2]$ and $[x, y, x, y] = [y, x, x, y] = [y, x^2, y] = [x^2, y, y] = [x^2, y^2]$. It then follows from Proposition 6.5 that the elements (6) all belong to the vector space spanned by

$$x, y, [x, y], [x, y^2], [y, x^2], x^2, y^2, [x^2, y^2],$$

and at the same time this vector space is closed with respect to Lie bracketing with $x$ and $y$. In other words, the Lie algebra generated by $x$ and $y$ is of dimension at most 8. Thus $\mathfrak{psl}_4(\mathbf{F})$ is not 2-generated. Furthermore, it follows from the same identity that any two elements in $\mathfrak{sl}_4(\mathbf{F})$ generate a Lie algebra of dimension at most 9. Note that this bound is sharp, for example the Lie algebra generated by the matrices $B$ and $B^{\mathrm{T}}$ from (5) is of dimension 9.

**Proof of Proposition 6.5.** Let $x \in \mathfrak{sl}_4(\mathbf{F})$. The characteristic polynomial of $x$ is $t^4 + \alpha(x)t^2 - \beta(x)t + \det(x)$, where $\alpha, \beta$ are forms in $x$ with coefficients in $\mathbf{F}_2$.[7] Therefore we have

$$x^4 + \alpha(x)x^2 - \beta(x)x = 0 \tag{7}$$

[7] These forms are computable as elementary symmetric polynomials $e_2, e_3$ in the eigenvalues of $x$. As we are in characteristic 2, these polynomials are not expressible in terms of power sums, so the formula is not as clear as the one in the previous section.

in $\mathfrak{psl}_4(\mathbf{F})$. As in the proof of Proposition 6.2, we multilinearize this identity by using it with the element $Tx + y$ with $T^2 = 0$. By Jacobson's formula, we have

$$(Tx + y)^2 = y^2 + T[x, y] \quad \text{and so} \quad (Tx + y)^4 = y^4 + T[x, y, y^2].$$

Note that $\alpha(Tx + y), \beta(Tx + y)$ are polynomials in $T$, since they are expressible as coefficients of the polynomial $\det(tI - Tx - y)$ in $t$. Write $\alpha(Tx+y) = c+Td$ in $\mathbf{F}[T]/(T^2)$ and similarly $\beta(Tx + y) = a + Tb$, where $a, b, c, d$ are forms on $\mathfrak{sl}_4(\mathbf{F})$ evaluated at $x, y$. By inserting $Tx + y$ into (7), we thus obtain

$$[x, y, y^2] + dy^2 + c[x, y] + ax + by = 0,$$

as required. □

A similar phenomenon to Corollary 6.3 appears to hold in this case as well, although we have not been able to prove it. Generically, the Lie algebra generated by two elements in $\mathfrak{psl}_4(\mathbf{F})$ seems to be isomorphic to $\mathfrak{sl}_3(\mathbf{F})$.

## Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Data availability

No data was used for the research described in the article.

## References


[1] M. Aschbacher, R.M. Guralnick, Some applications of the first cohomology group, J. Algebra 90 (2) (1984) 446–460.

[2] Y. Bahturin, A. Olshanskii, The approximation and characteristic subalgebras of free Lie algebras, Tr. Semin. Im. I.G. Petrovskogo 2 (2) (1976) 145–150.

[3] J.M. Bois, Generators of simple Lie algebras in arbitrary characteristics, Math. Z. 262 (4) (2009) 715–741.

[4] A. Chistopolskaya, On nilpotent generators of the Lie algebra $\mathfrak{sl}_n$, Linear Algebra Appl. 559 (2018) 73–79.

[5] R. Elman, N. Karpenko, A. Merkurjev, The Algebraic and Geometric Theory of Quadratic Forms, Colloquium Publications, vol. 56, American Mathematical Society, Providence, RI, 2008.

[6] R. Guralnick, B. Kunyavskiĭ, E. Plotkin, A. Shalev, Thompson-like characterizations of the solvable radical, J. Algebra 300 (1) (2006) 363–375.

[7] R.L. Grahams, Neil J.A. Sloane, On additive bases and harmonious graphs, SIAM J. Algebraic Discrete Methods 1 (1980) 382–404.

[8] R.M. Guralnick, Some applications of subgroup structure to probabilistic generation and covers of curves, in: Algebraic Groups and Their Representations, 1998, pp. 301–320.

[9] K. Hensel, Uber die Darstellung der Zahlen eines Gattungsbereiches fur einen beliebigen Primdivisor, J. Reine Angew. Math. 103 (1988) 230–237.

[10] T. Ionescu, On the generators of semisimple Lie algebras, Linear Algebra Appl. 15 (3) (1976) 271–292.
[11] N. Jacobson, Lie Algebras, Dover Publications, New York, 1979.
[12] M. Kuranishi, On everywhere dense imbedding of free groups in Lie groups, Nagoya Math. J. 2 (1951) 63–71.
[13] D. Leites, P. Grozman, Defining relations associated with the principal $\mathfrak{sl}(2)$-subalgebras, Am. Math. Soc. Transl. 175 (1996) 57–67.
[14] B. Lidl, H. Niederreiter, Finite Fields, Addison-Wesley, Reading, 1983.
[15] P.M. Neumann, C.E. Praeger, Cyclic matrices over finite fields, J. Lond. Math. Soc. 52 (2) (1995) 263–284.
[16] B.V. Petrenko, S.N. Sidki, On pairs of matrices generating matrix rings and their presentations, J. Algebra 310 (1) (2007) 15–40.
[17] R. Steinberg, Generators for simple groups, Can. J. Math. 14 (1962) 277–283.
[18] J. von zur Gathen, M. Giesbrecht, Constructing normal bases in finite fields, J. Symb. Comput. 10 (1990) 547–570.