Subgroups of simple groups are as diverse as possible

Martin Kassabov\(^1\)  |  Brady A. Tyburski\(^2\)  |  James B. Wilson\(^3\)

\(^1\)Department of Mathematics, Cornell University, Ithaca, New York, USA
\(^2\)Program in Mathematics Education, Michigan State University, East Lansing, Michigan, USA
\(^3\)Department of Mathematics, Colorado State University, Fort Collins, Colorado, USA

Correspondence
James B. Wilson, Department of Mathematics, Colorado State University, Fort Collins, CO 80523, USA.
Email: James.Wilson@ColoState.Edu

Funding information
NSF, Grant/Award Numbers: DMS-1620454, DMS-1601406; Simons Foundation, Grant/Award Number: 636189; EPSRC, Grant/Award Number: EP/R014604/1

Abstract
For a finite group \(G\), let \(\sigma(G)\) be the number of subgroups of \(G\) and \(\sigma_t(G)\) the number of isomorphism types of subgroups of \(G\). Let \(L = L_r(p^e)\) denote a simple group of Lie type, rank \(r\), over a field of order \(p^e\) and characteristic \(p\). If \(r \neq 1, L \not\cong 2B_2(2^{1+2m})\), there are constants \(c, d\), dependent on the Lie type, such that as \(re\) grows
\[ p^{(c-o(1))r^4e^2} \leq \sigma(L_r(p^e)) \leq \sigma(L_r(p^e)) \leq p^{(d+o(1))r^4e^2}. \]

For type \(A\), \(c = d = 1/64\). For other classical groups \(1/64 \leq c \leq d \leq 1/4\). For exceptional and twisted groups, \(1/2^{100} \leq c \leq d \leq 1/4\). Furthermore,
\[ 2^{(1/36-o(1))k^2} \leq \sigma_t(\text{Alt}_k) \leq \sigma(\text{Alt}_k) \leq 24^{(1/6+o(1))k^2}. \]

For abelian and sporadic simple groups \(G, \sigma_t(G), \sigma(G) \in O(1)\). In general, these bounds are best possible among groups of the same orders. Thus, with the exception of finite simple groups with bounded ranks and field degrees, the subgroups of finite simple groups are as diverse as possible.

MSC (2020)
20E07, 20E32, 20F69 (primary)
1 | INTRODUCTION

Recent and historic attention has considered the subgroups of finite simple groups. In small cases, these subgroups can be classified, at least up to conjugacy, and for general finite simple groups the maximal subgroups have also been detailed (cf. [1, 5, 8, 13]). Other works consider intersections of maximal subgroups [3, 6, 10] which give the potential to explore all subgroups of finite simple groups. Here, we prove bounds on the total number of distinct isomorphism types of subgroups within finite simple groups. The bulk of the variety is witnessed already by the nilpotent subgroups of finite simple groups.

Notation. Throughout this work, $p$ is a prime and for a positive integer $n$, $\nu_p(n)$ is largest $\nu$ such that $p^\nu|n$ and $\mu(n) = \max\{\nu_p(n) : p|n\}$. For a finite group $G$, define $\sigma(G)$ as the number of subgroups of $G$ and $\sigma_\nu(G)$ as the number of isomorphism types of subgroups of $G$. We note that

$$\sigma_\nu(G) \leq \sigma(G) \leq n^{\mu(n)+1} \leq 2^{(\log n)^2}.$$

The upper bounds follow from the cumulative work of Gaschütz, Kovács, Guralnick and Lucchini that proves a (sub)group of order $k|n$ is generated by a set of size $\mu(k)+1 \leq \mu(n)+1$ [2, Theorem 16.6]. For functions $f$, $g : \mathbb{R} \to \mathbb{R}$, we write $g \in O(f)$, respectively, $g \in \Omega(f)$ if $\exists C, N > 0$ such that $x > N \Rightarrow |g(x)| \leq C|f(x)|$, respectively, $x > N \Rightarrow |g(x)| \geq C|f(x)|$. Also let $\Theta(f) = \Omega(f) \cap O(f)$. We also write $g \in h + O(f)$, respectively, $g \in pO(f)$ if $g - h \in O(f)$, respectively, $\log p \in O(f)$ and likewise with $\Omega$ and $\Theta$.

Theorem 1.1. Let $L = L_\nu(p^e)$ denote a simple group of Lie type, rank $r$, over a field of order $p^e$ and characteristic $p$. If $L \not\approx PSL_2(p^e)$ and $L \not\approx 2B_2(2^{1+2m})$, then there are constants $c, d$, dependent on the Lie type, such that

$$c \leq \liminf_{r\to\infty} \log_p \frac{\sigma(L_\nu(p^e))}{r^4e^2} \leq \limsup_{r\to\infty} \log_p \frac{\sigma(L_\nu(p^e))}{r^4e^2} \leq d.$$

For type $A$, $c = d = 1/64$. For other classical groups, $1/64 \leq c \leq d \leq 1/4$. For exceptional and twisted groups, $1/2^{100} \leq c \leq d \leq 1/4$. Furthermore,

$$\frac{1}{36} \leq \liminf_{k\to\infty} \frac{\log_2 \sigma(Alt_k)}{k^2} \leq \limsup_{k\to\infty} \frac{\log_2 \sigma(Alt_k)}{k^2} \leq \frac{\log_2 24}{6}.$$

For abelian and sporadic simple groups $G$, $\sigma_\nu(G), \sigma(G) \in O(1)$.

An alternative formulation of the bounds is offered in the abstract and neither estimate is as precise as the bounds proved herein. Also within our characterization is the requirement that at least one of $r$ or $e$ grow, which further excludes groups like $PSL_3(p)$ where only the prime $p$ will grow. In general, we have not considered the effects of varying primes, and for small rank and degrees our estimates are likely far from tight, especially for exceptional and twisted groups. Remarks 2.5 and 3.3 speak to the limits of our counting method. We note that $\sigma_\nu(PSL_2(p^e)) \in p^{\Theta(e)}$, whereas $\sigma(PSL_2(p^e)) \in p^{\Theta(e^2)}$. So, the omission of the groups $PSL_2(p^e)$ from Theorem 1.1 is required.
On the other hand, we expect that the Suzuki groups $^2B_2(2^{1+2m})$ can be included in the statement of Theorem 1.1. Indeed, we can prove that these groups have many subgroups provided that there exists a small dimensional subspace in the field $\mathbb{F}_{2^{1+2m}}$ which ‘generates’ the field under some operation — unlike other simple groups, in the Suzuki case the commutator map in the Sylow 2-group is not related to the field multiplication which prevents us from using standard techniques to prove the existence of such subspaces for general $e = 1 + 2m$. See Subsection 6.6. However, we were able to exhibit such a subspace for $e < 1000$. Hence, we believe that the class of Suzuki groups will eventually be included in a statement like that of Theorem 1.1.

As a consequence of our proof of Theorem 1.1, we also bound general classes $\mathcal{X}_n$, respectively, $\mathcal{X}_{\leq n}$, of groups of order $n$, respectively, at most order $n$. We extend $\sigma$ to $\sigma(\mathcal{X}_n) = \max\{\sigma(G) \mid G \in \mathcal{X}_n\}$ and $\sigma(\mathcal{X}_{\leq n})$. When $\mathcal{X}_n$ is all groups of order at most $n$, we write simply $\sigma(n)$. Do likewise with $\sigma_i$.

**Theorem 1.2.** For the class $\mathcal{N}_n$ of nilpotent groups of order $n$, 

$$\sigma_i(\mathcal{N}_n), \sigma(\mathcal{N}_n) \in \prod_{p|n} p^{\nu_p(n)^2/4+\Theta(\nu_p(n))}. $$

Indeed, there are at least $\prod_{p|n} p^{\nu_p(n)^3/108+\Theta(\nu_p(n)^2)}$ pairwise non-isomorphic groups $G$ of order $n$ having $\sigma(G) \in \prod_{p|n} p^{\nu_p(n)^2/36+\Omega(\nu_p(n))}$. As a consequence for the class of nilpotent groups of order at most $n$, we have

$$\sigma_i(\mathcal{N}_{\leq n}), \sigma(\mathcal{N}_{\leq n}) \in 2^{(\log_2 n)^2/4+\Theta(\log_2(n))}. $$

For convenience we confine all our calculations to the context of finite simple groups but our method extends to almost simple, quasi-simple, algebraic, and Steinberg groups. In the latter cases, one may replace cardinality with dimensions of varieties. If one assume the Classification of Finite Simple Groups [11], then Theorem 1.1 indeed concerns all simple groups, but we have no explicit dependence on that theorem within our proof.

### 1.1 Proof overview

Throughout, $K = \mathbb{F}_q$ is a finite field of characteristic $p$ and order $q = p^e$, and $k = \mathbb{F}_p$. Abbreviate $\otimes := \otimes_K$ and $\Hom(-,-) := \Hom_K(-,-)$. We identify biadditive maps $U \times V \to W$ with linear maps $U \otimes V \to W$. We let $\End(V)$ denote endomorphisms and $\Aut(V)$ automorphisms.

To count subgroups of a finite group $G$, the usual strategy is linear algebra. Select a large $p$-elementary abelian section $L_1 = \Gamma_1/\Gamma_2$ of $G$ where the counting reduces to counting subspaces of a vector space. If $\log_p |L_1| \in \Theta(\log_p |G|)$, then the number of subspaces matches the targeted quantity of $p^{\Theta(\nu(|G|)^2)}$. Such a count gives no clue about the possible range of isomorphism classes of subgroups and indeed if the only large $p$-elementary abelian sections have $\Gamma_2 = 1$ then this process surveys just $O(\log_p |G|)$ isomorphism types.

To obtain a larger number of isomorphism classes, we appeal to multi-linear algebra. First we select a series $\Gamma_1 > \Gamma_2 > \Gamma_3 > \cdots$ arranged into a filter in the sense that for all $i, j$, $[\Gamma_i, \Gamma_j] \leq \Gamma_{i+j} \leq \Gamma_i \cap \Gamma_j$. This allows for the creation of an associated graded Lie algebra. Each $L_i = \Gamma_i/\Gamma_{i+1}$ is
abelian, in fact $p$-elementary abelian in our cases. Set $L = \bigoplus_i L_i$ with brackets $[,]_{i,j} : L_i \otimes L_j \to L_{i+j}$ induced from commutation in the group $\Gamma_1$.

