Almost All p-Groups Have Automorphism Group a p-Group When p is Odd

Geir T. Helleloid
Department of Mathematics, Bldg. 380
Stanford University
Stanford, CA 94305-2125
geir@math.stanford.edu

Ursula Martin
Department of Computer Science
Queen Mary University of London
Mile End Road
London E1 4NS, UK
Ursula.Martin@dcs.qmul.ac.uk

Abstract

Many common finite p-groups admit automorphisms of order coprime to p, and when p is odd, it is reasonably difficult to find finite p-groups with automorphism group a p-group. Yet the goal of this paper is to prove that almost all finite p-groups do have automorphism group a p-group when p is odd. The asymptotic sense in which the theorem holds involves bounding the Frattini length of the p-groups and letting the number of generators go to infinity. The proof of the theorem draws on a detailed analysis of the Frattini series of a free group and the combinatorics linking finite p-groups and representations of $\mathrm{GL}(n, \mathbb{F}_p)$. The case of $p = 2$ remains open.

1 Introduction

The goal of this paper is to prove that, in a specific sense, almost all finite p-groups have automorphism group a p-group when p is odd. The result in question was first announced by the second author in [17], but this paper represents the first published proof. (Although [17] included the case $p = 2$, there seems to be a gap in the proof that is discussed later in this paper.)

The result may not seem entirely plausible at first, as many common finite p-groups do not have automorphism group a p-group: $\mathbb{Z}_{p^n}$ for p odd and Sylow p-subgroups of simple groups and Chevalley groups, for example. Furthermore, Bryant and Kovács [1] show that any finite group occurs as the quotient $A(H)$ of the automorphism group of some finite p-group H (where $A(H)$ is as defined

Order	$p = 2$	$p = 3$	$p = 5$
p^3	3 of 5	0 of 5	0 of 5
p^4	9 of 14	0 of 15	0 of 15
p^5	36 of 51	0 of 67	1 of 77
p^6	211 of 267	30 of 504	

Table 1: The proportion of p-groups of a given order with automorphism group a p-group.

below). Intuitively, our result is saying that most p-groups are complicated and unnatural-looking, and that familiar examples are far from typical.

It is reasonably easy to find finite 2-groups with automorphism group a 2-group: Z_{2^n}, the dihedral 2-group D_{2^n} ($n \geq 3$), and the generalized quaternion group Q_{2^n} ($n \geq 4$). It is more difficult to find finite p-groups with automorphism group a p-group when p is odd. In [7], Horoševskiĭ constructs such a p-group with nilpotence class n for each $n \geq 2$ and such a p-group on d generators for each $d \geq 3$. Furthermore, Horoševskiĭ shows in [7] and [8] that for any prime p, if $H_1, H_2, \ldots, H_n$ are finite p-groups with automorphism group a p-group, then so is the iterated wreath product $H_1 \wr H_2 \wr \cdots \wr H_n$. Otherwise, most known examples arise from complicated and unnatural-looking constructions (see [21]). Table 1 summarizes data obtained via GAP 4 [2] and the package AutPGrp on the number of small p-groups with automorphism group a p-group.

Of course, the meaning of the statement "If p is odd, then almost all finite p-groups have automorphism group a p-group" depends on the asymptotic interpretation of "almost all." The most natural interpretation is to consider all p-groups of order less than p^n and let n go to infinity. Unfortunately, this is not the sense in which our result holds, and indeed, the question remains open for this interpretation (see [16, Question 9]). The precise statement of our main theorem relies on a central series of a group called the *Frattini series*, which will be defined in Section 2. Following the standard terminology for central series, the *Frattini length* of a group is the number of non-identity terms in the associated Frattini series. The main theorem of this paper may be concisely stated as follows.

Theorem 1.1. *Fix an odd prime p and $n \geq 2$. If $r_{d,n}$ is the proportion of p-groups generated by at most d elements and with Frattini length at most n whose automorphism group is a p-group, then* $\lim_{d\to\infty} r_{d,n} = 1$.

The proof of Theorem 1.1 breaks down into three parts, which are presented in Sections 2, 5, and 6, and will be assembled to prove (slightly more general versions of) Theorem 1.1 in Section 7. In the remainder of this section, we will outline the structure of the proof.

For the first part of the proof, write F for the free group on d generators and F_i for the i-th term in the Frattini series of F. It transpires that $\mathrm{GL}(d, p)$ is the quotient of $\mathrm{Aut}(F/F_{n+1})$ by a subgroup in the kernel of the $\mathrm{Aut}(F/F_{n+1})$ action

on F_n/F_{n+1}, so that $\mathrm{GL}(d,p)$ acts on F_n/F_{n+1}, and the $\mathrm{Aut}(F/F_{n+1})$-orbits of normal subgroups of F_n/F_{n+1} are $\mathrm{GL}(d,p)$-orbits.

For any finite p-group H, write $A(H)$ for the group of automorphisms of $H/\Phi(H)$ induced by $\mathrm{Aut}(H)$ (where $\Phi(H)$ is the Frattini subgroup of H). We shall see that if $A(H)$ is a p-group, then so is $\mathrm{Aut}(H)$; in fact, our main goal is to prove, in some sense, that $A(H)$ is usually trivial.

In Section 2, after defining and investigating the Frattini series, we prove the following theorem.

Theorem 1.2. *Fix a prime p and $n \geq 2$. Let*

$$\begin{aligned}
\mathcal{A}_{d,n} &= \{\textit{normal subgroups of } F/F_{n+1} \textit{ lying in } F_2/F_{n+1}\}\\
\mathcal{B}_{d,n} &= \{\textit{normal subgroups of } F/F_{n+1} \textit{ lying in } F_2/F_{n+1}\\
&\qquad\qquad \textit{and not containing } F_n/F_{n+1}\}\\
\mathcal{C}_{d,n} &= \{\textit{normal subgroups of } F/F_{n+1} \textit{ lying in } F_n/F_{n+1}\}\\
\mathcal{D}_{d,n} &= \{\textit{normal subgroups of } F/F_{n+1} \textit{ contained in the}\\
&\quad \textit{regular } \mathrm{GL}(d,p)\textit{-orbits of } \mathcal{C}_{d,n}\}
\end{aligned}$$

$$\begin{aligned}
\mathfrak{A}_{d,n} &= \{\mathrm{Aut}(F/F_{n+1})\textit{-orbits in } \mathcal{A}_{d,n}\}\\
\mathfrak{B}_{d,n} &= \{\mathrm{Aut}(F/F_{n+1})\textit{-orbits in } \mathcal{B}_{d,n}\}\\
\mathfrak{C}_{d,n} &= \{\mathrm{Aut}(F/F_{n+1})\textit{-orbits in } \mathcal{C}_{d,n}\} = \{\mathrm{GL}(d,p)\textit{-orbits in } \mathcal{C}_{d,n}\}\\
\mathfrak{D}_{d,n} &= \{(\textit{regular})\ \mathrm{GL}(d,p)\textit{-orbits in } \mathcal{D}_{d,n}\}.
\end{aligned}$$

There is a well-defined map $\pi_{d,n}$ from $\mathfrak{A}_{d,n}$ into all groups given by $\pi_{d,n} : L/F_{n+1} \mapsto F/L$, where $L/F_{n+1} \in \mathcal{A}_{d,n}$. Then $\pi_{d,n}$ gives bijections

$$\begin{aligned}
\mathfrak{A}_{d,n} &\leftrightarrow \{d\textit{-generator } p\textit{-groups of Frattini length at most } n\}\\
\mathfrak{B}_{d,n} &\leftrightarrow \{d\textit{-generator } p\textit{-groups of Frattini length } n\}\\
\mathfrak{D}_{d,n} &\leftrightarrow \{\textit{subgroups } H \textit{ in } \pi_{d,n}(\mathfrak{C}_{d,n}) \textit{ with } A(H) = 1\}.
\end{aligned}$$

Recall that a regular orbit is one in which every point has trivial stabilizer. Note that

$$\mathcal{D}_{d,n} \subseteq \mathcal{C}_{d,n} \subseteq \mathcal{B}_{d,n} \cup \{F_n/F_{n+1}\} \subseteq \mathcal{A}_{d,n}.$$

Section 3 follows with a detailed examination of the module structure of the quotient F_n/F_{n+1} that will be needed in Section 5. Section 4 merely contains combinatorial estimates needed in Sections 5 and 6.

The second part of the proof of Theorem 1.1 is contained in Section 5. Writing d_n for the rank of F_n/F_{n+1}, we can prove the following numerical estimate.

Theorem 1.3. *Fix an odd prime p. Let $n \geq 3$ and $w = d_{n-1} - d_n/2(n-1) + d^2$. Then*

$$1 \leq \frac{|\mathfrak{A}_{d,n}|}{|\mathfrak{C}_{d,n}|} \leq 1 + O(p^w),$$

where w is viewed as a function of d.

The proof of Theorem 1.3 uses a theorem estimating the number of normal subgroups of an arbitrary p-group, applying it to factors of the Frattini series of a free group. Note that this is where the proof fails in the case $p = 2$; in particular, we have no analogue for Theorem 3.4 when $p = 2$.

The final part of the proof of Theorem 1.1, presented in Section 6, uses another numerical estimate.

Theorem 1.4. *Fix a prime p. Let*

$$x = \begin{cases} -d & : \quad n = 2 \\ d^2 - d_n/2 & : \quad n \geq 3. \end{cases}$$

Then, viewing x as a function of d,

(a)
$$1 \leq \frac{|\mathfrak{C}_{d,n}| \cdot |\mathrm{GL}(d,p)|}{|\mathcal{C}_{d,n}|} \leq 1 + O(p^x).$$

(b)
$$1 \leq \frac{|\mathfrak{C}_{d,n}|}{|\mathfrak{D}_{d,n}|} \leq 1 + O(p^x).$$

As we will show in Section 7, Theorem 1.1 follows easily from Theorems 1.2, 1.3, and 1.4(b). We close with some observations and open questions.

Notation. There are several notational conventions in this paper that may be used without comment. The symbol p will always denote a prime; p may equal 2 unless otherwise noted. The Frattini series will always be defined relative to the prime p. F will always denote the free group on d generators. The symbol d will always denote the number of generators of a p-group or of F. The rank of F_n/F_{n+1} will be denoted d_n. When convenient, the group $\mathrm{GL}(d, \mathbb{F}_p) = \mathrm{GL}(d, p)$ will be denoted by Σ.

2 The Frattini Series

In the next two sections, we shall define and discuss the *Frattini series* (or *lower p-series*) of a group, particularly of a free group. In Theorems 2.7 and 2.8 we describe how isomorphism classes of p-groups in a variety may be enumerated, obtaining Theorem 1.2 as a corollary.

2.1 Preliminaries

The Frattini series seems to have been introduced by Skopin [20] and Lazard [12], and is described in detail by Huppert and Blackburn [10, Chapter VIII] (under the name λ-series) and by Bryant and Kovács [1]. It is particularly suited to computer analysis of p-groups and forms the basis of the nilpotent quotient algorithm of Macdonald and Neumann (see [14]).

For any prime p and group H the Frattini series $H = H_1 \geq H_2 \geq \cdots$ of H is defined by $H_{i+1} = H_i^p[H_i, H]$ for $i \geq 1$. In particular, if H is a finite p-group, then H_2 is the Frattini subgroup of H. Recall that a subgroup is *fully invariant* if every endomorphism of the group restricts to an endomorphism of the subgroup. Each H_i is fully invariant in H, since if ϕ is an endomorphism of H and H_i is fully invariant, then $\phi(H_{i+1}) = \phi(H_i^p)[\phi(H_i), \phi(H)] \leq H_{i+1}$ and H_{i+1} is fully invariant. Furthermore, H_{i+1} is the smallest normal subgroup of H lying in H_i such that H_i/H_{i+1} is central in H/H_{i+1} and is an elementary abelian p-group (see Huppert and Blackburn [10, Chapter VIII, Corollary 1.6]).

Write $H = \gamma_1(H) \geq \gamma_2(H) \geq \cdots$ for the *lower central series* of H, where $\gamma_{i+1}(H) = [\gamma_i(H), H]$. The following proposition contains three further properties of the Frattini series.

Proposition 2.1 (Huppert and Blackburn [10, Chapter VIII, Theorem 1.5]).

1. $[H_i, H_j] \leq H_{i+j}$ *for* $i, j \geq 1$.
2. $H_i^{p^j} \leq H_{i+j}$ *for* $i, j \geq 1$.
3. $H_i = \gamma_1(H)^{p^{i-1}}\gamma_2(H)^{p^{i-2}} \cdots \gamma_i(H)$ *for* $i \geq 1$.

H is said to have *Frattini length* (or *Frattini class*) n if H_n is the last non-identity element of the Frattini series. Note that a finite group which is not a p-group does not have finite Frattini length, since the factors of the Frattini series are all p-groups.