We focus specifically in filters where $d_i := \log_p |L_i|$ satisfies $d_1^2/4 \gg d_2^2 + d_3^2$, which guarantees a larger number of subgroups $Q \leq \Gamma_1$ containing $\Gamma_2$. We can restrict $[,]_{1,2}$ to $Q$ and obtain a linear map $Q/\Gamma_2 \otimes L_2 \to L_3$. By tensor-hom adjunction, such maps are captured as maps $Q/\Gamma_2 \to \text{Hom}(L_2, L_3)$. In this way, we may reduce the isomorphism types among the subgroups $Q$ to the $\text{Aut}(L_2) \times \text{Aut}(L_3)$-orbits on the subspaces of $\text{Hom}(L_2, L_3)$. Now the intuition of the count becomes clear. There are $p^{(d_1 - l)}$ subspaces of dimension $l = \text{rank } Q/\Gamma_2$. Meanwhile, $\text{Aut}(L_2) \times \text{Aut}(L_3)$ has only $d_2^2 + d_3^2$ parameters. For $\ell \approx d_1/2$, $\ell(d_1 - \ell) \gg d_2^2 + d_3^2$; thus, there are many orbits of subspaces in $L_1$ under the action of the automorphism group. Such a count is a variation on the method introduced by Higman to estimate the number of isomorphism types of finite $p$-groups [12].

The subtlety hidden here is that upon restricting to subgroups $Q \leq \Gamma_1$ containing $\Gamma_2$, there is no immediate requirement that such $Q$ will determine $\Gamma_i$, for $i > 1$, calling into question why isomorphisms between such $Q$ should restrict to isomorphisms of the maps $Q/\Gamma_2 \otimes L_2 \to L_3$. Indeed, this is not true in general.

We will focus on the cases where most subgroups $Q$ determine the subgroups $\Gamma_i$. For general bounds we look for examples where $[,]_{1,2} : R \otimes M \to M$, where $R$ is an algebra and $M$ is a left $R$-module. We consider subgroups $Q$ together with some additional data that can be used to reconstruct the subgroups $\Gamma_i$. The subgroups $Q$ with the necessary extra data we exploit undercounts the total number of isomorphism classes of subgroups, but it does provide easier counts in large ranks. To obtain counts that apply in small ranks, we instead recover appropriate rings that act on $[,]_{1,2}$ but are not part of the commutation themselves.

Upper bounds are established by a result of Wall [20] that shows that the number of $p^k$-order subgroups of a group of order $p^n$ is at most the number of $k$-dimensional subspaces of $\mathbb{F}_p$-vector spaces of dimension $n$. This combined with structure of maximal solvable groups of matrix groups affords a tight bound in type $A$ and a suitable bound for other groups.

### 2 MODULE NURSERIES AND KINDER

A filter $\Gamma_1 > \Gamma_2 > \Gamma_3 > \cdots$ of subgroups satisfies $[\Gamma_i, \Gamma_j] \leq \Gamma_{i+j} \leq \Gamma_i \cap \Gamma_j$. Thus, $L_i = \Gamma_i/\Gamma_{i+1}$ forms a graded Lie ring $L = \bigoplus_i L_i$. Call this filter a nursery if $L_1$ has more subspaces than the size of $\text{Aut}(L_2) \times \text{Aut}(L_3)$. By a module nursery, we mean there is an (unital) associative ring $R$, a faithful (left) $R$-module $M$, and isomorphisms $\alpha : L_1 \to R$; $\beta : L_2 \to M$ and $\gamma : L_3 \to M$ where

$$\gamma([u\Gamma_2, v\Gamma_3]\Gamma_4) = \alpha(u\Gamma_2)\beta(v\Gamma_3).$$

We call the nursery exact if $\Gamma_4 = [\Gamma_2, \Gamma_2]$, this condition is automatically satisfied if $\Gamma_4 = 1$. A primary example of nurseries are the generalized Heisenberg groups $\mathcal{H}_{abc}(K)$ defined as the block-upper triangular matrices inside $\text{GL}_d(K)$, $d = a + b + c$:

$$\mathcal{H} = \mathcal{H}_{abc}(K) = \left\{ \begin{bmatrix} I_a & U & W \\ 0 & I_b & V \\ 0 & 0 & I_c \end{bmatrix} \left| \begin{array}{l} U \in \mathbb{M}_{a \times b}(K) \\ V \in \mathbb{M}_{b \times c}(K) \\ W \in \mathbb{M}_{a \times c}(K) \end{array} \right. \right\}.$$ 

(2.2)
Suppose \( a \geq c \). Then these groups have a filter defined by

\[
\Gamma_1 = \mathcal{H} > \Gamma_2 = \left\{ \begin{bmatrix} I_a & 0 & W \\ 0 & I_b & V \\ 0 & 0 & I_c \end{bmatrix} \right\} > \Gamma_3 = \left\{ \begin{bmatrix} I_a & 0 & W \\ 0 & I_b & 0 \\ 0 & 0 & I_c \end{bmatrix} \right\} > \Gamma_{c \geq 4} = 1.
\]

If \( a = b \), then \( L_1 \cong \mathbb{M}_a(K), L_2 \cong L_3 \cong \mathbb{M}_a \times c(K) \) and \([,]_{1,2} : L_1 \otimes L_2 \rightarrow L_3\) is equivalent to the module action of \( R = \mathbb{M}_a(K) \) on the left of \( \mathbb{M}_a \times c(K) \). If \( a > 2c \), then the number of subspaces of \( L_1 \) is at least \( p^{a^2/4} \) while \( \text{Aut}(L_2) \times \text{Aut}(L_3) \) has order at most \( 2p^{a^2+c^2} \); so, these are exact module nurseries.

Already observed in [23, Section 3], for each \( \nu \geq 3 \), the groups \( \mathcal{H}_{\alpha \beta \gamma}(K) \) with \( a = b = \lceil \nu/3 \rceil, c = 1 \) contain \( p^{\nu^3/27 + O(\nu^2)} \) pairwise non-isomorphic subgroups of order \( p^\nu \). So, these groups have a diverse family of subgroups but we shall need many more subgroups to obtain meaningful lower bounds. The main result in this section is to generalize such counts by replacing generalized Heisenberg groups with the concept of exact module nurseries.

Throughout this and the next section, we concentrate on subgroups \( Q \) where \( \Gamma_2 \leq Q \leq \Gamma_1 \) for a nursery \( \Gamma^*_1 \). We call these subgroups kinder (or kind for one).

**Theorem 2.3.** Let \( \Gamma_1 > \Gamma_2 > \Gamma_3 > \cdots \) be an exact module nursery for a \( k \)-algebra \( R \) and \( R \)-module \( M \). Fix a generating set \( S \) containing 1 of \( R \) as a \( k \)-algebra, and a set \( T \subset M \) such that \( \bigcap_{x \in T} \text{Ann}_R(x) = 0 \).

Then the number of isomorphism types of kinder \( Q \) such that \( Q \subset \Gamma_2 \) and \( |Q/\Gamma_2| = p^{\ell} \) is at least

\[
p^{(\ell-s)(r-c)-\ell s-m t},
\]

where \( |R| = p^r, s = |S|, |M| = p^m, \) and \( t = |T| \).

**Proof.** Fix a kind \( Q \). Recall the meaning of \((\alpha, \beta, \gamma)\) from (2.1). Fix transversals \( V_i \leq \Gamma_i \) for \( \Gamma_i/\Gamma_{i+1} \). We consider the tuples \((Q, \rho, \mu)\), where \( Q \leq \Gamma_1 \), containing \( \Gamma_2, \rho : S \rightarrow V_1 \cap Q \) (\( \rho \) for ring) where \( \alpha(\rho(s)\Gamma_2) = s \) for all \( s \in S \) and \( \mu : T \rightarrow V_2 \) (\( \mu \) for module) such that \( \beta(\mu(t)\Gamma_3) = t \) for all \( t \in T \).

We claim that the data \((Q, \rho, \mu)\) are enough to reconstruct each \( \Gamma_i \).

Set \( X = \bigcap_{i \in T} \{ q \in Q \mid [q, \mu(t)] \leq \Gamma_4 \} \). As \( [\Gamma_2, \Gamma_2] \leq \Gamma_4 \), and because \( \mu(t) \in \Gamma_2 \), it follows that \( \Gamma_2 \leq X \). Suppose that \( q \in Y \), if \( q \notin \Gamma_2 \) then \( \alpha(q\Gamma_2) \neq 0 \) and there exists \( t \in T \) such that \( \alpha(\gamma(t)\Gamma_4) \neq 0 \), which is equivalent to \( \gamma([q, \mu(t)]\Gamma_4) \neq 0 \), but this contradicts the assumption that \( q \in X \). This shows that \( X = \Gamma_2 \).

Next, put \( Y = [\rho(1), X] \) and \( Z = [X, X] \). It follows from the definition of exact module nursery that \( Y = \Gamma_3 \) and \( Z = \Gamma_4 \).

It remains to reconstruct \( \Gamma_1 \), but \( \Gamma_1 \) is a super group so here we mean simply that data \((Q, \rho, \mu)\) identify how \( Q/\Gamma_2 \) sits in \( L_1 \). Therefore, the preimage of that embedding is fixed by the data provided. For that observe the usual additive mapping \( Q/\Gamma_2 \hookrightarrow \text{Hom}(L_2, L_3) \) is an embedding because the kernel \( X = \Gamma_2 \). So, we obtain an embedding \( \chi : Q/\Gamma_2 \rightarrow \text{End}(M) \), relative to \((\beta, \gamma)\). Finally, for \( s \in S \) and \( m \in M \), \( \chi(\rho(s))(\beta^{-1}(m)) = \gamma(\rho(s), \beta^{-1}(m)) = sm \). Since \( R = k(S) \), the \( k \)-algebra generated by the image of \( \chi \) contains the image of \( R \) in \( \text{End}(M) \), and because the image of \( \chi \) consists

\[\footnote{Equivalently consider mappings \([\rho] : S \rightarrow Q/\Gamma_2 \) and \([\mu] : T \rightarrow Q/\Gamma_3 \) and show the construction is unaffected by choice of coset representatives.}\]
of the $\gamma$-image of commutators, $\chi(Q)$ is contained in the image of $R$ in $\text{End}(M)$. Thus, $\chi$ leads to a unique embedding of $Q/\Gamma_2$ into $R \cong \Gamma_1/\Gamma_2$. Therefore, $(Q, \rho, \mu)$ determines the embedding of $Q$ into $\Gamma_1$.

To estimate the number of kinder, count the number of subspaces of $R$ which contain $\mathcal{S}$, which is at least $p^{(r-s)(r-\ell)}$ which is lower bound for the total number of $(Q, \rho, \mu)$ triples.

The choice for $\rho : S \to V_1 \cap Q$ is (at most) $p^{\ell s}$ and the choices for $\mu : T \to V_2$ are $p^{m t}$, therefore at most $p^{\ell s + m t}$ triples correspond to isomorphic groups $Q$. Thus, the number of isomorphism types of kinder is at least $p^{(r-s)(r-\ell)-\ell s - m t}$.

Let $U_d(F_q)$ denote the group of upper unitriangular $(d \times d)$-matrices.

**Corollary 2.4.** Fix $p$, for $d \geq 5$, the following holds:

$$p^{(1/64-\omega(1))d^4e^2} \leq \sigma_i(U_d(F_{p^e})) \leq \sigma(U_d(F_{p^e})) \leq p^{(1/64+\omega(1))d^4e^2}.$$  

For $d \in \{3, 4\}$, the following holds:

$$p^{(1/4-\omega(1))e^2} \leq \sigma_i(U_d(F_{p^e})).$$

Meanwhile, $\sigma(U_3(F_{p^e})) \leq p^{3e^2/4+O(e)}$ and $\sigma(U_4(F_{p^e})) \leq p^{3e^2/2+O(e)}$. For $d = 2$, $\sigma_i(U_2(F_{p^e})) = e + 1$ and $\sigma(U_2(F_{p^e})) \in p^{e^2/2+O(e)}$.

**Proof.** The group $U_d(K)$ contains $H_{abc}(K)$ where $a = b$ and $c = 1$ which has an exact module nursery with $R = M_a(K)$ and $M = K^a$. Fix a generator $\omega$ for $K/k$ so that $R = k\langle S \rangle$ where $S = \{I_a, \omega E_{11}, E_{12} + E_{23} + \cdots + E_{a-1,a} + E_{a,1}\}$. For $T$ choose a basis of $M$ over $K$. Subject to the constraint $d > 2a + 1$, by Theorem 2.3,

$$\sigma_i(U_d(K)) \geq \sigma_i(H_{aa1}(K)) \geq \max_{\ell} p^{(\ell-3)(a^2e-\ell)-3\ell-a^2e}.$$  

The maximum is achieved when $\ell = \lfloor a^2e/2 \rfloor$. Since $a = \lfloor (d-1)/2 \rfloor$, this yields a lower bound on $\sigma_i(U_d(F_{p^e}))$ of $p^{1/64(d-1)^4e^2-(d-1)^2e}$. As $|U_d(F_{p^e})| = p^v$ where $v = (d-1)e = d^2e/4 + O(de)$. By Wall’s theorem [20, (1.1)], $\sigma(U_d(F_{p^e})) \leq \sigma(F_{p^e}) \leq p^{v^2/4+O(v)}$. So, $\sigma(U_d(F_{p^e})) \leq p^{(1/64+\omega(1))d^4e^2}$. 

**Remark 2.5.** The bounds hidden in $\omega(1)$ can be resolved into the following (some which will be improved by our next estimate). With $p$ fixed, $\sigma_i(U_d(F_{p^e})) \geq p$ in the following cases: $d \in \{3, 4\}$ and $13 \leq e$; $d \in \{5, 6\}$ and $5 \leq e$; $d \in \{7, 8, 9, 10\}$ and $2 \leq e$; and $d \geq 11$ and $1 \leq e$.

## 3 | GENERAL NURSERIES

Having described the general bound we look here to improve the lower bounds by proving a stronger property about most subgroups of generalized Heisenberg groups $H := H_{abc}(K)$ and the filters $\Gamma_\ast$ we introduced in Section 2. Note that in this section, $(a, b, c)$ can be arbitrary and in general $\Gamma$ is an exact nursery but not typically a module nursery. Indeed, the associated Lie
algebra \( L = \bigoplus_i \Gamma_i / \Gamma_{i+1} \) recovers general matrix multiplication as the bracket \( [\cdot, \cdot]_{1,2} : L_1 \otimes L_2 \to L_3 \) instead:

\[
\mathcal{M}_{a \times b}(K) \otimes \mathcal{M}_{b \times c}(K) \to \mathcal{M}_{a \times c}(K).
\]

First a few remarks on the canonicity of the choice of \( \Gamma_i \): the subgroup \( \Gamma_3 \) is the commutator subgroup of \( \mathcal{H} \), and therefore is characteristic; identifying \( E := \Gamma_2 \) is more subtle. There is a competing choice of subgroup \( \Gamma_2 < F < \Gamma_1 \) where (in the notation of (2.2)) \( V = 0 \) and \( U \in \mathcal{M}_{a \times b}(K) \).

In fact, these coordinates are not in general group theoretic features so there could be many further choices.

The property we need is on pairs of subgroups. Witness that \( E \) and \( F \) are abelian normal subgroups such that \( \mathcal{H} = \langle E, F \rangle, \ E \cap F = \langle H, H \rangle \leq \mathcal{Z}(H) \). Such so-called hyperbolic pairs were first studied by Brahana [4] and developed further in [14, Section 6.1]. In [7, Lemma 3.5], a characterization of hyperbolic pairs showed they are in bijection with specific idempotents of a ring \( \mathcal{M} \) of adjoints. We say more about adjoints in (3.6) but suffice it for now to say that these arise as solution for \( (\phi, \tau) \) in the equation \( [\phi(u), v] = [u, \tau(v)] \) and the correspondence considers those \( (\phi, \tau) \) pairs for which \( E = \ker \phi \) and \( F = \text{Im} \phi \) afford a hyperbolic pair. The necessary properties on \( (\phi, \tau) \) become apparent by appealing to the associated graded algebra of the group where the condition becomes a familiar properties in the representation theory of associative modules. Note that [7] focuses on odd characteristic but the proofs of the necessary lemmas work in all characteristics, see, for example, [14, Proposition 6.4] for details on the case of characteristic 2. Combined with [22, Corollary 1.5], this implies that hyperbolic pairs in \( \mathcal{H}_{abc}(K) \) are in the same orbit under the action of the automorphism group. Thus, the assumption that \( a \geq c \) stipulates that we take the smaller of the two terms in any hyperbolic pair, or if \( a = c \) to pick any of the terms. In fact, when \( a, c > 1 \) there is exactly one hyperbolic pair for \( \mathcal{H}_{abc}(K) \), and if furthermore \( a > c \) then \( \Gamma_2 \) is the unique smallest subgroup in this hyperbolic pair. When \( a = c = 1 \) the automorphism group is unusually large and thus there are many hyperbolic pairs.

The main result in this section shows that for a generic kinder \( Q \) of \( \Gamma_* \), the same argument applies and the subgroups \( \Gamma_3 \) are characteristic in \( Q \) and functions \( \Gamma_2 \) are in a single \( \text{Aut}(Q) \)-orbit (Proposition 3.10). In addition, all isomorphisms between such subgroups come from automorphisms of \( \mathcal{H} \) fixing \( \Gamma_2 \). It is interesting to note that this result also holds when \( c = 1 \) and \( e > 7 \) even though in this case \( \Gamma_2 \) is far from being a characteristic subgroup of \( \mathcal{H} \).

We prove that under mild conditions for \( a, b, c \) — the size of the blocks, and \( e \) — the degree of the field extension over \( \mathbb{Z}_p \), isomorphisms between generic kinder extend to automorphisms of \( \Gamma_1 \). Our version of generic is measured as a probability but can also be generic in the sense of algebraic geometry.

**Theorem 3.1.** Fix the nursery \( \Gamma_* \) of \( \mathcal{H}_{abc}(\mathbb{F}_q) \) of Section 2. If \( a \leq b \) and \( \ell > 2 + b/a \), or \( b < a \) and \( \ell > 2 + a/b \), then among kinder \( Q \) of \( \Gamma_* \) with \( [Q : \Gamma_2] = p^\ell \),

\[
\Pr(\exists \alpha \in \text{Aut}(\Gamma_1), \alpha(Q) = \tilde{Q} \mid Q \cong \tilde{Q}) \geq 1 - O(1/p).
\]

That result leads to our counting claims, first one about \( \mathcal{H}_{abc}(K) \).

**Corollary 3.2.** For some constants \( C, D > 0 \)

\[
p^{(a b e)^2 / 4 - C a b e} \leq \sigma_1(\mathcal{H}_{abc}(\mathbb{F}_p^e)) \leq p^{(a b + b c + a c)^2 e^2 / 4 + D (a b + b c + a c) e}.
\]

Thus, for \( a, b \in d/2 + O(1) \), and \( c \in O(1) \), we find \( \sigma_1(\mathcal{H}_{abc}(\mathbb{F}_p^e)) \in p^{d^2 e^2 / 64 + \Theta(d^2 e^2)} \).
Proof. Without loss of generality, let \( a \geq c \). For the lower bound observe that \( \Gamma_1 / \Gamma_2 \cong \mathbb{M}_{axb}(K) \) as additive groups and the subgroups \( Q \) where \( \Gamma_2 < Q < \Gamma_1 \) are enumerated by \( \mathbb{F}_p \)-subspaces \( V \) of \( \mathbb{M}_{axb}(K) \), where \( |K| = p^e \) with \( |V| = p^f \). That yields \( p^{\ell(a+b-c)} \) choices of \( Q \). Assuming \( Q \) is generic, the set of generic subgroups isomorphic to \( Q \) are in the same orbit of the subgroup \( A := \text{Aut}(\mathcal{H}_{abc}(K)) \) which fix \( \Gamma_2 \). From the structure of \( A \) given in [22, Corollary 1.5], it follows that this action factors through 

\[
\text{Gal}(K) \ltimes (\text{GL}_a(K) \times \text{GL}_b(K) \times \text{GL}_c(K))/K^\times,
\]

if \( a > c \geq 1 \);

\[
2. \text{Gal}(K) \ltimes (\text{GL}_a(K) \times \text{GL}_b(K) \times \text{GL}_d(K))/K^\times,
\]

if \( a = c > 1 \);

\[
\text{Gal}(K) \ltimes \text{GSp}_{2b}(K),
\]

if \( a = c = 1 \).

Hence, each orbit has cardinality at most \( p^{O((a^2+b^2+c^2)e)} \). Maximizing over \( \ell' = (1 + o(1)) \frac{ab}{2} \), there are at least \( p^{(ab)^2/(4+O(ab))} \) distinct orbits.