2.2 The Frattini Series of p-Groups and Free Groups

Proposition 2.2. *If H is a finite p-group, then H has finite Frattini length.*

Proof. It suffices to show that if H_i is non-trivial, then $H_{i+1} < H_i$. Since H is nilpotent, $[H_i, H] < H_i$ (see Kurzweil and Stellmacher [11, Lemma 5.1.6]). Then $H_i/[H_i, H]$ is a non-trivial abelian p-group. Hence

$$H_i/[H_i, H] > (H_i/[H_i, H])^p = H_i^p[H_i, H]/[H_i, H],$$

and so $H_i > H_i^p[H_i, H] = H_{i+1}$. □

For the remainder of this paper, let F be the free group on d generators $y_1, \ldots, y_d$. The Frattini length of a p-group is related to the Frattini series of F in the following way. Any p-group H generated by at most d elements is isomorphic to F/U for some normal subgroup U of F. By induction, $H_i = F_iU/U$:

$$H_{i+1} = (F_iU/U)^p[F_iU/U, F/U] = F_i^p[F_i, F]U/U = F_{i+1}U/U.$$

Then the Frattini length of H is n, where F_{n+1} is the first term in the Frattini series of F contained in U. We will need two observations about the subgroup F_2, first recalling a simple result on the Frattini quotient.

Proposition 2.3. *If H is a finite p-group and θ is an endomorphism of H that induces an automorphism on the Frattini quotient of H, then θ is an automorphism of H.*

Proof. The image of H under θ contains coset representatives for each coset of H/H_2. Since H/H_2 is the Frattini quotient of H, these elements generate H and the image of H under θ is all of H. Hence θ is an automorphism. □

Proposition 2.4. *F_2 is a maximal fully invariant subgroup of F.*

Proof. Suppose $U > F_2$ is a fully invariant subgroup of F. The elements $y_1^{a_1} \cdots y_d^{a_d}$, with $0 \leq a_i < p$, form a complete set of coset representatives for the cosets of F_2 in F, so U contains an element $y = y_1^{a_1} \cdots y_d^{a_d}$ with some a_i nonzero. Then the endomorphism of F that sends y_j to 1 for $j \neq i$ and sends y_i to $y_k^{a_i^{-1}}$ for some choice $1 \leq k \leq d$ sends y to y_k, showing that $y_k \in U$. Hence $U = F$. □

Proposition 2.5. *Let U be a fully invariant subgroup of F contained in F_2 with $H = F/U$ a finite p-group. Then any automorphism θ of F/F_2 lifts to an automorphism of H.*

Proof. Since F is free, there is an endomorphism θ' of F such that $y_i\theta' \in (y_iF_2)\theta$ for $1 \leq i \leq d$. Therefore $y\theta' \in (yF_2)\theta$ for all $y \in F$. Then θ' induces θ on F/F_2, and since U is fully invariant, maps U to itself. So θ' induces an endomorphism θ'' of H. But θ'' induces θ, an automorphism of $F/F_2 \cong (F/U)/(F_2/U) \cong H/H_2$, the Frattini quotient of H. By Proposition 2.3, θ'' is an automorphism of H. Thus θ lifts to an automorphism θ'' of H. □

Finally, we note that by Huppert and Blackburn [10, Chapter VIII, Theorem 11.15], the rank of $F/[F,F]$, and hence of F/F_2, is d, and the rank of F_i/F_{i+1} is finite for each i (in Section 3, we will use the full statement of Theorem 11.15).

2.3 The Frattini Series and the Automorphism Group

In the next two subsections, we describe the automorphisms of a p-group H in terms of its Frattini series. Since each H_i is fully invariant in H, any automorphism of H induces by restriction automorphisms of each H_i/H_{i+1}. In particular any automorphism of H induces an element of $\mathrm{Aut}(H/H_2) = \mathrm{GL}(d,p)$ acting on H/H_2, where the rank of H/H_2 is d. Thus we obtain a map α_H from $\mathrm{Aut}(H)$ to $\mathrm{GL}(d,p)$, and an exact sequence

$$1 \to K(H) \to \mathrm{Aut}(H) \stackrel{\alpha_H}{\to} A(H) \to 1,$$

where $A(H)$ is a subgroup of $\mathrm{GL}(d,p)$. The group $K(H)$ acts trivially on H/H_2, and hence on each factor H_i/H_{i+1} (see Huppert and Blackburn [10, Chapter VIII, Theorem 1.7]). As $\mathrm{Aut}(H)$ acts on each H_i/H_{i+1} and the kernel of the action contains $K(H)$, we obtain an action of $A(H)$ on each H_i/H_{i+1}. Finally, the following key proposition is due to P. Hall [5, Section 1.3].

Proposition 2.6. *If H is a finite p-group, then so is $K(H)$.*

Proof. Suppose $\sigma \in K(H)$ has order q, where $q = 1$ or q is relatively prime to p. Any coset xH_2 of H_2 in H is fixed by σ, since σ acts trivially on H/H_2. The orbit of an element of xH_2 under σ has size dividing q, and $|xH_2|$ is a power of p, so some element of xH_2 is fixed by σ. Every coset of H_2 contains an element fixed by σ, and since H_2 is the Frattini subgroup of H, these coset representatives generate H. Thus σ fixes H and $q = 1$. Hence $K(H)$ is a p-group. □

2.4 Relatively Free Groups

A *variety of groups* V consists of all groups satisfying a set of relations that hold for all elements of the group (see Neumann [19]). For each positive integer d, the variety V contains a *relatively free group* on d generators, namely the unique group on d generators that satisfies only the defining relations. For example, all abelian groups form a variety, the variety in which the relation $ab = ba$ holds for all group elements a and b. Then the free abelian group on d generators is the relatively free group on d generators in the variety of abelian groups. We will only be interested in the variety of p-groups of Frattini length at most n, but the theorems in this subsection hold in more general situations.

Suppose that G is a finite non-trivial p-group that is the quotient of F by a fully invariant subgroup U, so that G is a relatively free group in some variety V on at most d generators. The relations defining V come from setting each word in U equal to the identity element. In this setting, we can describe $A(G)$ and $K(G)$ more precisely.

Since F_2 and U are fully invariant in F, we know that F_2U is a fully invariant subgroup of F containing F_2. By Proposition 2.4, either $F = F_2U$ or $F_2 = F_2U$. In the first case, $F = U$, contradicting the non-triviality of G. Thus $F_2 = F_2U$ and $U \leq F_2$. As noted in Subsection 2.2, F/F_2 has rank d. G is the quotient of F by U, and any minimal generating set of F maps to a generating set of G, so G is generated by at most d elements. But F/F_2 is the quotient of G by F_2/U, and F/F_2 has rank d, so G is a d-generator group.

Theorem 2.7. *Suppose that G is the relatively free group on d generators in a variety of groups V and that $|G| = p^g$. Then*

$$1 \to K(G) \to \mathrm{Aut}(G) \to \mathrm{GL}(d, p) \to 1$$

is exact and $|K(G)| = p^{d(g-d)}$. Furthermore, the map $L \mapsto G/L$ defines a bijection between $\mathrm{Aut}(G)$-orbits of normal subgroups L of G lying in G_2 and d-generator groups in V. If $H = G/L$, then

$$1 \to B(L) \to N_{\mathrm{Aut}(G)}(L) \to \mathrm{Aut}(H) \to 1$$

is exact, where $B(L)$ is the subgroup of $N_{\mathrm{Aut}(G)}(L)$ that acts trivially on H. If $|L| = p^m$, then $|B(L)| = p^{dm}$.

Proof. By Proposition 2.5, any automorphism θ of $F/F_2 \cong G/G_2$ lifts to an automorphism of G. Thus $A(G)$ is the full automorphism group of F/F_2, which is $\mathrm{GL}(d,p)$. This proves that $1 \to K(G) \to \mathrm{Aut}(G) \to \mathrm{GL}(d,p) \to 1$ is exact.

Let $x_1, \ldots, x_d$ be a minimal generating set for G. Also let L be a normal subgroup of G lying in G_2 and let $u_1, \ldots, u_d$ be any elements of L. Since G is relatively free, the map $\alpha : x_i \to x_i u_i$ for each i is an endomorphism of G (it suffices to check that if a word w in the x_i's equals 1, then $w\alpha = 1$, but every tuple of elements of G satisfies the same relations, so when x_i is replaced by $x_i u_i$ in w, the new word also equals 1). Note that α acts trivially on G/L and that by Proposition 2.3, α is an automorphism. Any automorphism of G that acts trivially on G/L has this form: it must act on each x_i as multiplication by an element of L. Thus the number of automorphisms of G that acts trivially on G/L is $|L|^d$. Taking $L = G_2$ gives $|K(G)| = p^{d(g-d)}$.

Next, we claim that any d-generator group H in V is isomorphic to G/L for some normal subgroup L of G lying in G_2. Evidently H is isomorphic to G/L for some normal subgroup L of G; it suffices to show that if $L \not\leq G_2$, then G/L will be generated by fewer than d elements. Choose $x_1 \in L \setminus G_2$. Extend $\{x_1\}$ to a generating set $\{x_1, \ldots, x_d\}$ of G. Then G/L is generated by the images of $\{x_2, \ldots, x_d\}$.

Clearly any normal subgroup of G in the same $\mathrm{Aut}(G)$-orbit as L has the same quotient, so the map $L \mapsto G/L$ is well-defined on $\mathrm{Aut}(G)$-orbits of normal subgroups of G lying in G_2. To show that this is a bijection, we must show that if M is a normal subgroup of G lying in G_2 with $G/M \cong G/L$, then M is in the same $\mathrm{Aut}(G)$-orbit as L. Let $\beta : G/L \to G/M$ be an isomorphism. Let $\delta : G \to G/M$ be the homomorphism given by the quotient map to G/L composed with β, and let $\alpha : G \to G/M$ be the quotient map. By [19, Theorem 44.21], G is projective, as in [19, Definition 44.11]; as α is surjective, this says that there exists an endomorphism $\gamma : G \to G$ so that $\gamma\alpha = \delta$. Since $\ker \delta = L$, it must be that $L\gamma \leq M$. Note that β induces an automorphism of G/G_2 as $(G/L)/(G_2/L) \cong G/G_2 \cong (G/M)/(G_2/M)$. As γ induces β, it follows from Proposition 2.3 that γ is an automorphism of G. Then $L\gamma = M$ and L and M are in the same $\mathrm{Aut}(G)$-orbit.

If we take $L = M$, we find that any automorphism of $H = G/L$ is induced by an automorphism of G, so that $\mathrm{Aut}(H) \cong N_{\mathrm{Aut}(G)}(L)/B(L)$, where $B(L)$ is the subgroup of $N_{\mathrm{Aut}(G)}(L)$ that acts trivially on H. By the second paragraph of this proof, $|B(L)| = |L|^d$. □

Theorem 2.8. *Suppose that G is the relatively free group on d generators in a variety of groups V and suppose that G has Frattini length n. The map $L \mapsto G/L$ defines a bijection between $\mathrm{GL}(d,p)$-orbits on normal subgroups of G lying in G_n and d-generator groups H in V with $H/H_n \cong G/G_n$. If $H = G/L$, then*

$$1 \to K(G)/B(L) \to \mathrm{Aut}(H) \to N_{\mathrm{GL}(d,p)}(L) \to 1$$

is exact, where $B(L)$ is the subgroup of $N_{\mathrm{Aut}(G)}(L)$ that acts trivially on H. Moreover, $K(H)$ is the image of $K(G)/B(L)$ in $\mathrm{Aut}(H)$.

Proof. $H/H_n = (G/L)/(G_nL/L) \cong G/G_nL$ is congruent to G/G_n if and only if $L \leq G_n$. Furthermore, $K(G)$ acts trivially on $G_n \cong G_n/G_{n+1}$ as noted in Subsection 2.3, so the $\mathrm{Aut}(G)$-orbits of normal subgroups of G lying in G_n are just the $\mathrm{GL}(d,p)$-orbits. This proves the bijection.

Since $K(G)$ fixes L, it also follows that

$$1 \to K(G) \to N_{\mathrm{Aut}(G)}(L) \to N_{\mathrm{GL}(d,p)}(L) \to 1$$

is exact. Combined with the second exact sequence in Theorem 2.7, we find that

$$1 \to K(G)/B(L) \to \mathrm{Aut}(H) \to N_{\mathrm{GL}(d,p)}(L) \to 1$$

is exact. Every automorphism in $K(G)$ induces an automorphism in $K(H)$ since $K(G)$ fixes L and $G/G_2 \cong H/H_2$. Conversely, every automorphism in $K(H)$ is induced by an automorphism in $K(G)$. The kernel of the map from $K(G)$ to $K(H)$ is $B(L)$, so $K(H)$ is the image of $K(G)/B(L)$. □

We can now prove Theorem 1.2, restated here for convenience.