The upper bound comes from Wall’s theorem [20].

\[\square\]

Remark 3.3. Improving the bounds from Remark 2.5 from Corollary 3.2 one obtains that \( p \leq \sigma_i(U_d(p^e)) \in p^{(1/64-o(1))d^4e^2} \) whenever \( d = 3 \) and \( e \geq 9 \), \( d = 4 \) and \( e \geq 5 \), \( d = 5 \) and \( e \geq 3 \), \( d = 6 \) and \( e \geq 2 \), and in general when \( d \geq 7 \). Furthermore, the secondary error term of Corollary 2.4 is improved from \(-Cd^3e^2\) to \(-Dd^2e\).

3.1 Some probabilistic estimates

Lemma 3.4. Let \( v_1, \ldots, v_s \) be independently random vectors of an \( n \)-dimensional vector space \( V \) over a finite field of order \( q \).

\[
\Pr(V = \langle v_1, \ldots, v_s \rangle) \geq 1 - \frac{q^{n-s} - q^{-s}}{q-1} \geq 1 - q^{n-s}.
\]

Proof. There are \( (q^n - 1)/(q - 1) \) maximal subspaces, and the probability that a random vector is in a given maximal subspace is \( q^{-1} \). So, the probability that all \( \{v_i\} \) are in a fixed maximal subspace is \( q^{-s} \). Multiplying this by the number of maximal subspaces gives an upper bound of the probability that the span of \( \{v_i\} \) is a proper subspace.

\[\square\]

Remark 3.5. When the field \( K \) is infinite say instead that the variety of \( s \) tuples of vectors in \( K^n \) which do not span the whole space has codimension \( x - n + 1 \).

For \((s \times b)\)-matrices \( \Phi_1, \ldots, \Phi_c \) and \((a \times t)\)-matrices \( Y_1, \ldots, Y_c \) over \( K \), we have a \( K \)-vector space

\[
\text{Hom}(\Phi_*, Y_*) = \{(A, B) \in \mathbb{M}_{axs}(K) \times \mathbb{M}_{bxt}(K) \mid (\forall i)(A\Phi_i = Y_iB^i)\}.
\]
As the notation suggests, these are morphisms in an abelian category (though not in general, a module category [21]) and so \( \text{End}(\Phi_e) = \text{Hom}(\Phi_e, \Phi_e) \) is a ring. This is in fact the ring \( \mathcal{M} \) alluded to in the introduction of this section. We now quantify the generic expectation of these morphisms sets.

**Theorem 3.7.** Let \( m \leq n \) and \( \Phi_1, \ldots, \Phi_s \) be independently random \((m \times n)\)-matrices over a finite field \( K \) of order \( q \). If \( 2 + n/m \leq s \), then

\[
\Pr(\text{End}(\Phi_e) \cong K) \geq 1 - O(1/q)
\]

\((m < n \text{ or } 2 < m = n) \quad \Pr(\text{Hom}(\Phi_e, \pm \Phi^t_e) = 0) \geq 1 - O(1/q).

**Proof.** The condition that \( \dim_K \text{Hom}(\Phi_e, \Gamma_e) > c \) is an algebraic condition in the entries of \((\Phi_e, \Gamma_e)\). If this condition defines a proper subvariety of codimension \( g \), then the number of points is less than \( Cq^{mn-g} \), which implies the resulting bound.

Since \( K \subset \text{End}(\Phi_e) \), to show that this is a proper subvariety it suffices to construct an example of \( \Phi_e \) with \( \text{End}(\Phi_e) \cong K \), that is, a generic point off the variety. Without loss of generality, we can assume that \( m \leq n \) (otherwise we can take transpose).

Let \( m = n \), then we can view \( \mathcal{M}_m(K) \) as generated as a \( K \)-algebra by \( 1, \alpha, \sigma \) where \( E := K\langle 1, \alpha \rangle \) is a field extension of degree \( m \) (this step assumes \( K \) is a finite field) and \( E^\sigma = E \) induces a field automorphism of \( E \) that generates the Galois group of \( E/K \). For \( \Phi_e \) we can take \( \Phi_1 = I_m, \Phi_2 = \alpha \) and \( \Phi_3 = \sigma \). Then \( \text{End}(\Phi_e) \) is the centralizer of the algebra generated by \( \Phi_e \) therefore we have \( \text{End}(\Phi_e) \cong K \). If \( m > 2 \) then \( \sigma(\alpha) \neq \sigma^{-1}(\alpha) \), which implies that \( \text{Hom}(\Phi_e, \pm \Phi^t_e) = 0 \).

Now suppose \( m < n \) and define

\[
\Phi_0 = [I_m \ 0] \in \mathcal{M}_{m \times n}(K),
\]

\[
\Phi_i = \begin{bmatrix} 0_{m \times (1+m(i-1))} & I_m & 0 \end{bmatrix} \in \mathcal{M}_{m \times n}(K) \quad \text{for } 1 \leq i \leq (n-1)/m, \text{ and}
\]

\[
\Phi_\infty = \begin{bmatrix} 0_{m \times (n-m)} & I_m \end{bmatrix} \in \mathcal{M}_{m \times n}(K).
\]

Note that \( \bigcap_i \ker \Phi_i = 0 \) which implies that for a given matrix \( A \) there is at most one matrix \( B \) such that for all \( i \), \( A\Phi_i = \Phi_i B^i \). Define the subspaces \( U_j, U'_j, W_j \leq K^m \) inductively by

\[
U_1 = \Phi_2(ker \Phi_1)
\]

\[
U'_{j+1} = \Phi_2(\Phi^{-1}_1(U_j))
\]

\[
U_{j+1} = \Phi_2(\Phi^{-1}_1(U'_j))
\]

\[
W_j = U_j \cap U_{m+1-j}.
\]

Then \( \dim U_j = \dim U'_j = j \) and \( \dim W_j = 1 \) for \( 1 \leq j \leq m \) and \( \Phi_1 \Phi_2^{-1} \) induces an isomorphism \( \gamma_j : W_j \to W_{j+1} \). The condition \( (vi)(A\Phi_i = \Phi_i B^i) \) implies that \( AU_j \leq U_j \) and \( AU'_j \leq U'_j \). Therefore, \( A \) sends the 1-dimensional spaces \( W_j \) to themselves and it is compatible with the isomorphism \( \gamma_i \). Since \( K^m = \bigoplus W_j \) this implies that \( A \) is a scalar matrix, and so is \( B \). This shows that \( \text{End}(\Phi_e) \cong K \).

To see that \((A, B) \in \text{Hom}(\Phi_e, \pm \Phi^t_e) = 0 \), \( A\Phi_i = \pm \Phi^t_i B^i \) implies that the first rows \( A_i \) of \( A \) are 0 wherever \( \Phi_i^t \) has a 0 row, and wherever \( \Phi_i^t \neq 0 \), \( A_{1+m(i-1)+k} B_k \), and column \( B^i \) of \( B \) is 0 whenever \( \Phi_i \) has 0 columns. Running over \( i, j, A = 0 \) and \( B = 0. \)
For \( m = n \), the bound of \( s \geq 3 \) is best possible and for \( m = 1, s = n + 1 \) is best possible. Similar to results appear as far back as Kronecker, one needs a more nuanced tool than linear algebra to prove the result generically. See, for example, [10].† These enable the following computation related to the commutator of generic kinder of \( \mathcal{H}_{abc}(K) \).

**Corollary 3.8.** Fix \( a \leq b \) and \( f \geq 2 + b/a \), or \( b \leq a \) and \( f \geq 2 + a/b \). Given random \( \Phi_1, \ldots, \Phi_f \in \mathcal{M}_{a \times b}(K) \) define
\[
(\forall \nu) \Lambda_{\nu} = \begin{bmatrix} 0 & \Phi_\nu \\ -\Phi_\nu' & 0 \end{bmatrix}.
\]

Then if \( a = b \) with high probability \( \text{End}(\Lambda_{\nu}) \cong \mathcal{M}_{2}(K) \) and if in \( a \neq b \) then with high probability \( \text{End}(\Lambda_{\nu}) \cong (K \oplus K) \rtimes J \) where \( J \) is the Jacobson radical.

**Proof.** Without loss of generality, let \( a \leq b \). The equations defining \( \text{End}(\Lambda_{\nu}) \) say
\[
\begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \begin{bmatrix} 0 & \Phi_\nu \\ -\Phi_\nu' & 0 \end{bmatrix} = \begin{bmatrix} 0 & \Phi_\nu' \\ -\Phi_\nu & 0 \end{bmatrix} \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix}^t.
\]

Expanding these equations, we get the four defining properties
\[
\begin{align*}
(A_{12}, B_{12}) &\in \text{Hom}(\Phi_\nu^t, \Phi_\nu) & (A_{11}, B_{22}) &\in \text{End}(\Phi_\nu) \\
(A_{22}, B_{11}) &\in \text{End}(\Phi_\nu^t, \Phi_\nu^t) & (A_{21}, B_{21}) &\in \text{Hom}(\Phi_\nu, -\Phi_\nu^t).
\end{align*}
\]

Theorem 3.7 implies that with high probability, \( \text{End}(\Phi_\nu) \cong \text{Hom}(\Phi_\nu, -\Phi_\nu^t) \cong \text{Hom}(\Phi_\nu^t, \Phi_\nu) \cong K \) if \( a = b \), and if \( a \neq b \) then \( \text{End}(\Phi_\nu) \cong K \cong \text{End}(\Phi_\nu^t) \) and \( \text{Hom}(\Phi_\nu, -\Phi_\nu^t) = 0 \). The result follows.  

---

### 3.2 | Lifting isomorphisms: Proof of Theorem 3.1

Now we setup the mechanics to prove Theorem 3.1. Our process is in two steps. First we show that generically \( \Gamma_3 \) is a characteristic subgroup of \( Q \). Second we show the \( \Gamma_2 \) come from a unique orbit under the automorphism group of \( \text{Aut}(Q) \) and that the embedding from \( Q/\Gamma_2 \) into \( \mathcal{M}_{a \times c}(K) \) is unique up to the action by \( \text{GL}(K^a) \times \text{GL}(K^c) \).

**Proposition 3.9.** Let \( Q \) range over kinder of \( \mathcal{H}_{abc}(K) \), with respect to the nursery \( \Gamma_{\nu} \), and such that \( |Q/\Gamma_2| = p^\ell \) with \( \ell > b/a \). Then with high probability \( [Q, Q] = \Gamma_3 \).

**Proof.** The condition \( [Q, \Gamma_2] = \Gamma_3 \) is equivalent to saying: the \( K \) span of the elements in \( Q/\Gamma_2 \), viewed as elements in \( \mathcal{M}_{a \times b}(K) \), generate \( K^b \). The columns of the generators of \( Q/\Gamma_2 \) are random vector in \( K^b \); thus, it suffices that the total number of columns is at least \( b \). This happens when \( \ell > b/a \). Following Lemma 3.4, this happen with probability at least \( 1 - q^{b-a\ell} \).

As \( [Q, \Gamma_2] \leq [Q, Q] \leq [\Gamma_1, \Gamma_1] = \Gamma_3 \), and with high probability \( [Q, \Gamma_2] = \Gamma_3 \), it follows that with high probability \( [Q, Q] = \Gamma_3 \).  

†The result above may be classically known though we did not find a version to cite.
**Proposition 3.10.** Let $|K/k| = e$ and $abe > 1$. Let $Q$ range over kinder of the above nursery $\Gamma_{abc}(K)$ and $\iota : Q \hookrightarrow \mathcal{H}_{abc}(K)$ an arbitrary embedding. If $ae > 2$ and $\epsilon \approx ab/2$, with high probability there is an $\alpha \in \text{Aut}(Q)$ such that $\iota(\alpha(\Gamma_2)) = \Gamma_2$.

**Proof.** By Proposition 3.9, we know that $\Gamma_3$ is the commutator subgroup of $\Gamma$, which allows us to restrict $[,]_H$ to a biadditive map $[,]_Q : (Q/\Gamma_3)^{\otimes 2} \to \Gamma_3$. Note that $\Gamma_2$ is part of a hyperbolic pair $(E,F := \Gamma_2)$ for $Q$. So as described above, such decompositions are in bijective correspondence with so-called hyperbolic idempotents $(e, 1-e) \in \text{End}(\Lambda_*(Q))$ where $\Lambda_*(Q)$ is the coordinate representation of the $k$-bilinear map $[,]_Q$; see [7, Lemma 3.5]. Following Corollary 3.8, $	ext{End}(\Lambda_*(Q))/J \cong k \oplus k$ where $J$ is the Jacobson radical, or else $\text{End}(\Lambda_*(Q)) \cong \mathbb{M}_2(K)$. In the first case, $\text{End}(\Lambda_*(Q))/J$ has precisely two proper nontrivial idempotents $(e, 1-e)$ and $(1-e,e)$. By the lifting of idempotents, all proper nontrivial idempotents of $\text{End}(\Lambda_*(Q))$ are part of a hyperbolic pair. Furthermore, all hyperbolic pairs are conjugate by some $1+z, (z,-z) \in J$. Hence, $1+z$ lifts to an automorphism of $Q$, which can be checked directly or compared with the argument in [7, Theorem 3.15b]. In the second case, there are many proper nontrivial primitive idempotents but all are conjugate and one of them has the form $(e, 1-e)$, so they all do. \[\square\]

Once we know that $\Gamma_2$ and $\Gamma_3$ are isomorphism invariants for $Q$, we can consider the biadditive maps $[,] = [,]_Q : Q/\Gamma_2 \otimes \Gamma_2/\Gamma_3 \to \Gamma_3$ and look at the algebra of operators which act trivially on the $Q/\Gamma_2$ factor

$$R_Q = \left\{ (g,h) \in \text{End}(\Gamma_2/\Gamma_3) \times \text{End}(\Gamma_3) \mid \forall q \in Q/\Gamma_2, v \in \Gamma_2/\Gamma_3, [q,gv] = h[q,v] \right\}.$$ 

Note that this definition is a permuted variant of $\text{End}(\Phi_*)$ called the right nucleus; see [22, Section 1.1]. Since $\Gamma_2/\Gamma_3$ and $\Gamma_3$ can be identified with spaces of matrices and $Q/\Gamma_2$ can be embedded in a space of matrices, the algebra $R_Q$ contains a copy of $\mathbb{M}_e(K)$ acting naturally on $\Gamma_2/\Gamma_3$ and $\Gamma_3$. As $\mathbb{M}_e(K)$ is Morita equivalent to $K$ we can condense the system $\Phi_*$ of $(\ell \times bc)$-matrices to a random system $\Phi_* E_{11}$ (here $E_{11} \in \mathbb{M}_e(K)$ is the matrix with 1 in position 11 and 0 elsewhere). The result is a random system of $(\ell \times b)$-matrices where we may apply the counts of Theorem 3.7 to conclude that generically $R_Q = K \otimes \mathbb{M}_e(K)$.

**Proposition 3.11.** For generic $Q$, the algebra $R_Q \cong \mathbb{M}_e(K)$, if $\ell > 2 + b/a$.

**Proof of Theorem 3.1.** Let $Q$ and $\tilde{Q}$ be two kinder of $\mathcal{H}_{abc}$ and $\phi : Q \to \tilde{Q}$ an isomorphism. By Proposition 3.10, we may assume $\phi(\Gamma_2) = \Gamma_2$ and $\Gamma_3 = [Q,Q] = [\tilde{Q},\tilde{Q}]$.

By the definition of $R_Q$ and Proposition 3.11, the biadditive map $[,]_Q$ induces a linear map

$$t_Q : Q/\Gamma_2 \to \text{Hom}_{R_Q}(\Gamma_2/\Gamma_3, \Gamma_3) \cong \text{Hom}_{\mathbb{M}_e(K)}(\mathbb{M}_{b\times c}(K), \mathbb{M}_{a\times c}(K)) \cong \mathbb{M}_{b\times a}(K).$$

The same applies to $\tilde{Q}$.

In light of these identifications, $\phi$ induces an isomorphism $\text{Hom}_{R_Q}(\Gamma_2/\Gamma_3, \Gamma_3) \cong \text{Hom}_{R_{\tilde{Q}}}(\Gamma_2/\Gamma_3, \Gamma_3)$. Since both of these spaces can be identified with $\mathbb{M}_{a\times b}(K)$, then $\phi$ induces a $k$-linear automorphism of $\mathbb{M}_{a\times b}(K)$ which can be extended to an automorphism of $\mathcal{H}_{abc}$. \[\square\]

**Remark 3.12.** We can summarize the above steps in a generalized manner by considering a coordinate-free interpretation. First, the $(a \times b)$-matrices $(\Phi_1, \ldots, \Phi_e)$ are replaced
with multilinear maps, or tensors, \( t = \sum_{i,j,k} [\Phi_k]_{ij} \otimes e_i \otimes e_j \otimes e_k \) in \( K^a \otimes K^b \otimes K^c \). The rings \( \mathcal{M} \) and \( \mathcal{R} \) are universal in that they are the largest faithful ring representations such that \( t \in K^a \otimes \mathcal{M} K^b \otimes \mathcal{R} K^c \). For example, the \((a, b, c)\)-matrix multiplication tensor \( t \) resides naturally in \( \mathcal{M}_{a} \otimes \mathcal{M}_{b} \otimes \mathcal{M}_{c} \) and for generic \( \hat{Q} \leq \mathcal{M}_{a} \otimes \mathcal{M}_{b} \otimes \mathcal{M}_{c} \), the restriction \( t|_Q \) only resides in \( \hat{Q} \otimes K \mathcal{M}_{b} \otimes \mathcal{M}_{c} \otimes \mathcal{M}_{c} \otimes \mathcal{M}_{c} \). Theorem 3.7 considers the ring \( K \), and Proposition 3.11 recovers \( R = \mathcal{M}_{c} \). Corollary 3.8 is necessary since, instead of \( t|_Q \), we first recover from commutation an element of \( \wedge^2 \mathcal{M}(\hat{Q} \oplus \mathcal{M}_{b} \otimes \mathcal{M}_{c} \otimes \mathcal{M}_{c} \otimes \mathcal{M}_{c}) \) and from that the structure of the ring \( \mathcal{M} \) permits us to reconstruct a generic tensor of \( \hat{Q} \otimes K \mathcal{M}_{b} \otimes \mathcal{M}_{c} \otimes \mathcal{M}_{c} \).

In general, operators in \( \text{End}(K^a) \otimes \text{End}(K^b) \otimes \text{End}(K^c) \) acting on \( K^a \otimes K^b \otimes K^c \) are called transverse tensor operators. The above argument can be restated for a larger class of modules, for example, any modules for which the rings above are Azumaya algebras, using this generalized point of view.

### 3.3 Proof of Theorem 1.2

We now consider how large numbers of nilpotent groups \( G \) obtain the theoretical upper bound on the size of \( \sigma(G) \) and \( \sigma(G) \).

By Corollary 3.2 with \( a \leq b + O(1) \) and \( c > 1 \) constant, there are groups \( S_p \) in \( H_{abc} \) of order \( p^{ab+bc+ac} = p^{b^3+O(b)} \) having \( \sigma(S_p) \in p^{b^4/4+\Theta(b^2)} \). For the upper bound, apply Wall [20] to show that \( \sigma(p^c) \in p^{2c/4+O(c)} \).

For a larger family consider the subgroups \( \Gamma_2 < K \leq H_{abc}(\mathbb{F}_p) \) with \( c > 1 \) constant and \( a = b = \lfloor \nu/3c \rfloor \). Let \( \log_p |K| = \nu = \ell + 2bc \). There are \( p^{\ell(b^2-\ell-2bc)} = p^{b^2/27c^2+\Omega(\nu^2)} \) isomorphism classes of such subgroups. Furthermore, each subgroup has \( p^{c^2/4+\Theta(c)} \subset p^{c^2/36+\Theta(c)} \) pairwise non-isomorphic subgroups containing \( \Gamma_2 \).

To pass to nilpotent groups \( G \), fix the direct decomposition \( G = \prod_{p | n} S_p(G) \) into Sylow \( p \)-subgroups \( S_p \). Then every subgroup \( H \) of order \( k \) has \( H = \prod_{p | k} S_p(H) \) and \( S_p(H) \leq S_p(G) \). So, the claims hold.