Theorem 1.2. *Fix a prime p and $n \geq 2$. Let*

$$\begin{aligned}
\mathcal{A}_{d,n} &= \{\textit{normal subgroups of } F/F_{n+1} \textit{ lying in } F_2/F_{n+1}\} \\
\mathcal{B}_{d,n} &= \{\textit{normal subgroups of } F/F_{n+1} \textit{ lying in } F_2/F_{n+1} \\
&\qquad\qquad \textit{and not containing } F_n/F_{n+1}\} \\
\mathcal{C}_{d,n} &= \{\textit{normal subgroups of } F/F_{n+1} \textit{ lying in } F_n/F_{n+1}\} \\
\mathcal{D}_{d,n} &= \{\textit{normal subgroups of } F/F_{n+1} \textit{ contained in the} \\
&\qquad \textit{regular } \mathrm{GL}(d,p)\textit{-orbits of } \mathcal{C}_{d,n}\}
\end{aligned}$$

$$\begin{aligned}
\mathfrak{A}_{d,n} &= \{\mathrm{Aut}(F/F_{n+1})\textit{-orbits in } \mathcal{A}_{d,n}\} \\
\mathfrak{B}_{d,n} &= \{\mathrm{Aut}(F/F_{n+1})\textit{-orbits in } \mathcal{B}_{d,n}\} \\
\mathfrak{C}_{d,n} &= \{\mathrm{Aut}(F/F_{n+1})\textit{-orbits in } \mathcal{C}_{d,n}\} = \{\mathrm{GL}(d,p)\textit{-orbits in } \mathcal{C}_{d,n}\} \\
\mathfrak{D}_{d,n} &= \{(\textit{regular})\ \mathrm{GL}(d,p)\textit{-orbits in } \mathcal{D}_{d,n}\}.
\end{aligned}$$

There is a well-defined map $\pi_{d,n}$ from $\mathfrak{A}_{d,n}$ into all groups given by $\pi_{d,n} : L/F_{n+1} \mapsto F/L$, where $L/F_{n+1} \in \mathcal{A}_{d,n}$. Then $\pi_{d,n}$ gives bijections

$$\begin{aligned}
\mathfrak{A}_{d,n} &\leftrightarrow \{d\textit{-generator } p\textit{-groups of Frattini length at most } n\} \\
\mathfrak{B}_{d,n} &\leftrightarrow \{d\textit{-generator } p\textit{-groups of Frattini length } n\} \\
\mathfrak{D}_{d,n} &\leftrightarrow \{\textit{subgroups } H \textit{ in } \pi_{d,n}(\mathfrak{C}_{d,n}) \textit{ with } A(H) = 1\}.
\end{aligned}$$

Proof. Take V to be the variety of p-groups of Frattini length at most n. Then F/F_{n+1} is the relatively free group on d generators in V. That the $\mathrm{Aut}(F/F_{n+1})$- and $\mathrm{GL}(d,p)$-orbits in $\mathcal{C}_{d,n}$ are the same follows from the first exact sequence in Theorem 2.7 and the fact that $K(F/F_{n+1})$ acts trivially on F_n/F_{n+1} as in Subsection 2.3.

The map $\pi_{d,n}$ is well-defined and defines bijections for $\mathfrak{A}_{d,n}$ and $\mathfrak{B}_{d,n}$ by Theorem 2.7. A normal subgroup L of F/F_{n+1} lying in F_n/F_{n+1} is in a regular $\mathrm{GL}(d,p)$-orbit if $N_{\mathrm{GL}(d,p)}(L) = 1$. By Theorem 2.8, L is in a regular orbit if and only if $A(H) = 1$. Thus the bijection for $\mathfrak{D}_{d,n}$ is proved. □

Note, by the way, that since F_n/F_{n+1} is elementary abelian and central in F/F_{n+1}, the set $\mathcal{C}_{d,n}$ is just the set of subspaces of the vector space F_n/F_{n+1}.

3 The Frattini Factors of a Free Group

Let K be the field of p elements and $\Sigma = \mathrm{GL}(d,p)$. For $n \geq 1$, let $L_n = \gamma_n(F)/\gamma_n(F)^p\gamma_{n+1}(F)$, an elementary abelian p-group whose rank is given by Witt's formula $w_d(n) = (1/n)\sum_{j|n} d^j\mu(n/j)$, where μ is the Mobiüs function (see Huppert and Blackburn [10, Chapter VIII, Theorem 11.15]). In particular, $L_1 \cong F/F_2$ has rank d. Bryant and Kovács [1] show that both L_n and F_n/F_{n+1} are $K\Sigma$-modules. In preparation for Sections 5 and 6, we need to analyze the structure of F_n/F_{n+1} as a $K\Sigma$-module, as well as investigate certain power and commutator maps from F_n/F_{n+1} to F_{n+1}/F_{n+2}. Write $L(n) = L_1 \oplus \cdots \oplus L_n$.

Theorem 3.1. *Define a map $\alpha_n : L(n) \to F_n/F_{n+1}$ by*

$$\alpha_n : (\overline{a}_1, \ldots, \overline{a}_n) \to a_1^{p^{n-1}} a_2^{p^{n-2}} \cdots a_n F_{n+1},$$

where $a_i \in \gamma_i(F)$ and $\overline{a}_i$ is the image of a_i in L_i.

1. [10, Chapter VIII, Theorem 1.9b] *The map α_n is well-defined and is a bijection.*

2. [1, Section 3], [10, Chapter VIII, Theorem 1.9c] *If p is odd, then the map α_n is a $K\Sigma$-isomorphism.*

Corollary 3.2. *The rank of F_n/F_{n+1} is equal to*

$$\sum_{i=1}^{n} w_d(i) = \sum_{i=1}^{n} (1/i) \sum_{j|i} d^j \mu(i/j),$$

which is asymptotic to d^n/n as $d \to \infty$.

The map α_n is connected with a power map in the following theorem.

Theorem 3.3. *Let ι be the natural embedding of $L(n)$ into $L(n+1)$ and let $\phi_n : F_n/F_{n+1} \to F_{n+1}/F_{n+2}$ be the power map $\phi_n : xF_{n+1} \to x^pF_{n+2}$. Unless $p = 2$ and $n = 1$, ϕ_n is an injective homomorphism and $\phi_n = \alpha_n^{-1}\iota\alpha_{n+1}$.*

Proof. Suppose $x, y \in F_n$ and either $p > 2$ or $n > 1$. Then

$$(xy)^p \equiv x^p y^p \mod \gamma_2(F)^p\gamma_p(F_n)$$

by [10, Chapter VIII, Lemma 1.1a]. By Proposition 2.1, $\gamma_2(F_n)^p\gamma_p(F_n) \leq F_{2n+1}F_{pn} \leq F_{n+2}$. So $(xy)^p \equiv x^p y^p \mod F_{n+2}$ and ϕ_n is a homomorphism. Furthermore, if

$$x = a_1^{p^{n-1}} \cdots a_n F_{n+1} = (\overline{a}_1, \ldots, \overline{a}_n)\alpha_n \in F_n/F_{n+1},$$

then

$$x\phi_n = a_1^{p^n} \cdots a_n^p F_{n+2} = x\alpha_n^{-1}\iota\alpha_{n+1}.$$

Since α_n^{-1}, ι, and α_{n+1} are all injective, by Theorem 3.1, so is ϕ_n. □

In Section 5, we will also need a commutator map as in the following theorem.

Theorem 3.4. *Fix an odd prime p. For any generator y_k of F, define the map $\rho_{n,k} : L(n+1) \to L(n+1)$ by*

$$\rho_{n,k} : (\overline{a}_1, \ldots, \overline{a}_{n+1}) \mapsto (1, \overline{[a_1, y_k]}, \ldots, \overline{[a_n, y_k]}).$$

Then $\rho_{n,k}$ is a homomorphism, and for $xF_{n+1} \in F_n/F_{n+1}$,

$$(xF_{n+1})\alpha_n^{-1}\iota\rho_{n,k}\alpha_{n+1} = [x, y_k]F_{n+2}.$$

Furthermore, the kernel of $\alpha_n^{-1}\iota\rho_{n,k}\alpha_{n+1}$ is $\left\langle y_k^{p^{n-1}} F_{n+1} \right\rangle$.

Proof. First we need to show that $\rho_{n,k}$ is well-defined. Namely, we need to show that if $z \in \gamma_i(F)^p\gamma_{i+1}(F)$, then $[a_i, y_k] \equiv [a_i z, y_k] \mod \gamma_{i+1}(F)^p\gamma_{i+2}(F)$. By [10, Chapter VIII, Theorem 1.8a], z can be written in the form $z = z_i^p z_{i+1}$, where $z_i \in \gamma_i(F)$ and $z_{i+1} \in \gamma_{i+1}(F)$. Then

$$\begin{aligned}
[a_i z, y_k] &= [a_i, y_k]^z [z, y_k] \\
&= [a_i, y_k]^z [z_i^p, y_k]^{z_{i+1}} [z_{i+1}, y_k] \\
&\equiv [a_i, y_k][z_i^p, y_k] \mod \gamma_{i+1}(F)^p\gamma_{i+2}(F),
\end{aligned}$$

because $[z_{i+1}, y_k] \in \gamma_{i+2}(F)$, $[a_i, y_k], [z_i^p, y_k] \in \gamma_{i+1}(F)$, and L_{i+1} is central in $F/\gamma_{i+1}(F)^p\gamma_{i+2}(F)$. By [10, Chapter VIII, Theorem 1.1b],

$$[z_i^p, y_k] \equiv [z_i, y_k]^p \mod \gamma_2(\langle z_i, [z_i, y_k]\rangle)^p\gamma_p(\langle z_i, [z_i, y_k]\rangle).$$

By [9, Chapter III, Lemma 1.11], the subgroup $\gamma_2(\langle z_i, [z_i, y_k]\rangle)$ is the normal closure of $[z_i, y_k, z_i]$ in $\langle z_i, [z_i, y_k]\rangle$. Thus $\gamma_2(\langle z_i, [z_i, y_k]\rangle) \leq \gamma_{2i+1}(F) \leq \gamma_{i+2}(F)$, so

$$\begin{aligned}
[a_i z, y_k] &\equiv [a_i, y_k][z_i, y_k]^p \mod \gamma_{i+1}(F)^p\gamma_{i+2}(F) \\
&\equiv [a_i, y_k] \mod \gamma_{i+1}(F)^p\gamma_{i+2}(F).
\end{aligned}$$

Thus $\rho_{n,k}$ is well-defined. Next, to show $\rho_{n,k}$ is a homomorphism, we observe that if $a_i, b_i \in \gamma_i(F)$, then

$$\begin{aligned}
[a_i b_i, y_k] &= [a_i, y_k]^{b_i}[b_i, y_k] \\
&\equiv [a_i, y_k][b_i, y_k] \mod \gamma_{i+1}(F)^p\gamma_{i+2}(F),
\end{aligned}$$

since $[a_i, y_k] \in \gamma_{i+1}(F)$ and L_{i+1} is central in $F/\gamma_{i+1}(F)^p\gamma_{i+2}(F)$. Thus $\rho_{n,k}$ is a homomorphism. For $xF_{n+1} = x_1^{p^{n-1}} x_2^{p^{n-2}} \cdots x_n F_{n+1} \in F_n/F_{n+1}$,

$$\begin{aligned}(xF_{n+1})\alpha_n^{-1}\iota\rho_{n,k}\alpha_{n+1} &= (x_1, x_2, \ldots, x_n, 1)\rho_{n,k}\alpha_{n+1} \\ &= (1, [x_1, y_k], \ldots, [x_n, y_k])\alpha_{n+1} \\ &= [x_1, y_k]^{p^{n-1}}[x_2, y_k]^{p^{n-2}} \cdots [x_n, y_k]F_{n+2}.\end{aligned}$$

On the other hand,

$$\begin{aligned}[x, y_k] &= [x_1^{p^{n-1}} \cdots x_n, y_k] \\ &= [x_1^{p^{n-1}}, y_k]^{x_2^{p^{n-2}} \cdots x_n}[x_2^{p^{n-2}}, y_k]^{x_3^{p^{n-3}} \cdots x_n} \cdots [x_n, y_k] \\ &\equiv [x_1^{p^{n-1}}, y_k] \cdots [x_n, y_k] \mod F_{n+2},\end{aligned}$$

since $[x_1^{p^{n-1}}, y_k], \ldots, [x_n, y_k] \in F_{n+1}$ and F_{n+1}/F_{n+2} is central in F/F_{n+2}. Furthermore, by [10, Chapter VIII, Theorem 1.1b],

$$\begin{aligned}&[x_i^{p^{n-i}}, y_k] \\ \equiv\ &[x_i, y_k]^{p^{n-i}} \mod \gamma_2(\langle x_i, [x_i, y_k]\rangle)^{p^{n-i}} \prod_{r=1}^{n-i} \gamma_{p^r}(\langle x_i, [x_i, y_k]\rangle)^{p^{n-r}}.\end{aligned}$$

By [9, Chapter III, Lemma 1.11], $\gamma_2(\langle x_i, [x_i, y_k]\rangle)^{p^{n-i}} \leq \gamma_{n+i+1}(F) \leq F_{n+2}$ and

$$\gamma_{p^r}(\langle x_i, [x_i, y_k]\rangle)^{p^{n-r}} \leq \gamma_{ip^r+n-r}(F) \leq F_{n+2}.$$

Thus

$$(xF_{n+1})\alpha_n^{-1}\iota\rho_{n,k}\alpha_{n+1} = [x, y_k] \mod F_{n+2}.$$

To show that the kernel of $\alpha_n^{-1}\iota\rho_{n,k}\alpha_{n+1}$ is generated by $y_k^{p^{n-1}}F_{n+1}$, since α_n^{-1}, ι, and α_{n+1} are all injective, it suffices to show that the kernel of $\rho_{n,k}|_{L(n)}$ is generated by $y_k^{p^{n-1}}\alpha_n^{-1}\iota = (y_k, 1, \ldots, 1)$.

Let $\delta_i : L_i \to L_{i+1}$ be the homomorphism given by $x \mapsto [x, y_k]^{-1} = [y_k, x]$ (this is a homomorphism because L_{i+1} is elementary abelian). We need to show that the kernel of δ_1 is generated by y_k and that for $i > 1$, δ_i is injective. Clearly we may assume that $k = 1$.

The group L_i has a basis given by standard bracketings of Lyndon words of length i, as explained in [3, Section 3]. In this case, a Lyndon word of length i is a word on the alphabet $\{y_1, \ldots, y_d\}$ of length i that is strictly smaller than all its (non-empty) tails; here, we are linearly ordering our alphabet $y_1 < \cdots < y_d$. Given a Lyndon word w, write $w = w_1w_2$, where w_2 is the longest Lyndon tail of w. Then w_1 is a Lyndon word and $w_1 < w_2$. The standard bracketing of w is recursively defined as $b[w] = [b[w_1], b[w_2]]$. The set $\{b[w] : w \text{ is a Lyndon word of length } i\}$ is a basis for L_i.

Suppose w is a Lyndon word of length i. Unless $i = 1$ and $w = y_1$, we see that $y_1 w$ is smaller than w, and hence smaller than all of its tails, and so $y_1 w$ is a Lyndon word of length $i + 1$. Furthermore, w is the longest Lyndon tail of $y_1 w$, so the standard bracketing of $y_1 w$ is given by $b[y_1 w] = [y_1, b[w]]$. Thus the image of $b[w]$ under δ_i is a basis element for L_{i+1}, unique for each w. Since δ_i is a homomorphism, it follows that δ_1 has kernel generated by y_1 and δ_i is injective for $i > 1$. □

4 Gaussian Coefficient Estimates

The purpose of this section is to prove several estimates needed in Sections 5 and 6. Most of the estimates involve Gaussian coefficients, and so we will begin with the relevant definitions and bounds on the Gaussian coefficients obtained by Wilf [23].

The *Gaussian coefficient*

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n - 1) \cdots (q^n - q^{k-1})}{(q^k - 1) \cdots (q^k - q^{k-1})}$$

is the number of k-dimensional subspaces of a vector space of dimension n over the field of q elements. We shall be concerned with estimates for $\begin{bmatrix} n \\ k \end{bmatrix}_q$ and for the *Galois number*

$$\mathcal{G}_n(q) = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q,$$

which is the total number of subspaces of a vector space of dimension n over the field of q elements. These numbers have been studied for a long time in connection with elliptic functions, partitions of integers, and the lattice of subspaces of a finite dimensional vector space; a survey is given by Goldman and Rota [4]. As $q \to 1$, we have $\begin{bmatrix} n \\ k \end{bmatrix}_q \to \binom{n}{k}$, the usual binomial coefficient, and it turns out that many identities involving binomial coefficients arise in this way from their q-analogues, in which the binomial coefficient is replaced by the corresponding Gaussian coefficient. For instance,

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q + q^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q$$

becomes the familiar Pascal's triangle identity as $q \to 1$, and

$$x^n = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q (x-1)(x-q) \cdots (x-q^{k-1})$$

is a q-analogue of the binomial theorem. The following estimates are obtained in Wilf [23].

Lemma 4.1. *Let*

$$\begin{aligned} D(q) &= \prod_{j=1}^{\infty}(1-q^{-j})^{-1} \\ C(q) &= \sum_{r=-\infty}^{\infty} q^{-r^2} \\ C'(q) &= \sum_{r=-\infty}^{\infty} q^{-(r-1/2)^2} \\ S_n(q) &= \sum_{k=0}^{n} q^{k(n-k)} = q^{n^2/4}\sum_{k=0}^{n} q^{-(k-n/2)^2}. \end{aligned}$$

Then

$$D(q)q^{k(n-k)}(1-O(q^{-\min(k,n-k)})) \le \begin{bmatrix} n \\ k \end{bmatrix}_q \le D(q)q^{k(n-k)} \quad (1)$$

$$S_n(q)D(q)(1-O(q^{-n/2})) \le \mathcal{G}_n(q) \le S_n(q)D(q) \quad (2)$$

$$S_n(q) \sim q^{n^2/4}C(q) \quad (n\to\infty,\ n\ even) \quad (3)$$

$$S_n(q) \sim q^{n^2/4}C'(q) \quad (n\to\infty,\ n\ odd) \quad (4)$$

$$\lim_{n\to\infty}\mathcal{G}_n(q)q^{-n^2/4} = D(q)C(q) \quad (n\to\infty,\ n\ even) \quad (5)$$

$$\lim_{n\to\infty}\mathcal{G}_n(q)q^{-n^2/4} = D(q)C'(q) \quad (n\to\infty,\ n\ odd) \quad (6)$$

$$(7)$$

The next lemma will allow us to give an upper bound for $\mathcal{G}_n(q)$, among other uses.

Lemma 4.2. *Let $f(x) = -ax^2 + bx + c$ with $a > 0$, let $|q| > 1$, and set $A(q) = \sum_r q^{f(r)}$, where the sum is over all integers r with $t \le r \le u$. Then $A(q) \le C(q^a)q^{f(y)}$ for some $y \in [t,u]$.*

Proof. Suppose the maximum of $f(x)$ in $[t,u]$ occurs at $x = y$. The global maximum of $f(x)$ occurs at $x = b/2a$, so one of three cases holds: $b/2a \le y = t$, $u = y \le b/2a$, or $t \le y = b/2a = u$. In each case, for all $r \in [t,u]$,

$$\begin{aligned} & -a(r-y)^2 - f(r) + f(y) \\ = \ & -a(r-y)^2 - (-ar^2+br+c) + (-ay^2+by+c) \\ = \ & (2ay-b)(r-y) \\ \ge \ & 0. \end{aligned}$$

Thus

$$\begin{aligned} A(q) &= q^{f(y)} \sum_{t \le r \le u} q^{f(r)-f(y)} \\ &\le q^{f(y)} \sum_{t \le r \le u} q^{-a(r-y)^2} \\ &\le q^{f(y)} \sum_{r=-\infty}^{\infty} q^{-a(r-y)^2}, \end{aligned}$$

and it suffices to show that

$$g(y) = \sum_{r=-\infty}^{\infty} s^{-(r-y)^2} \le g(0),$$

where $s = q^a$. This is a consequence of Jacobi's functional equation for the theta function

$$\theta_3(z,w) = \sum_{r=-\infty}^{\infty} e^{r^2 \pi i w} e^{2riz},$$

where $|e^{\pi i w}| < 1$. Section 21.51 of Whittaker and Watson [22] gives the functional equation

$$\theta_3(z,w) = \frac{1}{\sqrt{-iw}} e^{z^2/\pi i w} \theta_3(z/w, -1/w)$$

where $\sqrt{e^{i\theta}}$ denotes $e^{i\theta/2}$ for $0 \le \theta \le 2\pi$. Now

$$\begin{aligned} g(y) &= s^{-y^2} \sum_{r=-\infty}^{\infty} s^{-r^2} e^{-2ri(iy \log s)} \\ &= s^{-y^2} \theta_3(-iy \log s, w), \end{aligned}$$

where $s^{-1} = e^{\pi i w}$ so that $\pi i w = -\log s$. Hence

$$\begin{aligned} g(y) &= \frac{s^{-y^2}\sqrt{\pi}}{\sqrt{\log s}} e^{y^2 \log s} \theta_3(-\pi y, -1/w) \\ &= \sqrt{\frac{\pi}{\log s}} \sum_{r=-\infty}^{r=\infty} e^{-r^2\pi^2/\log s} e^{-2ir\pi y} \\ &= \sqrt{\frac{\pi}{\log s}} (1 + 2\sum_{r=1}^{\infty} e^{-r^2\pi^2/\log s} \cos 2r\pi y) \\ &\le \sqrt{\frac{\pi}{\log s}} (1 + 2\sum_{r=1}^{\infty} e^{-r^2\pi^2/\log s}) \\ &= g(0). \end{aligned}$$

□

It is easy to derive an upper bound for $\mathcal{G}_n(q)$.

Lemma 4.3. *For any positive integer n, we have $\mathcal{G}_n(q) \le q^{n^2/4} D(q) C(q)$.*

Proof. By Lemma 4.1, Equation 2, we have

$$\begin{aligned} \mathcal{G}_n(q) &\le S(n) D(q) \\ &= D(q) \sum_{k=0}^{n} q^{k(n-k)} \\ &\le D(q) C(q) q^{n^2/4}, \end{aligned}$$

where the last inequality follows from Lemma 4.2, taking $f(x) = x(n-x) = -x^2 + nx$ and noting that $x(n-x) \le n^2/4$ for all x. □

Finally we shall prove Theorem 4.4, which will be needed in Section 5 to bound products of Gaussian coefficients, and Lemma 4.5, which will be used in Section 6.

Theorem 4.4. *Fix a prime p and $n \ge 2$. Let d_n be the rank of F_n/F_{n+1}. For $1 \le i \le n-1$ and $0 \le u_i \le d_i$, let*

$$A_{p,i}(u_i) = \sum \prod_{j=i}^{n-1} p^{-(u_{j+1}-d_{j+1})(u_{j+1}-u_j/j)},$$

where the sum is over all integers $u_{i+1}, \ldots, u_n$ such that

$$\begin{array}{rcll} 0 \le & u_j & \le d_j & i+1 \le j \le n-2 \\ 1 \le & u_{n-1} & \le d_{n-1} & \\ 2 \le & u_n & \le d_n. & \end{array}$$

Write $m = 1 - 1/4(n-1)^2$ and $M = C(p^m) p^{-m + d_n^2/4 + d_{n-1} - d_n/2(n-1)}$. Then for $1 \le i \le n-2$ and large enough d,

$$A_{p,i}(u_i) \le C(p)^{n-i-1} M p^{-u_i(d_{i+1}-1)/i}.$$

Proof. First note that

$$A_{p,n-1}(u_{n-1}) = \sum_{u_n=2}^{d_n} p^{-(u_n-d_n)(u_n-u_{n-1}/(n-1))}.$$

As a function of u_n, the expression $-(u_n - d_n)(u_n - u_{n-1}/(n-1))$ is at most $(d_n - u_{n-1}/(n-1))^2/4$, so that

$$A_{p,n-1}(u_{n-1}) \le C(p) p^{(d_n - u_{n-1}/(n-1))^2/4}$$

by Lemma 4.2.

The proof of the theorem is by backward induction on i. Note that

$$A_{p,i}(u_i) = \sum_{u_{i+1}} p^{-(u_{i+1}-d_{i+1})(u_{i+1}-u_i/i)} A_{p,i+1}(u_{i+1}).$$

When $i = n-2$, using our bound on $A_{p,n-1}(u_{n-1})$ gives

$$\begin{aligned} & A_{p,n-2}(u_{n-2}) \\ \leq \; & C(p) \sum_{u_{n-1}=1}^{d_{n-1}} p^{-(u_{n-1}-d_{n-1})(u_{n-1}-u_{n-2}/(n-2))+(d_n-u_{n-1}/(n-1))^2/4}. \end{aligned}$$

Now

$$\begin{aligned} & -(u_{n-1}-d_{n-1})(u_{n-1}-u_{n-2}/(n-2)) + (d_n - u_{n-1}/(n-1))^2/4 \\ = \; & -mu_{n-1}^2 + (d_{n-1} + u_{n-2}/(n-2) - d_n/2(n-1))u_{n-1} \\ & \qquad +(d_n^2/4 - d_{n-1}u_{n-2}/(n-2)) \end{aligned} \tag{8}$$

is a function of u_{n-1} maximized at

$$u_{n-1} = (d_{n-1} + u_{n-2}/(n-2) - d_n/2(n-1))/2m. \tag{9}$$

By Corollary 3.2, $d_n \sim d^n/n$ as $d \to \infty$, so that for large enough d, Equation 9 is negative. Thus for $1 \leq u_{n-1} \leq d_{n-1}$, Equation 8 is maximized at $u_{n-1} = 1$. By Lemma 4.2,

$$\begin{aligned} & A_{p,n-2}(u_{n-2}) \\ \leq \; & C(p)C(p^m)p^{-m+d_{n-1}+u_{n-2}/(n-2)-d_n/2(n-1)+d_n^2/4-d_{n-1}u_{n-2}/(n-2)} \\ = \; & C(p)Mp^{-u_{n-2}(d_{n-1}-1)/(n-2)}. \end{aligned}$$

This proves the base case $i = n-2$. By induction, for $i \leq n-3$,

$$\begin{aligned} A_{p,i}(u_i) &= \sum_{u_{i+1}=1}^{d_{i+1}} p^{-(u_{i+1}-d_{i+1})(u_{i+1}-u_i/i)} A_{p,i+1}(u_{i+1}) \\ &\leq C(p)^{n-i-2} M \sum_{u_{i+1}=1}^{d_{i+1}} p^{-(u_{i+1}-d_{i+1})(u_{i+1}-u_i/i)-u_{i+1}(d_{i+2}-1)/(i+1)}. \end{aligned}$$