### 4 CLASSICAL GROUPS

**Theorem 4.1.** Fix a prime \( p \). For \( G = A_{d-1}(p^e) = \text{PSL}_d(\mathbb{F}_p) \)

\[
p^{(1/64-o(1))d^4e^2} \leq \sigma_1(G) \leq \sigma(G) \leq p^{(1/64+o(1))d^4e^2}.
\]

If \( G \) is one of \( 2A_{2m-1}(p^e) = \text{PSU}_{2m}(\mathbb{F}_p^e), C_m(p^e) = \text{PSp}_{2m}(\mathbb{F}_p^e), \) or \( D_m(p^e) = \text{PO}^+_{2m}(\mathbb{F}_p^e) \)

\( (5 \leq m) \)

\[
p^{(1/64-o(1))m^4e^2} \leq \sigma_1(G) \leq \sigma(G) \leq p^{(1/4-o(1))m^4e^2}.
\]

\( (3 \leq m \leq 4) \)

\[
p^{(1/4-o(1))e^2} \leq \sigma_1(G) \leq \sigma(G) \leq p^{(1/4-o(1))m^4e^2}.
\]

If \( G \) is one of \( 2A_{2m}(p^e) = \text{PSU}_{2m+1}(\mathbb{F}_p^e), B_m(p^e) = \text{PSO}_{2m+1}(\mathbb{F}_p^e), 2D_m(p^e) = \text{PO}^-_{2m}(\mathbb{F}_p^e) \)

\( (6 \leq m) \)

\[
p^{(1/64-o(1))m^4e^2} \leq \sigma_1(G) \leq \sigma(G) \leq p^{(1/4-o(1))m^4e^2}.
\]
(4 ≤ m ≤ 5) \[ p^{(1/4−o(1))e^2} \leq \sigma_r(G) \leq \sigma(G) \leq p^{(1/4−o(1))m^4e^2}. \]

Our upper bounds follow the technique of Pyber in [16, Section 3] and are applied only in the case of type A. We expect that tight bounds for other classical groups require both an improved lower bound by inspecting their Sylow p-subgroups in place of \( U_d(K) \), as well as improving the upper bound by inspecting the solvable subgroups of general classical groups.

**Lemma 4.2.** For fixed \( p \), \( \sigma(GL_d(p^e)) \leq 2O(d^2)p^{d^2e}p^{O(d^3e\log d)} \sigma(U_d(K)). \)

**Proof.** By the work of Aschbacher–Guralnick [2, Theorem 16.4], every group \( H \) is generated by a solvable subgroup \( S \) and one more element \( g \in S \). So, first we enumerate the number of solvable subgroups of \( GL_d(p^e) \) by first selecting a conjugacy class of a maximal solvable subgroup \( M \). Pálfy shows there are at most \( A = 2O(d^2) \) such classes [2, Theorem 14.1] and each conjugacy class has order at most \( B = |GL_d(p^e)| \leq p(1−o(1))d^2e \). Let \( U \) be the \( p \)-core of \( M \). We claim \( |M/U| \leq p^{2d\log d} \). Consequently, \( M = \langle U, g_1, \ldots, g_{[2d\log d\log p]} \rangle \). The maximum size of a solvable group is \( C = p^{(1/2−o(1))d^2e} \) attained by the minimal Borel subgroups.

Altogether, each solvable subgroup \( S \) resides in one of the \( A \) many conjugacy classes of maximal solvable group \( M \), so that \( M \) is one of at most \( B \) conjugates one of which contains \( S \) and \( U \leq U_d(K) \). There are \( \sigma(U_d(K)) \) choices of \( U \) and \( C^{2d\log d\log p} \) choices of \( g_i \). So, the number of choices of \( S \) is

\[ ABC^{2d\log d\log p} \sigma(U_d(K)). \]

To see the bound on \( |M/U| \), we proceed by Suprenenko’s structure theory of solvable matrix groups (compare [2, pp. 127–128]). Let \( V_1 > \cdots > V_{c+1} = 0 \) be a composition series for \( V = K^d \) as an \( M \)-module. Then \( \overline{V} := \bigoplus_i V_i/V_{i+1} \) is a semisimple \( M \)-module \( \overline{M} = M/\ker_{M} \overline{V} \) has trivial unipotent normal subgroups, that is, \( \ker_{M} \overline{V} \) is the \( p \)-core \( U \). Now \( \overline{M} \) embeds into \( T \rtimes \Sigma \) where \( T \leq \prod_{i=1}^c E_i \rtimes \text{Gal}(E_i/k) \) with \( E_i/K \) field extensions with \( \sum_{i=1}^c |E_i : K| = d \), and \( \Sigma \leq \text{Sym}_c \). So \( |\overline{M}| \leq p^{d\log c_1} \Sigma^{c_1} \). So, the claim holds.

**Proof of Theorem 4.1.** For type \( A_{d-1}(p^e) \), use the natural embedding of \( U_d(K) \subset PSL_d(K) \) and Corollaries 2.4 and 3.2. For the remaining classical groups, use Witt’s extension lemma to embed \( U_m(K) \) into \( \text{Isom}(\phi) \) where \( \phi \) is a sesquilinear or quadratic form on \( K^d \) where \( 2m \leq d \leq 2m + 2 \) and \( m \) is the Witt index of \( \phi \) over the finite field \( K \). From this observe that this embedding has determinant 1 and factors through \( G = PS \text{Isom}(\phi) \). In all but the orthogonal groups, specifically \( \text{PSO}_d(K) \), this leads to a finite simple group of classical type. In the orthogonal groups we further take commutator subgroup of \( G \). When \( d \geq 12 \) and \( m \geq 5 \), by Corollary 2.4, \( \sigma_r(G) \geq p^{(1/1024−o(1))d^2e^2} \). The remaining bounds concern \( m \in \{3,4\} \), adjusted in the case of \( \Omega^- \).

For the upper bounds, we apply Lemma 4.2. 

**Remark 4.3.** It is difficult to estimate the value of \( \mu(n) \) when \( n = |PSL_d(p^e)| \) because of the accumulation of small prime divisors of \( n \) coming from factors \( (p^{ke} - 1) \), \( 1 \leq k \leq d \), in the order of \( GL_d(p^e) \) that remain as factors of \( |PSL_d(p^e)| \). These can lead to primes \( r \) where \( \nu_r(n) > \nu_p(n) = \binom{d-1}{2} \) (cf. Remark 6.1). However, for many \( d \) and \( p \), \( \mu(n) = \nu_p(n) \) and in those cases the bound \( \sigma(n) \leq n^{(d+1)n+1} \) implies that our above bounds have \( \sigma(PSL_d(p^e)) \) attaining the asymptotic bound \( \sigma(G) \) as \( G \) ranges over all groups of order \( n = |PSL_d(p^e)| \) for such \( n \). Jeff Achter has suggested to us that this happens for infinitely many \( d \), perhaps even for dense set of dimensions \( d \).
5 | ALTERNATING GROUPS

Next we estimate the isomorphism types of subgroups of the alternating groups. Pyber [16, Corollary 2.3] has shown that alternating groups \( \text{Alt}_k \) of order \( n = k!/2 \) have

\[
2^{k^2/16+\Omega(k)} \leq \sigma(\text{Alt}_k) \leq 24(1/6+o(1))k^2.
\]

By a formula of Legendre, if \( p \) is prime and \( p^e | k! \) then \( e = \sum_{i>0} \lfloor n/p^i \rfloor \) and so \( e < \frac{k}{p-1} \). Therefore, \( \mu(k!) < k \) and so

\[
\sigma(k!/2) \in 2^{\Theta(k^2)}.
\]

Therefore, on an asymptotic log scale, alternating groups attain the maximum possible \( \sigma \). We now prove the same for \( \sigma_1 \).

**Theorem 5.1.** The group \( \text{Alt}_k \) has at least \( 2^{k^2/36+\Omega(n \log n)} \) isomorphism types of subgroups. In particular, for alternating and symmetric groups \( G \) of order \( n \), \( \log_2 \sigma_1(G) \in \Theta(\log_2 \sigma(n)) \).

**Proof.** Similar to the count above for classical groups, we proceed by counting subgroups within a fixed group. An obvious choice might be to consider Sylow 2-subgroups, however, we obtain a suitable lower bound by instead counting with the groups \( \Gamma := \Gamma_k \) of a direct sum of \( k \) copies of the symmetric group on 3 letters. This acts on \( 3k \) points as a union of \( k \) orbits. So, \( \Gamma_k \) embeds in the symmetric group \( \text{Sym}_{3k} \) and in turn into \( \text{Alt}_{3k+2} \).† We will show that for large \( k \),

\[
\sigma_1(\Gamma_k) \in 2^{k^2/4+\Omega(k \log k)}.
\]

Let us consider the subgroups \( H \) containing the subgroup \( \Gamma_2 := [\Gamma, \Gamma] = C^k_3 \). Note that the subgroup \( \Gamma_2 \) is characteristic in \( H \) and the quotient \( \Gamma / \Gamma_2 \) is naturally identified with \( F^k_2 \) and comes with Hamming distance \( \varpi : \Gamma / \Gamma_2 \rightarrow [0, ..., k] \) counting the number of components where the corresponding coordinate is nonzero.

Now we cannot use this function directly since its definition depends on the embedding of \( H \) into \( \Gamma \). Instead, observe that the elements of \( H / \Gamma_2 \) come with their action of \( \Gamma_2 \) and for each \( h \in H \) we have

\[
|\langle [h, g] \mid g \in \Gamma_2 \rangle| = 3^{\varpi(h)}
\]

This shows that the restriction of the Hamming distance to \( H / \Gamma_2 \) can be determined only by the isomorphism type of the group \( H \).

Finally, up to code equivalence (see [15]), the number of binary codes of degree \( k \) and dimension \( e \) is at least \( 2^{e(d−e)/k!} \). This is maximized at \( e = k/2 \) where we get \( 2^{k^2/4+\Omega(k \log k)} \).

**Remark 5.2.** Another way to rephrase this argument is that we view \( F^k_2 \) as the maximal slit torus in \( \text{GL}_k(F_3) \), the subgroup \( H \) corresponds to a subgroup of the torus (together its action on \( F^k_3 \)). If this subgroup is sufficiently large then it has no repeated eigenvalues and it can be diagonalized in

† We can pass to a subgroup of index 2 in \( \Gamma_1 \) which embeds in \( \text{Alt}_{3k} \).
only one way (up to a permutation matrix) which gives a subspace of $F^k_2$ modulo the action of $S_k$. Since the number of subspaces is of the order of $2^{O(k^2)}$, which is significantly larger than $|S_k|$, this leads to a lower bound for the number of isomorphism types of subgroup which is of the order of $2^{O(k^2)}$.

Remark 5.3. The is a variant of this construction using 2-groups — instead of working with $S_3$ one can use $D_8 \subset S_4$. In this case the analog $\Gamma_2$, the group $C_4^k$ has slightly more complicated definition (since it is not a Sylow subgroup) †. This leads to at least $2^{n^2/64+\Omega(n \log n)}$ isomorphism types of 2-subgroups inside $\text{Alt}_n$. This can be generalized further to $p$-groups for odd primes $p$ using $C_p \triangleleft C_p \subset S_{p^2}$, in this case the analog of $\Gamma_2$ is defined as the unique elementary abelian subgroup of $H$ of size $p^{k_p}$.

6 | SMALL RANK AND EXCEPTIONAL GROUPS

We now consider the finite simple groups not covered in Theorems 4.1 and 5.1.

6.1 | Small rank counts

We turn now to the language of Steinberg groups. Indeed, the method for Steinberg groups can be used for classical groups as well albeit with less sharp bounds. We recall terminology from Steinberg (see [11]).

We consider the subgroup $U_\Delta(R)$ of the Steinberg group generated by the root subgroups corresponding to the positive roots, and we let $G_\Delta(R)$ be the corresponding Steinberg group. Note that $U_\Delta(R)$ is nilpotent and any element in it can be written uniquely as a product $\prod_{\alpha \in \Delta^+} e_\alpha(r_\alpha)$. There are variations of this construction for twisted root systems, if the ring $R$ has a suitable automorphism, also in certain case these groups can be defined when the ring $R$ is non-commutative.

The cases not covered in the previous section are all groups with bounded Lie rank. So our aim is to prove that, on a log scale, $\sigma(G_\Delta(R))$ is comparable $\sigma(R, +)$ when the rank of $\Delta$ is bounded. Since $|G_\Delta(R)| \in |R|^{O(1)}$ the results will follow.

If the Dynkin diagram for the root system $\Delta$ contains $A_2$ as a subdiagram then $U_\Delta(R)$ contains $U(3, R)$ as a subgroup, thus we can use the results for classical groups to deduce that the Heisenberg group $U_\Delta(F_p^2)$ contains at least $p^{O(e^2/4)}$ isomorphism types of subgroups. This bound is easy to apply (and as in Remark 3.3 it applies only once $e \geq 9$). Tighter bounds would appear to require detailed study of the subgroups of unipotent groups of exceptional and twisted groups. We encourage such work but do not pursue it here.

Excluding the groups in Theorem 4.1 and groups of Lie type with a diagramatic embedding of $A_2$ exclude all but the following cases: $A_1$, $2A_2$, $2A_3$, $2A_4$, $B_2$, $2B_2$, $3D_4$, $2F_4$, $G_2$, $2G_2$. The groups $2B_2$, $2F_4$, and $2G_2$ exist only in for fields of orders $2^{1+2n}$, $2^{1+2n}$, and $3^{1+2n}$ respectively. We can avoid going over all cases, by relaxing the condition of containing $A_2$ as a subdiagram, to the containment of the corresponding root systems (maybe over a slightly smaller field).

† There is a unique element $c$ in the center of $H$, such that the set $\{g \in H | g^2 = c\}$ has exactly $2^k$ elements. The group $\Gamma_2$ is generated by all elements $g \in H$ such that $g^2 = c$. 


This leaves only

\[ A_1, \quad 2A_2, \quad B_2, \quad 2B_2, \quad 2F_4, \quad 2G_2. \]

We now cover these cases.

### 6.2 Type \( A_1 \) (PSL\(_2(\mathbb{F}_{p^e})\))

The Sylow \( p \)-subgroups of PSL\(_2(\mathbb{F}_{p^e})\) are isomorphic to \( \mathbb{Z}_{p^e} \) and so \( \sigma(\text{PSL}_2(\mathbb{F}_{p^e})) \in p^{\Theta(e^2)} \). Since \( |\text{PSL}_2(\mathbb{F}_{p^e})| \in p^{\Theta(e^2)} \) this bound is sufficient for our estimates. However, the \( p \)-subgroups are elementary abelian and so \( \sigma_i(\mathbb{Z}_{p^e}) = e + 1 \). In fact, the subgroups of PSL\(_2(\mathbb{F}_{p^e})\) have been classified. The maximal subgroups are either upper triangular, dihedral, \( \text{Alt}_5 \), or PSL\(_2(\mathbb{F}_{p^k})\) for \( k = e/q, q \) a prime dividing \( e \). The isomorphism types of subgroups of \( \text{Alt}_5 \) is bounded, and the subgroups of dihedral groups are dihedral or cyclic. Both of these groups are characterized up to isomorphism by their orders so they contribute at most \( |\text{PSL}_2(\mathbb{F}_{p^e})| \) distinct isomorphism classes. Finally, the group of upper triangular matrices is isomorphic to \( K^X \rtimes K \). If \( H \leq K^X \rtimes K \) then \( H \cap U_2(K) \) is normal in \( H \) and \( |H : H \cap U| = |HU : U| \) divides \( |K^X| \) is prime to \( p \). So \( H \cap U \) is the Sylow \( p \)-subgroup of \( H \). As \( H \) is solvable, it has a Hall \( p' \)-subgroup \( Q \) and so \( H = Q \rtimes \rho(H \cap U) \). Furthermore, \( Q \) is drawn from the subgroups of the cyclic group \( K^X \) and \( H \cap U \) is drawn from subspaces of \( (\mathbb{Z}/p)^e \). Therefore, the isomorphism of subgroups of a fixed order determined by the conjugacy classes of the images of the maps \( \rho : \mathbb{Z}/m \to K^X \rtimes GL_e(\mathbb{F}_p) \). Such images are conjugate if they have the same order. So, in total \( \sigma_i(\text{PSL}_2(\mathbb{F}_{p^e})) \in O(e^2 \log p) \).

**Remark 6.1.** If we constrain the rank and exponent and allow only the prime to vary then in general the diversity of subgroups of simple groups is severely limited. For instance, for every Mersenne prime \( p = 2^k - 1, n = |\text{PSL}_2(\mathbb{F}_p)| \) has \( \mu(n) \geq k + 1 \) and so \( \sigma_i(n) \in 2^{\Theta((\log n)^2)} \). Yet \( \sigma_i(\text{PSL}_2(\mathbb{F}_p)) \in O(\log n) \).

### 6.3 Type \( 2A_2 \) (PSU\(_3(\mathbb{F}_{p^{2e}})\))

We note that for \( p > 3 \), the Sylow \( p \)-subgroups of PSU\(_3(\mathbb{F}_{p^{2e}})\) are isomorphic to the Sylow \( p \)-subgroups of PSL\(_3(\mathbb{F}_{p^e})\). However, an estimate for all \( p \) is to use \( F = \mathbb{F}_{p^{2e}} \) with quadratic field involution \( \sigma \). To apply Theorem 2.3, use \( R = F^\sigma = \{ \alpha \in F \mid \alpha = \alpha^* \}, M = \{ \alpha \in F \mid \alpha + \alpha^* = 0 \}, S = \{ 1, \omega \} \) where \( F = \mathbb{F}_{p^e}[\omega] \) and \( T \) is any nonzero element in \( M \). Then apply Theorem 2.3.

### 6.4 Type \( B_2, \text{char } F \neq 2 \) (PSO\(_5(\mathbb{F}_{p^e})\))

Again this follows from Theorem 2.3 this time with \( R = M = F \), note that the natural commutator map is not the usual multiplication, but \( (r, m) \to 2rm \). However, if the characteristic is not equal to 2, then the multiplication is isotopic to the usual one. Another way to rephrase this is to say that \( U_{B_2}(F) \) contain a subgroup isomorphic to \( U_3(F) \).
6.5 Type $B_2$, char $F = 2$ ($\text{PSO}_5(2^e)$)

The main difference between $B_2(F)$ when char $F \neq 2$ and char $F = 2$ is that the nilpotency class of group $U := U_\Delta$ drops from 3 to 2 and the center becomes larger. This prevents us from applying Theorem 2.3 which needs three steps to form the nursery. However, we can modify the proof of that theorem to split the center as a direct sum.

In this case, $U$ is an extension of $F^2$ by $F^2$ where the commutator bi-map is:

$$[(r,s),(f,s)] = (r\bar{s} - \bar{r}s, r\bar{s}^2 - \bar{r}s^2).$$

We will also work with the quadratic map $\phi : F^2 \rightarrow F^2$ given by $\phi((r,s)) = (rs, rs^2)$.

The new series we consider for our nursery is

$$\Gamma_1 = U$$
$$\Gamma_2 = \{(r,0), z) \mid r \in F, z \in Z(U)\}$$
$$\Gamma_3 = Z(U) = [U, U]U^2 \cong \{(r,s) \mid r, s \in F\}$$
$$\Gamma_4 = \{(0,s) \mid s \in F\}$$
$$\Gamma_5 = 1.$$

To be precise, we use the epimorphisms $\alpha : U/\Gamma_3 \rightarrow F^2$ and the isomorphism $\beta : Z(U) \rightarrow F^2$; so, $\Gamma_2 = \alpha^{-1}(F,0)$ and $\Gamma_4 = \beta^{-1}(0,F)$. Once more we shall be interested in kinder $Q$ where $\Gamma_2 \leq Q \leq \Gamma_1$ and we shall need to expose what data in addition to the structure of $Q$ recover $\Gamma_i$.

Let $F = F_2[\omega]$ and consider kinder $Q$ that contain, $\alpha^{-1}((\omega^i, 0) \mid i \in \{-1,0,1\})$. This condition implies that $Z(Q) = [Q, Q] = \Gamma_3$. The quadratic map $\phi : Q/\Gamma_3 \rightarrow \Gamma_3$ has two maximal totally singular subspaces (since $\phi((r,s)) = 0$ if, and only if, $r = 0$ or $s = 0$) and the preimage of larger one in $Q$ is the subgroup $\Gamma_2$. Thus, $\Gamma_2 \leq Q$ can be characterized as the largest elementary abelian subgroup of $Q$. Hence, $\Gamma_2$ and $\Gamma_3$ are isomorphism invariants of kinder $Q$ containing $\alpha^{-1}((\omega^i, 0) \mid i \in \{-1,0,1\})$.

The first step is to construct enough elements in $\Gamma_1/\Gamma_2$ that will allow us to identify this space with the field $F$. For $i \in \{-1,0,1\}$ choose representatives $A_i \in \alpha^{-1}(\omega^i, 0)$ and $B_i \in \alpha^{-1}(0, \omega^i)$. We proceed by inductively defining further coset representatives $A_i$, by appealing to the following recurrence relation:

$$[A_{k+1}, B_{-1}][A_k, B_0] = [A_{k-2}, B_1][A_{k-1}, B_0].$$

This definition depends only on the initial choice of $A_i$, and $B_i$ for $i \in \{-1,0,1\}$, and commutation in $Q$ — which is an isomorphism invariant.