Now

$$\begin{aligned} & -(u_{i+1}-d_{i+1})(u_{i+1}-u_i/i) - u_{i+1}(d_{i+2}-1)/(i+1) \\ = \; & -u_{i+1}^2 + (d_{i+1} + u_i/i - (d_{i+2}-1)/(i+1))u_{i+1} - d_{i+1}u_i/i, \end{aligned}$$

is a function of u_{i+1} maximized at

$$u_{n-1} = (d_{i+1} + u_i/i - (d_{i+2}-1)/(i+1))/2,$$

which is negative for large d. Thus for $0 \leq u_{i+1} \leq d_{i+1}$, this function is maximized at $u_{i+1} = 0$, and hence is less than $-(d_{i+1} - 1)u_i/i$. Then by Lemma 4.2,

$$A_{p,i}(u_i) \leq C(p)^{n-i-1} M p^{-(d_{i+1}-1)u_i/i},$$

proving the result. □

Lemma 4.5. *Suppose that $\alpha_1, \ldots, \alpha_s$ are positive integers with $n = \alpha_1 + \cdots + \alpha_s$. Then*

$$\alpha_1^2 + \cdots + \alpha_s^2 \leq (n - s + 1)^2 + (s - 1), \tag{10}$$

and this bound is achieved when $\alpha_1 = \alpha_2 = \cdots = \alpha_{s-1} = 1$. Furthermore, if $n \geq 1 + \varepsilon$ and $s \geq 2$, then

$$\varepsilon s + \alpha_1^2 + \cdots + \alpha_s^2 \leq (n - 1)^2 + 1 + 2\varepsilon. \tag{11}$$

Proof. For Equation 10, we use a simple induction argument. It is clearly true for $s = 1$. Suppose it is true up through s; we will prove it for $s + 1$.

$$\begin{aligned} \alpha_1^2 + \cdots + \alpha_s^2 + \alpha_{s+1}^2 &\leq (n - \alpha_{s+1} - s + 1)^2 + (s - 1) + \alpha_{s+1}^2 \\ &\leq (n - s + 1 - \alpha_{s+1})^2 + \alpha_{s+1}^2 + (s - 1) \\ &\leq (n - s + 1 - 1)^2 + 1^2 + (s - 1) \\ &= (n - s)^2 + s, \end{aligned}$$

proving Equation 10. As for Equation 11,

$$\begin{aligned} \varepsilon s + \alpha_1^2 + \cdots + \alpha_s^2 &\leq \varepsilon s + (n - s + 1)^2 + (s - 1) \\ &= ((n - 1) - (s - 2))^2 + s - 1 + \varepsilon s \\ &= (n - 1)^2 - 2(n - 1)(s - 2) + (s - 2)^2 + s - 1 + \varepsilon s \\ &\leq (n - 1)^2 - (\varepsilon + s - 1)(s - 2) + (s - 2)^2 + s - 1 + \varepsilon s \\ &= (n - 1)^2 + 1 + 2\varepsilon, \end{aligned}$$

where the first inequality follows from Equation 10 and the second inequality follows from the fact that since $n \geq 1 + \varepsilon$ and $n \geq s$, we know that $n \geq (\varepsilon + s + 1)/2$. □

5 From Subgroups of F_2/F_{n+1} to Subgroups of F_n/F_{n+1}

The goal of this section is to prove Theorem 1.3, essentially showing that most orbits of $\mathrm{GL}(d, p)$ acting on normal subgroups of F/F_{n+1} contained in F_2/F_{n+1} are orbits of $\mathrm{GL}(d, p)$ acting on normal subgroups of F/F_{n+1} contained in F_n/F_{n+1}. We will prove Theorem 1.3 by estimating the number of normal subgroups of F/F_{n+1} contained in F_2/F_{n+1}. Theorem 5.1 offers an estimate on the number of normal subgroups of an arbitrary p-group that share a particular property. Our estimate depends on certain parameters which are difficult to

work out in general, but are calculated for factors of the Frattini series of a free group in Theorem 5.3. This will give us the tools to prove Theorem 1.3.

Let H be a finite p-group of Frattini length n. Given a normal subgroup U of H, note that by the second isomorphism theorem,

$$(U \cap H_i)/(U \cap H_{i+1}) \cong (U \cap H_i)H_{i+1}/H_{i+1},$$

and this quotient is elementary abelian. Let

$$A_H(\underline{u}) = \{U \lhd H \ : \ \mathrm{rank}((U \cap H_i)H_{i+1}/H_{i+1}) = u_i\},$$

where $\underline{u} = (u_1, \ldots, u_n)$ and the integers u_i satisfy $0 \leq u_i \leq h_i = \mathrm{rank}(H_i/H_{i+1})$ for $1 \leq i \leq n$.

Theorem 5.1. *Suppose that for each $U \in A_H(\underline{u})$,*

$$\begin{aligned} \mathrm{rank}((\Phi(U) \cap H_i)H_{i+1}/H_{i+1}) &\geq v_i \quad \textit{and} \\ \mathrm{rank}((U^p[U,H] \cap H_i)H_{i+1}/H_{i+1}) &\geq w_i. \end{aligned}$$

Then

$$|A_H(\underline{u})| \leq \begin{bmatrix} h_1 \\ u_1 \end{bmatrix}_p \prod_{i=2}^{n} \begin{bmatrix} h_i - w_i \\ u_i - w_i \end{bmatrix}_p p^{(u_1+\cdots+u_{i-1}-v_1-\cdots-v_{i-1})(h_i-u_i)}.$$

Proof. The proof proceeds by induction on n, the Frattini length of H. If $n = 1$, then H is elementary abelian of rank h_1, so that $\underline{u} = (u_1)$ and $A_H(\underline{u}) = \begin{bmatrix} h_1 \\ u_1 \end{bmatrix}_p$.

Now suppose that the result holds in $J = H/H_n$, a group which has Frattini length $n-1$. Any normal subgroup U of H lying in $A_H(\underline{u})$ determines the subgroup $K = U \cap H_n$ of H_n and the normal subgroup $L = UH_n/H_n$ of J. The subgroup K contains $U^p[U,H] \cap H_n$, by hypothesis $\mathrm{rank}(U^p[U,H] \cap H_n) \geq w_n$, and $\mathrm{rank}(K) = \mathrm{rank}(U \cap H_n) = u_n$.

For $1 \leq i \leq n-1$, since $J_i = H_i/H_n$,

$$\begin{aligned} (L \cap J_i)J_{i+1}/J_{i+1} &= (UH_n/H_n \cap H_i/H_n)(H_{i+1}/H_n)/(H_{i+1}/H_n) \\ &\cong (UH_n \cap H_i)H_{i+1}/H_{i+1} \\ &\cong (U \cap H_i)H_{i+1}/H_{i+1}. \end{aligned} \tag{12}$$

Thus $L \in A_J(\underline{t})$, where $\underline{t} = (u_1, \ldots, u_{n-1})$. Furthermore, if M is the inverse image of L in H, then

$$M^p[M,H] = (UH_n)^p[UH_n, H] = U^p[U,H],$$

since $H_{n+1} = H_n^p[H_n, H] = 1$. Thus L determines $U^p[U,H] \cap H_n$.

Given L, the subgroup K is a subspace of H_n of dimension u_n containing $M^p[M,H] \cap H_n$, which has dimension at least w_n. Let $w = \mathrm{rank}(M^p[M,H] \cap H_n)$. Then there are

$$\begin{bmatrix} h_n - w \\ u_n - w \end{bmatrix}_p = \begin{bmatrix} h_n - w \\ h_n - u_n \end{bmatrix}_p$$

choices for K. This Gaussian coefficient is a decreasing function of w, so there are at most

$$\begin{bmatrix} h_n - w_n \\ u_n - w_n \end{bmatrix}_p$$

choices for K. Hence the number of possible pairs K and L given by subgroups in $A_H(\underline{u})$ is at most

$$|A_J(\underline{t})| \cdot \begin{bmatrix} h_n - w_n \\ u_n - w_n \end{bmatrix}_p.$$

There is a bijection between subgroups $U \in A_H(\underline{u})$ that give K and L and complements to H_n/K in M/K, given by $U \mapsto U/K$. In the one direction, U/K is a complement to H_n/K since $U \cap H_n = K$ and $UH_n/K = M/K$. In the other direction, a complement U/K to H_n/K satisfies $U \cap H_n = K$ and $UH_n/K = M/K$, so U gives K and L.

Recall that in general, if G is a group with normal subgroup N, then the number of complements to N in G is either 0 or $|\mathrm{Der}(G/N, N)|$. When N is central, $\mathrm{Der}(G/N, N) = \mathrm{Hom}(G/N, N)$, and if the number of complements is 0, then $\mathrm{Hom}(G/N, N)$ is trivial (see Lubotsky and Segal [13, Lemma 1.3.1]).

Since H_n/K is central in M/K ($H_n \in Z(H)$), the number of complements to H_n/K in M/K is

$$|\mathrm{Hom}(M/H_n, H_n/K)| = |\mathrm{Hom}(L, H_n/K)| = |\mathrm{Hom}(L/\Phi(L), H_n/K)|.$$

The rank of $H_n/K = H_n/(H_n \cap U)$ is $h_n - u_n$. Also,

$$\begin{aligned} & \mathrm{rank}(L/\Phi(L)) \\ = \; & \mathrm{rank}(L) - \mathrm{rank}(\Phi(L)) \\ = \; & \sum_{i=1}^{n-1} \mathrm{rank}((L \cap J_i)J_{i+1}/J_{i+1}) - \sum_{i=1}^{n-1} \mathrm{rank}((\Phi(L) \cap J_i)J_{i+1}/J_{i+1}). \end{aligned}$$

Note that $\Phi(L) = \Phi(U)H_n/H_n$, and a similar calculation to Equation 12 shows that

$$(\Phi(L) \cap J_i)J_{i+1}/J_{i+1} \cong (\Phi(U) \cap H_i)H_{i+1}/H_{i+1},$$

which by hypothesis has rank at least v_i. Thus

$$\mathrm{rank}(L/\Phi(L)) \leq u_1 + \cdots + u_{n-1} - (v_1 + \cdots + v_{n-1})$$

and

$$|\mathrm{Hom}(L/\Phi(L), H_n/K)| \leq p^{(h_n - u_n)(u_1 + \cdots + u_{n-1} - v_1 - \cdots - v_{n-1})}.$$

Using the inductive hypothesis gives

$$\begin{aligned} A_H(\underline{u}) &\leq A_J(\underline{t}) \cdot \begin{bmatrix} h_n - u_n \\ u_n - w_n \end{bmatrix}_p \cdot p^{(h_n - u_n)(u_1 + \cdots + u_{n-1} - v_1 - \cdots - v_{n-1})} \\ &\leq \begin{bmatrix} h_1 \\ u_1 \end{bmatrix}_p \prod_{i=2}^{n} \begin{bmatrix} h_i - w_i \\ u_i - w_i \end{bmatrix}_p p^{(u_1 + \cdots + u_{i-1} - v_1 - \cdots - v_{i-1})(h_i - u_i)}. \end{aligned}$$

□

In Theorem 5.3 and Corollary 5.4, we estimate v_i and w_i when $H = F/F_{n+1}$, using some linear algebra from Lemma 5.2.

Lemma 5.2. *Let*

$$M = A_1 \oplus \cdots \oplus A_{n+1}$$

be a direct sum of vector spaces, let $\phi : M \to M$ be a homomorphism with

$$A_i\phi \subseteq A_{i+1} \oplus \cdots \oplus A_{n+1}$$

for $1 \leq i \leq n$ and $A_{n+1}\phi = 0$, and let N be a subspace of M with $N \cap \ker\phi = 0$. Then $\dim(N + N\phi) \geq (1 + 1/n)\dim N$.

Proof. As $N \cap \ker\phi = 0$, we have $\dim N = \dim N\phi$. The proof is by induction on n. If $n = 1$, then $N\phi \subseteq M\phi \subseteq A_2 \subseteq \ker\phi$, so that $N \cap N\phi = 0$, and $\dim(N + N\phi) = \dim N + \dim N\phi = 2\dim N$.

Now suppose that $n \geq 2$ and let π be the projection of M onto A_1, so that $\ker\pi = A_2 \oplus \cdots \oplus A_{n+1}$ and $N\phi\pi = 0$. Let $Q = N \cap \ker\pi$; then $\dim N = \dim Q + \dim N\pi$. We may assume by induction that

$$\dim(Q + Q\phi) \geq (1 + 1/(n-1))\dim Q.$$

Then

$$\begin{aligned}
\dim(N + N\phi) &= \dim N\pi + \dim((N + N\phi) \cap \ker\pi) \\
&= \dim N\pi + \dim(Q + N\phi) \\
&\geq \dim N\pi + \max\{\dim(Q + Q\phi), \dim N\phi\} \\
&\geq \dim N - \dim Q + \max\{(n/(n-1))\dim Q, \dim N\} \\
&\geq \max\{\dim N + (1/(n-1))\dim Q, 2\dim N - \dim Q\} \\
&\geq (1 + 1/n)\dim N,
\end{aligned}$$

where the two cases to consider are $\dim Q \geq ((n-1)/n)\dim N$ and $\dim Q \leq ((n-1)/n)\dim N$. □

The proof of the next theorem makes heavy use of the definitions and results proved in Section 3.

Theorem 5.3. *Fix an odd prime p. Let U be a normal subgroup of the free group F lying in F_2. Let $n \geq 2$,*

$$\begin{aligned}
Q &= (U \cap F_n)F_{n+1}/F_{n+1}, \\
R &= (\Phi(U) \cap F_{n+1})F_{n+2}/F_{n+2}, \text{ and} \\
S &= (U^p[U, F] \cap F_{n+1})F_{n+2}/F_{n+2}.
\end{aligned}$$

Suppose that these groups have ranks q, r, and s respectively. Then $r \geq q$ and $s \geq (1 + 1/n)q$.

Proof. Replacing U by $U \cap F_n$ leaves Q unchanged and clearly does not increase the ranks of R and S, so we may assume that $U \leq F_n$. Then

$$\begin{aligned} R &= \Phi(U)F_{n+2}/F_{n+2} \\ S &= U^p[U,F]F_{n+2}/F_{n+2}. \end{aligned}$$

Furthermore, replacing U by UF_{n+1} leaves Q unchanged, and

$$\begin{aligned} \Phi(UF_{n+1})F_{n+2}/F_{n+2} &= (UF_{n+1})^p[UF_{n+1}, UF_{n+1}]F_{n+2}/F_{n+2} \\ &= U^p[U, UF_{n+1}]^{F_{n+1}}[F_{n+1}, UF_{n+1}]F_{n+2}/F_{n+2} \\ &= U^p[U, F_{n+1}][U,U]^{F_{n+1}}F_{n+2}/F_{n+2} \\ &= U^p[U,U]F_{n+2}/F_{n+2} \\ &= \Phi(U)F_{n+2}/F_{n+2}. \end{aligned}$$

$$\begin{aligned} (UF_{n+1})^p[UF_{n+1}, F]F_{n+2}/F_{n+2} &= U^p[F_{n+1}, F][U,F]^{F_{n+1}}F_{n+2}/F_{n+2} \\ &= U^p[U,F]F_{n+2}/F_{n+2}. \end{aligned}$$

So we may assume that $F_{n+1} \leq U \leq F_n$. Now $Q \leq F_n/F_{n+1}$ and $Q\phi_n \leq U^pF_{n+2}/F_{n+2} \leq R$. Since ϕ_n is an injection, $r = \mathrm{rank}(R) \geq \mathrm{rank}(Q) = q$ and the first inequality holds.

To prove the second inequality, let $T = Q\alpha_n^{-1}\iota \leq L(n+1)$; note that $\mathrm{rank}(T) = \mathrm{rank}(Q)$ as α_n^{-1} is an injection. Also, $T\rho_{n,k}\alpha_{n+1} \leq [Q, y_k]F_{n+2} \leq S$ by Lemma 3.4. Then, remembering that α_{n+1} is an injection,

$$\begin{aligned} \mathrm{rank}(T\rho_{n,k} + T) &= \mathrm{rank}(Q\alpha_n^{-1}\iota\rho_{n,k} + Q\alpha_n^{-1}\iota) \\ &= \mathrm{rank}(Q\alpha_n^{-1}\iota\rho_{n,k}\alpha_{n+1} + Q\phi_n) \\ &\leq \mathrm{rank}(S). \end{aligned}$$

Suppose first that for some k, $T \cap \ker\rho_{n,k} = 1$. Then we may apply Lemma 5.2, since $T \leq L(n+1)$, $T \cap \ker\rho_{n,k} = 1$, and

$$\begin{aligned} L_i\rho_{n,k} \subseteq L_{i+1} \oplus \cdots \oplus L_{n+1} \quad &\text{for each } 1 \leq i \leq n \\ L_{n+1}\rho_{n,k} &= 1. \end{aligned}$$

We deduce that $s \geq (1 + 1/n)q$.

On the other hand, if $T \cap \ker\rho_{n,k} \neq 1$ for some k, it follows from Lemma 3.4 that $y_k^{p^{n-1}}F_n \in Q$, so $y = (y_k^{p^{n-1}}F_n)\alpha_n^{-1}\iota \in T$. Now pick a complement H to $\langle y\rangle$ in T, and define ρ on T by $\rho|_{\langle y\rangle} = \rho_{n,j}$ and $\phi|_H = \rho_{n,k}$, where $j \neq k$. Then $T \cap \ker\rho = 1$, $L_i\rho \subseteq L_{i+1} \oplus \cdots \oplus L_{n+1}$ for each $1 \leq i \leq n$, and $L_{n+1}\rho = 1$, so that we deduce again from Lemma 5.2 that $s \geq (1 + 1/n)q$. □

Corollary 5.4. *Fix an odd prime p. Let U be a normal subgroup of F/F_n lying in F_2/F_n. Let $i \geq 2$,*

$$\begin{aligned} Q &= (U \cap F_i/F_n)(F_{i+1}/F_n)/(F_{i+1}/F_n), \\ R &= (\Phi(U) \cap F_{i+1}/F_n)(F_{i+2}/F_n)/(F_{i+2}/F_n), \text{ and} \\ S &= (U^p[U, F/F_n] \cap F_{i+1}/F_n)(F_{i+2}/F_n)/(F_{i+2}/F_n). \end{aligned}$$

Then $\operatorname{rank}(R) \geq \operatorname{rank}(Q)$ *and* $\operatorname{rank}(S) \geq (1+1/i)\operatorname{rank}(Q)$.

We can now prove Theorem 1.3, restated here for convenience.

Theorem 1.3. *Fix an odd prime* p. *Let* $n \geq 3$ *and* $w = d_{n-1} - d_n/2(n-1) + d^2$. *Then*

$$1 \leq \frac{|\mathfrak{A}_{d,n}|}{|\mathfrak{C}_{d,n}|} \leq 1 + O(p^w),$$

where w *is viewed as a function of* d.

Proof. To prove this result, we need to apply the estimates of Theorems 4.1 and 4.4 to the upper bound for $A_H(\underline{u})$ obtained in Theorem 5.1 in the case when $H = F/F_{n+1}$. By Corollary 5.4, we may choose $v_{i+1} = u_i$ and $w_{i+1} \in \mathbb{Z}$ with

$$1 > w_{i+1} - u_i(1+1/i) \geq 0,$$

so that in particular, $w_{i+1} = 0$ if $u_i = 0$. By Equation 1 of Theorem 4.1, we have

$$\begin{bmatrix} n \\ k \end{bmatrix}_p \leq D(p)p^{k(n-k)}.$$

Substituting in the bound obtained in Theorem 5.1, we find that, if $u_1 = 0$, then

$$|A_H(\underline{u})| \leq D(p)^{n-1}p^h,$$

where

$$\begin{aligned} h &= u_2(d_2-u_2) + (u_3-w_3)(d_3-u_3) + \cdots + (u_n-w_n)(d_n-u_n) \\ &\qquad + u_2(d_3-u_3) + \cdots + u_{n-1}(d_n-u_n) \\ &\leq -(u_2-d_2)u_2 - (u_3-d_3)(u_3-u_2/2) - \cdots \\ &\qquad - (u_n-d_n)(u_n-u_{n-1}/(n-1)). \end{aligned}$$

Hence

$$|\mathcal{A}_{d,n}| \leq |\mathcal{C}_{d,n}| + \sum_{\underline{u}} D(p)^{n-1}p^h = |\mathcal{C}_{d,n}| + D(p)^{n-1}\sum_{\underline{u}} p^h,$$

where the sum is taken over all $\underline{u}$ such that $U \in A_H(\underline{u})$ if and only if $U \leq F_2/F_{n+1}$ and $U \not\leq F_n/F_{n+1}$. In terms of $\underline{u}$, this means that $u_{n-1} \geq 1$ and $u_1 = 0$. By Theorem 5.4, $u_n \geq w_n > u_{n-1}$, so $u_n \geq 2$. Then by Theorem 4.4, we have

$$|\mathcal{A}_{d,n}| \leq |\mathcal{C}_{d,n}| + D(p)^{n-1}C(p)^{n-2}C(p^m)p^y,$$

where

$$y = 1/4(n-1)^2 - 1 + d_n^2/4 + d_{n-1} - d_n/2(n-1)$$

and hence, as $|\mathcal{C}_{d,n}| = \mathcal{G}_{d_n}(p)$, we have by Theorem 4.1, that

$$\begin{aligned} |\mathcal{A}_{d,n}|/|\mathcal{C}_{d,n}| &\leq 1 + D(p)^{n-1}C(p)^{n-1}p^y/\mathcal{G}_{d_n}(p) \\ &= 1 + O(p^{d_{n-1}-d_n/2(n-1)}). \end{aligned}$$

Now by Theorems 2.7 and 2.8, $|\mathfrak{A}_{d,n}|$ and $|\mathfrak{C}_{d,n}|$ are the number of $\mathrm{GL}(d,p)$-orbits on $\mathcal{A}_{d,n}$ and $\mathcal{C}_{d,n}$ respectively. Hence

$$0 \leq |\mathfrak{A}_{d,n}| - |\mathfrak{C}_{d,n}| \leq |\mathcal{A}_{d,n}| - |\mathcal{C}_{d,n}|,$$

since $|\mathfrak{A}_{d,n}| - |\mathfrak{C}_{d,n}|$ is the number of $\mathrm{GL}(d,p)$ orbits on $\mathcal{A}_{d,n} \setminus \mathcal{C}_{d,n}$. Also $|\mathcal{C}_{d,n}| \leq |\mathfrak{C}_{d,n}| \cdot |\mathrm{GL}(d,p)|$, since $\mathcal{C}_{d,n}$ falls into $|\mathfrak{C}_{d,n}|$ orbits, each of size at most $|\mathrm{GL}(d,p)|$. Then

$$\begin{aligned} 0 &\leq \frac{|\mathfrak{A}_{d,n}|}{|\mathfrak{C}_{d,n}|} - 1 \\ &= \frac{|\mathcal{C}_{d,n}|}{|\mathfrak{C}_{d,n}|} \left(\frac{|\mathfrak{A}_{d,n}| - |\mathfrak{C}_{d,n}|}{|\mathcal{C}_{d,n}|} \right) \\ &\leq |\mathrm{GL}(d,p)| \left(\frac{|\mathcal{A}_{d,n}| - |\mathcal{C}_{d,n}|}{|\mathcal{C}_{d,n}|} \right) \\ &= O(p^{d_{n-1} - d_n/2(n-1)+d^2}). \end{aligned}$$

Therefore

$$1 \leq \frac{|\mathfrak{A}_{d,n}|}{|\mathfrak{C}_{d,n}|} \leq 1 + O(p^w).$$

□

6 Most Orbits on Subgroups of F_n/F_{n+1} are Regular

In this section we shall prove Theorem 1.4. This depends on estimating $|\mathfrak{C}_{d,n}|$, the number of $|\mathrm{GL}(d,p)|$-orbits on subspaces of F_n/F_{n+1}, via the Cauchy-Frobenius Lemma. To do this, we obtain in Theorem 6.2 an upper bound for the number of subspaces of F_n/F_{n+1} normalized by an element of $\mathrm{GL}(d,p)$, and refine this in Theorem 6.3 to obtain a stronger bound in the case $n = 2$.

Let $\Sigma = \mathrm{GL}(d,p)$ and K be the finite field of p elements. Suppose V is a $K\Sigma$-module, and let $g \in \Sigma$. We want to count the number of subspaces of V (viewed as a K-vector space) normalized by g, which is the number of submodules of V as a $K\langle g \rangle$-module. The following preliminaries are based on Macdonald [15, Chapter IV, Section 2].

Let Φ be the set of all polynomials in $K[t]$ which are irreducible over K and P the set of all partitions of non-negative integers. Let U be the set of all functions $\mu : \Phi \to P$ such that $n = \sum_{f \in \Phi} \deg(f)|\mu(f)|$, where $|\mu(f)|$ is the sum of the parts of the partition $\mu(f)$. Then there is a one-to-one correspondence between $K\langle g \rangle$-modules V of dimension n and functions $\mu \in U$. This correspondence is given by

$$V \cong \oplus_{f \in \Phi} \oplus_i \frac{K[t]}{(f)^{\mu_i(f)}},$$

where $\mu_i(f)$ is the i-th part of $\mu(f)$, (f) is the ideal of $K[t]$ generated by f, and g acts upon $K[t]/(f)^s$ as multiplication by t. For convenience, let $V_f =$

$\oplus_i K[t]/(f)^{\mu_i(f)}$; then we call $\mu(f)$ the type of V_f. Any submodule W of V can be written $W = \oplus_{f\in\Phi} W_f$ with $W_f \subseteq V_f$ for each $f \in \Phi$. That is, every submodule of V is the direct sum of submodules of the summands V_f. By Macdonald [15, Chapter II, 3.1] the type λ of any $K\langle g\rangle$-submodule or quotient module of V_f satisfies $\lambda \subseteq \mu(f)$.

For each $f \in \Phi$, let $K[t]_f$ denote the localization of $K[t]$ at the prime ideal (f). Then $K[t]_f$ is a discrete valuation ring with residue field of order $q = p^{\deg(f)}$ and V_f is a finite $K[t]_f$-module of type $\mu(f)$.