The elements $A_i$ allow us to identify $\Gamma_1/\Gamma_2$ with the field $F$, but after that to decompose the center $\Gamma_3$ as a direct sum $F \oplus F$. The subgroup $\Gamma_4$ can be characterized as the subgroup generated by $[A_{k+1}, B_{-1}][A_k, B_0]$ when $k$ varies, similarly we can identify its complement as the subgroup generated by $[A_{k+1}, B_{-1}][A_k, B_0]$ when $k$ varies. Finally, we can identify both $\Gamma_3/\Gamma_4$ and $\Gamma_4$ with $F$ by sending the $[A_k, B_0]\Gamma_0$ to $\omega^k$ and $[A_{k+1}, B_{-1}][A_k, B_0]$ to $\omega^k + \omega^{k-1}$. After all these we can map $Q$ to a additive subgroup of $F$ by sending $Q$ to image of $[Q, A_0]$ inside $\Gamma_3/\Gamma_4$. 

Thus, the number of isomorphism types of subgroups of $Q$ is at least the number of additive subgroups of $F$ which contain $1, \omega, \omega^{-1}$ divided by the number of possible choices for the elements $A_i$ and $B_i$ (only modulo $\Gamma_3$). Since $A_i$ and $B_i$ are constrained to be in the two totally singular subspaces, the number of choices for the $A_i$ is $p^{3e}$ and for the $B_i$ is $|Q/\Gamma_3|^3$.

Therefore, the number of isomorphism types of subgroups of $Q$ such that $|Q/\Gamma_2| = 2^\ell$ is at least at least $2^N$ where

$$N = (e - \ell)(\ell - 3) - 3e - 3\ell.$$ 

This is maximized when $\ell \approx e/2$ and gives $N = O(e^2/4)$ This bound is trivial for $e \leq 24$ and becomes nontrivial once $e > 24$.

### 6.6 Type $2B_2(F_{2e+1})$, Suzuki groups

Theorem 1.1 purposefully omits Suzuki groups because we have no proof of a bound for this case. What we include here is a reduction of the enumeration to a purely field property which we have verified computationally for all fields $F_{2^1+2e}$ with $1 + 2e \leq 1001$. This suggests to us that Suzuki groups indeed also fit a bound of the type reported in Theorem 1.1.

Assume that in a field $F_{2^1+2e}$ there is a subset $S$ such that $|S| \leq 3\sqrt{1 + 2e}$ and \{xy^{2e+1} - yx^{2e+1} | x, y \in S\} contains a basis for $F_{2^1+2e}$.

The group $U = U_3(F)$ is an extension of the additive group of $F$ by $F$ where the square is given by the $F_2$-quadratic map

$$\phi(x) = x^{1+2e+1}$$

(after the standard identification of the center and the abelianization with $F = F_{2^{2e+1}}$).

Fix a minimal $F_2$ subspace $V$ of $F$, such that the image of $V$ under $\phi$ spans the whole $F$ as an $F_2$ vector space, which by our assumption permits $\dim V \leq 3\sqrt{1 + 2e}$. Fix a basis $v_1, \ldots, v_f$ for $V$. (Evidently $\dim V \geq \sqrt{1 + 2e}$ at minimum. The size of $V$ is the so-called Sims rank of $U$; cf. [2, Section 5.2; 17].)

We will count the subgroups $H$ of $U$ whose projection into the $U/[U, U]$ contains the space $V$, together with specified elements $h_1, \ldots, h_f$ which project to $v_i$ in $U/[U, U]$. Taking the squares of all possible products of $h_i$ we can identify the subgroups $U^2$ (which is equal to $[U, U]$) with the field $F$ (of course this is only possible if all these elements satisfy the necessary linear relations), the important observation is that this identification does not depend on the embedding of $H$ in $U$. Using this identification, we can identify the quotient $H/H^2$ with the subspace of $F$ which contains $V$. The number of such spaces is of the order of $2^{(2e+1-f)2/4}$ and at most $2^{(2e+1+f)f/2}$ of these correspond to the same isomorphism type (the number of choices of $h_i$ modulo $H^2$). Thus, the number of isomorphism types of subgroups of $U$ is at least $2^N$ where

$$N = e^2 - 2ef = e^2 - O(e^{3/2}).$$

As in the other cases this bound is trivial for the first few Suzuki groups, and as we stress it is proved under the above assumption on fields of order $2^{1+2e}$. 
**6.7 | Type $2F_4(F_{2^{2e+1}})$, large Ree groups**

These groups contain a Heisenberg subgroup over $F$ and so a suitable lower bound on the number of isomorphism types comes from the above count of Heisenberg groups (cf. [11, 18]).

**6.8 | Type $2G_2(F_{3^{2e+1}})$, small Ree groups**

Finally, the small Ree groups contain a subgroup with the same associate graded Lie ring as the Heisenberg group (this can be seen from the commutation relations in [9]) over $F$ and we may appeal to Theorem 2.3 with $R = M = F$. If $F = F_{3^{2e+1}}$ this leads to about $3^{(2e-1)^2/4 - 8e - 4}$ different isomorphism types of subgroups in $U$ while the number of subgroups is bounded above by $3^{(9 - o(1))e^2}$.

**ACKNOWLEDGEMENTS**

We are grateful to Bob Guralnick and Bill Kantor for answers to questions on simple groups, and to the referee for helpful remarks and questions. Part of this work comprised the Master’s thesis of the second author at Colorado State University [19]. This work was partially supported by NSF Grants DMS-1620454 and DMS-1601406, and the Simons Foundation #636189, with thanks to the Hausdorff Institute for Mathematics and Isaac Newton Institute (EPSRC Grant Number: EP/R014604/1).

**JOURNAL INFORMATION**

The Bulletin of the London Mathematical Society is wholly owned and managed by the London Mathematical Society, a not-for-profit Charity registered with the UK Charity Commission. All surplus income from its publishing programme is used to support mathematicians and mathematics research in the form of research grants, conference grants, prizes, initiatives for early career researchers and the promotion of mathematics.

**REFERENCES**

1. M. Aschbacher, *On the maximal subgroups of the finite classical groups*, Invent. Math. **76** (1984), no. 3, 469–514. MR746539.
2. S. R. Blackburn, P. M. Neumann, and G. Venkataraman, *Enumeration of finite groups*, Cambridge Tracts in Mathematics, vol. 173, Cambridge University Press, Cambridge, 2007. MR2382539.
3. E. Bayer-Fluckiger, *Principe de Hasse faible pour les systèmes de formes quadratiques*, J. Reine Angew. Math. **378** (1987), 53–59 (French). MR895284.
4. H. R. Brahana, *Metabelian groups and trilinear forms*, Duke Math. J. **1** (1935), 185–197.
5. J. N. Bray, D. F. Holt, C. M. Roney-Dougal, *The maximal subgroups of the low-dimensional finite classical groups*, London Mathematical Society Lecture Note Series, vol. 407, Cambridge University Press, Cambridge, 2013. MR3098485.
6. P. A. Brooksbank and J. B. Wilson, *Computing isometry groups of Hermitian maps*, Trans. Amer. Math. Soc. **364** (2012), no. 4, 1975–1996. MR2869196.
7. P. A. Brooksbank, J. Maglione, and J. B. Wilson, *A fast isomorphism test for groups whose Lie algebra has genus 2*, J. Algebra **473** (2017), 545–590. MR3591162.
8. E. B. Dynkin, *Maximal subgroups of the classical groups*, Trudy Moskov. Mat. Obšč. **1** (1952), 39–166 (Russian). MR0049903.
9. F. Haot, K. Struyve, and H. Van Maldeghem, *Ree geometries*, Forum Math. **23** (2011), no. 1, 75–98.
10. D. Goldstein and R. M. Guralnick, *Alternating forms and self-adjoint operators*, J. Algebra **308** (2007), no. 1, 330–349, MR2290925.

11. D. Gorenstein, R. Lyons, and R. Solomon, *The classification of the finite simple groups. Number 3. Part I. Chapter A*, Mathematical Surveys and Monographs, vol. 40, Amer. Math Soc., Providence, RI, 1998. MR1490581.

12. G. Higman, *Enumerating $p$-groups. I. Inequalities*, Proc. London Math. Soc. (3) **10** (1960), 24–30. MR113948.

13. P. Kleidman and M. Liebeck, *The subgroup structure of the finite classical groups*, London Mathematical Society Lecture Note Series, vol. 129, Cambridge University Press, Cambridge, 1990. MR1057341.

14. M. L. Lewis and J. B. Wilson, *Isomorphism in expanding families of indistinguishable groups*, Groups Complex. Cryptol. **4** (2012), no. 1, 73–110. MR2921156.

15. F. J. MacWilliams, and N. J. A. Sloane, *The theory of error-correcting codes. II*, North-Holland Mathematical Library, vol. 16, North-Holland Publishing Co., Amsterdam–New York–Oxford, 1977. MR0465510.

16. L. Pyber, *Enumerating finite groups of given order*, Ann. of Math. (2) **137** (1993), no. 1, 203–220. MR1200081.

17. C. C. Sims, *Enumerating $p$-groups*, Proc. Lond. Math. Soc. (3) **15** (1965), 151–166. https://doi.org/10.1112/plms/s3-15.1.151. MR169921.

18. J. Tits, *Moufang octagons and the Ree groups of type $^2F_4$*, Amer. J. Math. **105** (1983), no. 2, 539–594. https://doi.org/10.2307/2374268.

19. B. A. Tyburski, *Asymptotic enumeration of matrix groups*, Thesis delivered to Department of Mathematics, The Colorado State University, 2018. https://hdl.handle.net/10217/191288.

20. G. E. Wall, *Some applications of the Eulerian functions of a finite group*, J. Austral. Math. Soc. **2** (1961/1962), 35–59. MR0125156.

21. J. B. Wilson, *Division, adjoints, and dualities of bilinear maps*, Comm. Algebra **41** (2013), no. 11, 3989–4008. MR3169502.

22. J. B. Wilson, *On automorphisms of groups, rings, and algebras*, Comm. Algebra **45** (2017), no. 4, 1452–1478, MR3576669.

23. J. B. Wilson, *The threshold for subgroup profiles to agree is logarithmic*, Theory Comput. **15** (2019), no. 19, 1–25.