Both Theorems 6.2 and 6.3 depend on Theorem 6.1, where we calculate the number of submodules of fixed type in a module of fixed type over a discrete valuation ring. This is a generalization of the result of Miller [18] on the number of subgroups of an abelian p-group.

Theorem 6.1. *Let $\mathfrak{a}$ be a discrete valuation ring with maximal ideal $\mathfrak{p}$ and let $\mathfrak{k} = \mathfrak{a}/\mathfrak{p}$ be the residue field of order q. Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_s)$ and $\beta = (\beta_1, \beta_2, \ldots, \beta_r)$ be partitions with $\beta \subseteq \alpha$ and let M be a finite $\mathfrak{a}$-module of type α'. Then the number of submodules of M of type β' is*

$$A(\alpha', \beta', q) = \prod_{i=1}^{r} \begin{bmatrix} \alpha_i - \beta_{i+1} \\ \beta_i - \beta_{i+1} \end{bmatrix}_q q^{\beta_{i+1}(\alpha_i - \beta_i)}.$$

Proof. The proof is by induction on β_1. If $\beta_1 = 0$, then $A(\alpha', \beta', q) = 1$ and the result holds. Suppose $\beta_1 > 0$, and let the smallest part of β' be t, so that either $\beta_1 = \cdots = \beta_t > \beta_{t+1}$ and $t < s$, or $\beta_1 = \cdots = \beta_s$ and $t = s$. Write

$$\overline{\beta} = (\beta_1 - 1, \beta_2 - 1, \ldots, \beta_t - 1, \beta_{t+1}, \ldots).$$

Let N be any submodule of M of type $\overline{\beta}'$ and x any element of M with $\mathfrak{p}^t x = 0$, $\mathfrak{p}^{t-1} x \neq 0$, and $\mathfrak{p}x \cap N = 0$. Then $\langle N, x\rangle$ has type β'. There are $A(\alpha', \overline{\beta}', q)$ choices for N, and for each N it follows from [15, Chapter II, Equation 1.8] that the number of choices for x is just

$$q^{\alpha_1 + \cdots + \alpha_t}(1 - q^{\beta_t - \alpha_t - 1}). \tag{13}$$

On the other hand, fix a submodule L of M of type β'; we can count the number of choices of N and x so that $L = \langle N, x\rangle$. Here N is a submodule of L of type $\overline{\beta}'$ whose quotient has type (t), and by [15, Chapter II, Equation 4.13], the number of choices for N is

$$\frac{1 - q^{\beta_{t+1} - \beta_t}}{1 - q^{-1}} q^{\sum_i \binom{\beta_i}{2} - \sum_i \binom{\overline{\beta}_i}{2}} = \frac{1 - q^{\beta_{t+1} - \beta_t}}{1 - q^{-1}} q^{t(\beta_t - 1)}.$$

Given N, it follows from [15, Chapter II, Equation 1.8] that there are

$$q^{\beta_1 + \cdots + \beta_t}(1 - q^{-1})$$

choices for x. Thus any submodule L of M of type β' arises as $\langle N, x\rangle$ in

$$q^{\beta_1 + \cdots + \beta_t + t(\beta_t - 1)}(1 - q^{\beta_{t+1} - \beta_t})$$

ways. The total number of submodules L of M of type β' is then

$$\begin{aligned} A(\alpha',\beta',q) &= \frac{A(\alpha',\overline{\beta}',q)q^{\alpha_1+\cdots+\alpha_t}(1-q^{\beta_t-\alpha_t-1})}{q^{\beta_1+\cdots+\beta_t+t(\beta_t-1)}(1-q^{\beta_{t+1}-\beta_t})} \\ &= \frac{A(\alpha',\overline{\beta}',q)q^{\alpha_1+\cdots+\alpha_t}(1-q^{\beta_t-\alpha_t-1})}{q^{2t\beta_t-t}(1-q^{\beta_{t+1}-\beta_t})}, \end{aligned} \tag{14}$$

where the second inequality uses $\beta_1 = \cdots = \beta_t$. By induction, we know that

$$\begin{aligned} A(\alpha',\overline{\beta}',q) &= \prod_{i=1}^{r} \begin{bmatrix} \alpha_i - \overline{\beta}_{i+1} \\ \overline{\beta}_i - \overline{\beta}_{i+1} \end{bmatrix}_q q^{\overline{\beta}_{i+1}(\alpha_i-\overline{\beta}_i)} \\ &= \prod_{i=1}^{t-1} \begin{bmatrix} \alpha_i - \beta_{i+1}+1 \\ \beta_i - \beta_{i+1} \end{bmatrix}_q q^{(\beta_{i+1}-1)(\alpha_i-\beta_i+1)} \\ &\qquad \cdot \begin{bmatrix} \alpha_t - \beta_{t+1} \\ \beta_t - \beta_{t+1}-1 \end{bmatrix}_q q^{\beta_{t+1}(\alpha_t-\beta_t+1)} \\ &\qquad \cdot \prod_{i=t+1}^{r} \begin{bmatrix} \alpha_i - \beta_{i+1} \\ \beta_i - \beta_{i+1} \end{bmatrix}_q q^{\beta_{i+1}(\alpha_i-\beta_i)} \\ &= \prod_{i=1}^{r} \begin{bmatrix} \alpha_i - \beta_{i+1} \\ \beta_i - \beta_{i+1} \end{bmatrix}_q q^{\beta_{i+1}(\alpha_i-\beta_i)} \\ &\qquad \cdot \prod_{i=1}^{t-1} \frac{q^{\alpha_i-\beta_{i+1}+1}-1}{q^{\alpha_i-\beta_i+1}-1} q^{\beta_{i+1}+\beta_i-\alpha_i-1} \cdot \frac{q^{\beta_t-\beta_{t+1}}-1}{q^{\alpha_t-\beta_t+1}-1} q^{\beta_{t+1}} \\ &= \prod_{i=1}^{r} \begin{bmatrix} \alpha_i - \beta_{i+1} \\ \beta_i - \beta_{i+1} \end{bmatrix}_q q^{\beta_{i+1}(\alpha_i-\beta_i)} \\ &\qquad \cdot q^{2(t-1)\beta_t-\alpha_1-\cdots-\alpha_{t-1}-(t-1)} \cdot \frac{q^{\beta_t-\beta_{t+1}}-1}{q^{\alpha_t-\beta_t+1}-1} q^{\beta_{t+1}} \\ &= \prod_{i=1}^{r} \begin{bmatrix} \alpha_i - \beta_{i+1} \\ \beta_i - \beta_{i+1} \end{bmatrix}_q q^{\beta_{i+1}(\alpha_i-\beta_i)} \cdot \frac{q^{2t\beta_t}}{q^{\alpha_1+\cdots+\alpha_t+t}} \cdot \frac{1-q^{\beta_{t+1}-\beta_t}}{1-q^{\beta_t-\alpha_t-1}}. \end{aligned}$$

Subbing into Equation 14 gives the result. □

Using Theorem 6.1 and the techniques of Section 4, we can now upper bound the total number of submodules of a finite $K\langle g\rangle$-module V. It is clear that every subspace of V is a $K\langle g\rangle$-module if and only if g acts as a scalar on V, that is as multiplication by an element of K. Apart from this case, it turns out that the largest number of subspaces occurs when g acts as a scalar on a hyperplane U in V and as a different scalar on a complement to U.

Theorem 6.2. *Let $g \in \Sigma$ and V be a $K\langle g\rangle$-module of dimension n over K. Let m_V be the number of submodules of V. Then either*

1. *g acts as a scalar on V and $m_V = \mathcal{G}_n(p)$, or*

2. g does not act as a scalar and

$$\log_p m_V \leq 2\varepsilon + (n^2 - 2n + 2)/4$$

for $n \geq 2 + \varepsilon$, where $\varepsilon = \log_p(C(p)D(p))$.

Proof. Write $V = \oplus_{i=1}^m V_i$ where for each i, $V_i = V_{f_i}$ for some $f_i \in \Phi$ and $\dim_K V_i = n_i$. If $m \geq 2$, then since each submodule of V is a sum of submodules of the modules V_i, $m_V = \prod_{i=1}^m m_{V_i} \leq \mathcal{G}_{n_1}(p)\mathcal{G}_{n-n_1}(p)$, so that by Lemma 4.3,

$$m_V \leq C(p)^2 D(p)^2 p^{n_1^2/4 + (n-n_1)^2/4} \leq C(p)^2 D(p)^2 p^{(n^2-2n+2)/4},$$

since $0 < n_1 < n$.

On the other hand, if $m = 1$, then $V = V_f$ for some $f \in \Phi$. Let $u = \deg(f)$ and $q = p^u$, and let V have type α' as a $K[t]_f$-module, where $\alpha = (\alpha_1, \ldots, \alpha_s)$. First suppose that α has at least two parts. If $\beta = (\beta_1, \ldots, \beta_r)$ and $\beta \subseteq \alpha$, then by Theorem 6.1 and Lemma 4.1 Equation 1, the number of submodules of V of type β' is

$$\begin{aligned} A(\alpha', \beta', q) &\leq \prod_{i=1}^r D(q) q^{(\beta_i - \beta_{i+1})(\alpha_i - \beta_i) + \beta_{i+1}(\alpha_i - \beta_i)} \\ &= D(q)^r \prod_{i=1}^r q^{\beta_i(\alpha_i - \beta_i)}. \end{aligned}$$

Thus

$$\begin{aligned} m_V &= \sum_{\beta' \subseteq \alpha'} A(\alpha', \beta', q) \\ &\leq D(q)^s \sum_{\beta' \subseteq \alpha'} \prod_{i=1}^r q^{\beta_i(\alpha_i - \beta_i)} \\ &\leq D(q)^s \prod_{i=1}^s \sum_{u=0}^{\alpha_i} q^{u(\alpha_i - u)} \\ &\leq D(q)^s C(q)^s \prod_{i=1}^s q^{\alpha_i^2/4}, \end{aligned}$$

where the last inequality follows from Theorem 4.2. Now $D(q) \leq D(p)$ and $C(q) \leq C(p)$ so, remembering that $u(\alpha_1 + \cdots + \alpha_s) = n$ and using Lemma 4.5,

$$\begin{aligned} \log_p m_V &\leq s\varepsilon + u(\alpha_1^2 + \cdots + \alpha_s^2)/4 \\ &\leq s\varepsilon + ((u\alpha_1)^2 + \cdots + (u\alpha_s)^2)/4 \\ &\leq 2\varepsilon + (n/2 - 1)^2 + 1 \\ &\leq 2\varepsilon + (n^2 - 2n + 2)/4, \end{aligned} \tag{15}$$

if $n \geq 2 + 2\varepsilon$.

If instead $s = 1$ and α has just one part, then $\alpha_1 = n/u$. If $u \geq 2$, then by Lemma 4.1 Equation 1,

$$\begin{aligned} m_V &= \sum_{0 \leq \beta_1 \leq \alpha_1} \begin{bmatrix} \alpha_1 \\ \beta_1 \end{bmatrix}_q \\ &\leq C(q)D(q)q^{n^2/4u^2} \\ &\leq C(p)^2 D(p)^2 p^{n^2/4u} \\ &\leq C(p)^2 D(p)^2 p^{(n^2-2n+2)/4}, \end{aligned}$$

since $u \geq 2$. On the other hand, if $u = 1$, then $f = t - k$ for some $k \in K$ and $V \cong \oplus^n \{K[t]/(f)\}$ so that g acts as the scalar k on V and $m_V = \mathcal{G}_n(p)$. □

The next theorem strengthens this result when the module structure is known more precisely and will be needed to deal with groups of Frattini length 2.

Theorem 6.3. *Let $1 \neq g \in \Sigma$ and let V be a non-trivial $K\langle g \rangle$-module of dimension n over K. Suppose that W is a $K\langle g \rangle$-module extension of $V \wedge V$ by V and let m_W be the number of submodules of W. Then*

$$\log_p m_W \leq \theta + (N-4)^2/4$$

for $n \geq 10$, where $N = n(n+1)/2$, $\varepsilon = \log_p(C(p)D(p))$, and $\theta = \max\{3\varepsilon + 4, 4\varepsilon + 5/2, 5\varepsilon + 1\}$.

Proof. Write $W = \oplus_{i=1}^m W_i$, where for each i, $W_i = W_{f_i}$ for some $f_i \in \Phi$ and $\dim_K W_i = n_i$; we may assume that $n_1 \geq n_2 \geq \cdots \geq n_m$. Note that $n_1 + \cdots + n_m = N$. Then $V = \oplus_{i=1}^m W_i \pi$ where π is the projection from W onto V.

Fix $0 < t < m$ and set $X = W_1 \oplus \cdots \oplus W_t$. Also let $x = \dim X = n_1 + \cdots + n_t$. Then $m_W \leq \mathcal{G}_x(p)\mathcal{G}_{N-x}(p)$ since any submodule of W is a direct sum of submodules of the W_i. By Lemma 4.3,

$$m_W \leq C(p)^2 D(p)^2 p^{x^2/4 + (N-x)^2/4}.$$

When $4 \leq x \leq N-4$, it follows that

$$\begin{aligned} m_W &\leq C(p)^2 D(p)^2 p^{4 + (N-4)^2/4} \text{ and} \\ \log_p m_W &\leq 2\varepsilon + 4 + (N-4)^2/4, \end{aligned}$$

proving the result. If we cannot choose t so that $4 \leq x \leq N-4$, then since $N > 9$ implies that $n_1 \not\leq 3$, it must be that $n_1 \geq N-3$ and $m \leq 4$. Write $Y = W_2 \oplus \cdots \oplus W_m$; then $y = \dim Y \leq 3$. At this point we need to prove a technical claim which we will use twice.

Claim: Suppose that V is the direct sum of $K\langle g \rangle$-modules A and B of dimensions $a \geq 4$ and $n - a$ over K, with $A \subset W_1 \pi$. If g acts as a scalar k on A, then $k = 1$ and $A \otimes B$ is the direct sum of a copies of B.

Proof of claim: If $V = A \oplus B$, then $V \wedge V \cong (A \wedge A) \oplus (B \wedge B) \oplus (A \otimes B)$. If g acts as a scalar k on A, then $A \cong \oplus\{K[t]/(t-k)\}^a$ and $W_1 = W_{(t-k)}$. In this case g acts as the scalar k^2 on $A \wedge A$, so $A \wedge A \cong \{K[t]/(t-k^2)\}^{a(a-1)/2}$. Then $A \wedge A \not\subseteq W_1$ and hence $A \wedge A \subseteq Y$. But then $a(a-1)/2 = \dim(A \wedge A) \leq \dim Y \leq 3$, which is impossible. Therefore $k = 1$. Since V is non-trivial, the action on B is non-trivial and $A \otimes B$ is the direct sum of a copies of B.

Now take $A = W_1\pi$ and $B = Y\pi$ so that $V = A \oplus B$. Suppose that g acts on A as a scalar k. Since $n \geq 7$ and $\dim B \leq \dim Y \leq 3$, we see that $a \geq 4$, and by the claim, $A \otimes B$ is the direct sum of a copies of B. But since B is the image of Y, it follows that $A \otimes B \subseteq Y$, and $a(n-a) \leq \dim Y \leq 3$, which is false. Therefore g does not act on $W_1\pi$ as a scalar, and hence does not act on W_1 as a scalar.

We may assume that $W_1 = W_f$ where f has degree u over K and W_1 and $W_1\pi$ have types α' and β' respectively, where $\beta \subseteq \alpha$. Write $\alpha = (\alpha_1, \ldots, \alpha_s)$ and $\beta = (\beta_1, \ldots, \beta_r)$. If $u > 1$, then

$$\begin{aligned} m_{W_1} &\leq \mathcal{G}_{n_1/u}(q) \\ &\leq C(q)D(q)q^{n_1^2/4u^2} \\ &\leq C(p)D(p)p^{n_1^2/4u} \\ &\leq C(p)D(p)p^{n_1^2/8}. \end{aligned}$$

Then

$$\begin{aligned} m_W &\leq m_{W_1}\mathcal{G}_y(p) \\ &\leq C(p)^2D(p)^2p^{n_1^2/8+y^2/4} \\ &\leq C(p)^2D(p)^2p^{N^2/8+9/4} \\ &\leq C(p)^2D(p)^2p^{(N-4)^2/4+9/4}, \end{aligned}$$

where the last line uses the fact that $N \geq 14$. Thus $\log_p m_W \leq \theta + (N-4)^2/4$. So we may assume that $u = 1$ and $f = t - k$ for some $k \in K$. Since g does not act as a scalar on W_1 or $W_1\pi$, $\alpha_2 \geq \gamma_2 > 0$.

By Equation 15,

$$\log_p m_{W_1} \leq s\varepsilon + (\alpha_1^2 + \cdots + \alpha_s^2)/4,$$

so

$$\log_p m_W \leq \log_p m_{W_1} + \log_p \mathcal{G}_y(p) \leq (s+1)\varepsilon + (\alpha_1^2 + \cdots + \alpha_s^2 + y^2)/4.$$

Suppose that $\alpha_1 \leq N - 4$. If $s = 2$, then

$$\begin{aligned} \log_p m_W &\leq 3\varepsilon + (\alpha_1^2 + \alpha_2^2 + y^2)/4 \\ &\leq 3\varepsilon + ((N-4)^2 + 4^2 + 0^2)/4 \\ &\leq \theta + (N-4)^2/4. \end{aligned}$$

If $s = 3$, then

$$\begin{aligned} \log_p m_W &\leq 4\varepsilon + (\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + y^2)/4 \\ &\leq 4\varepsilon + ((N-4)^2 + 3^2 + 1^2 + 0^2)/4 \\ &\leq \theta + (N-4)^2/4. \end{aligned}$$

Finally, if $4 \leq s \leq N$, then by Lemma 4.5, we get

$$\log_p m_W \leq (s+1)\varepsilon + ((N-s)^2 + s)/4.$$

This is maximized at $s = 4$, where we get a bound of $5\varepsilon + 1 + (N-4)^2/4$.

So we may assume that $\alpha_1 \geq N - 3$. Then $\alpha_2 + \cdots + \alpha_s + y \leq 3$. Since $\beta_1 + \cdots + \beta_r + \dim(\pi Y) = n \geq 10$, it follows that $\beta_1 \geq 7$ and $\beta_1 - \beta_2 \geq 4$. Note that $\beta_1 - \beta_2$ is the number of summands of $W_1\pi$ that are isomorphic to $K[t]/(f-k)$. So write $W_1\pi = A \oplus C$, where $a = \dim A = \beta_1 - \beta_2$ and g acts as the scalar k on A and not on C. Set $B = C \oplus Y\pi$. Then $V = A \oplus B$ and by the claim, $k = 1$ and $A \otimes B$ is a direct sum of a copies of B. Then $A \otimes B$ is contained in Y plus the components of W_1 that g does not act as a scalar on, so that $a\beta_2 \leq \dim(A \otimes B) \leq \alpha_2 + y \leq 3$, which is impossible. □

We can now prove Theorem 1.4, restated here for convenience.

Theorem 1.4. *Fix a prime p. Let*

$$x = \begin{cases} -d & : \quad n = 2 \\ d^2 - d_n/2 & : \quad n \geq 3. \end{cases}$$

Then, viewing x as a function of d,

(a)
$$1 \leq \frac{|\mathfrak{C}_{d,n}| \cdot |\mathrm{GL}(d,p)|}{|\mathcal{C}_{d,n}|} \leq 1 + O(p^x).$$

(b)
$$1 \leq \frac{|\mathfrak{C}_{d,n}|}{|\mathfrak{D}_{d,n}|} \leq 1 + O(p^x).$$

Proof. Recall that $\mathfrak{C}_{d,n}$ are the $\mathrm{GL}(d,p)$-orbits in $\mathcal{C}_{d,n}$, $\mathfrak{D}_{d,n}$ are the regular orbits in $\mathfrak{C}_{d,n}$, and $|\mathcal{C}_{d,n}| = \mathcal{G}_{d_n}(p)$. If $g \in \Sigma$, then $|(\mathcal{C}_{d,n})^g|$, the number of elements of $\mathcal{C}_{d,n}$ fixed by g, is just the number of submodules of F_n/F_{n+1} viewed as a $K\langle g \rangle$-module, which we estimated in the previous theorems.

We explain first why only the identity element of Σ can act as a scalar on F_n/F_{n+1}. By Theorem 3.1, F_n/F_{n+1} has a $K\Sigma$-submodule $(L_1 \oplus L_2)\alpha_n$ which is $K\Sigma$-isomorphic to $V \oplus (V \wedge V)$, where V is the natural $K\Sigma$-module. If $g \in \Sigma$ acts on F_n/F_{n+1} as a scalar $k \in K$, then it acts on V as the scalar k, and hence on $V \wedge V$ as the scalar k^2. Thus $k = k^2$ and $k = 1$, so that g is the identity on V, that is the identity of Σ.

Suppose first that $n > 2$. We know from Theorem 6.2 that if $g \neq 1$, $|(\mathcal{C}_{d,n})^g| \leq C(p)^2 D(p)^2 p^u$, where $u = (d_n^2 - 2d_n + 2)/4$. By the Cauchy-Frobenius counting lemma,

$$\begin{aligned} |\mathrm{GL}(d,p)| \cdot |\mathfrak{C}_{d,n}| &= \sum_{g \in \mathrm{GL}(d,p)} |(\mathcal{C}_{d,n})^g| \\ &= |\mathcal{C}_{d,n}| + \sum_{g \neq 1} |(\mathcal{C}_{d,n})^g| \\ &\leq |\mathcal{C}_{d,n}| + (|\mathrm{GL}(d,p)| - 1) C(p)^2 D(p)^2 p^u. \end{aligned}$$

By Lemma 4.1, for large enough d,

$$|\mathcal{C}_{d,n}| \geq (1/2) C'(p) D(p) p^{d_n^2/4} (1 - O(p^{-d_n/2})),$$

and $|\mathrm{GL}(d,p)| \leq p^{d^2}$, so

$$\begin{aligned} 1 &\leq \frac{|\mathrm{GL}(d,p)| \cdot |\mathfrak{C}_{d,n}|}{|\mathcal{C}_{d,n}|} \\ &\leq 1 + \frac{2C(p)^2 D(p)}{C'(p)} \, p^{u + d^2 - d_n^2/4} (1 + O(p^{-d_n/2})) \\ &= 1 + \frac{2C(p)^2 D(p)}{C'(p)} \, p^{d^2 - d_n/2 + 1/2} (1 + O(p^{-d_n/2})) \\ &= 1 + O(p^{d^2 - d_n/2}). \end{aligned}$$

If $n = 2$, then F_2/F_3 is an extension of $V \wedge V$ by V, and using the estimates of Lemma 6.3 and the argument above we obtain

$$\begin{aligned} 1 &\leq \frac{|\mathrm{GL}(d,p)| \cdot |\mathfrak{C}_{d,n}|}{|\mathcal{C}_{d,n}|} \\ &\leq 1 + \frac{2}{C'(p) D(p)} \, p^{\theta + (d_2 - 4)^2/4 - d_2^2/4 + d^2} (1 + O(p^{-d_2/2})) \\ &= 1 + \frac{2}{C'(p) D(p)} \, p^{\theta + 4 - d} (1 + O(p^{-d_2/2})) \\ &= 1 + O(p^{-d}). \end{aligned}$$

To prove part (b), we observe that $|\mathcal{C}_{d,n}| = \sum |\mathrm{GL}(d,p)| / |\mathrm{GL}(d,p)_{(w)}|$, where the sum is over all $\mathrm{GL}(d,p)$-orbits on $\mathcal{C}_{d,n}$ and $|\mathrm{GL}(d,p)_{(w)}|$ is the order of the stabilizer in $\mathrm{GL}(d,p)$ of a typical element w of the orbit under consideration. Now $|\mathfrak{D}_{d,n}|$ is just the number of orbits for which $|\mathrm{GL}(d,p)_{(w)}| = 1$, so

$$|\mathcal{C}_{d,n}| \leq |\mathrm{GL}(d,p)| \cdot |\mathfrak{D}_{d,n}| + |\mathrm{GL}(d,p)| (|\mathfrak{C}_{d,n}| - |\mathfrak{D}_{d,n}|)/2.$$

That is,

$$(2/|\mathrm{GL}(d,p)|) |\mathcal{C}_{d,n}| - |\mathfrak{C}_{d,n}| \leq |\mathfrak{D}_{d,n}|,$$

so that

$$\begin{aligned}\frac{|\mathfrak{D}_{d,n}|}{|\mathfrak{C}_{d,n}|} &\geq \frac{2|\mathcal{C}_{d,n}|/|\mathrm{GL}(d,p)| - |\mathfrak{C}_{d,n}|}{|\mathfrak{C}_{d,n}|} \\ &\geq \frac{2|\mathcal{C}_{d,n}|}{|\mathrm{GL}(d,p)| \cdot |\mathfrak{C}_{d,n}|} - 1 \\ &\geq 2(1 - O(p^x)) - 1 \\ &= 1 - O(p^x).\end{aligned}$$

Since $x \to -\infty$ as $d \to \infty$, the result follows. □

7 Summary

In this section we use Theorems 1.2, 1.3, and 1.4 to prove a slightly more general version of Theorem 1.1, obtaining it as a corollary.

Theorem 7.1. *Fix an odd prime p and $n \geq 2$. If $s_{d,n}$ is the proportion of p-groups generated by d elements and with Frattini length at most n whose automorphism group is a p-group, then* $\lim_{d\to\infty} s_{d,n} = 1$.

Proof. The set of p-groups generated by d elements and with Frattini length at most n is $\mathfrak{A}_{d,n}$. When $n = 2$, $\mathfrak{A}_{d,n} = \mathfrak{C}_{d,n}$. When $n \geq 3$, $d_{n-1} - d_n/2(n-1) + d^2 \sim d^n/2n^2$ as $d \to \infty$. Thus by Theorem 1.3, for all $n \geq 2$,

$$\lim_{d\to\infty} \frac{|\mathfrak{A}_{d,n}|}{|\mathfrak{C}_{d,n}|} = 1.$$

The set $\mathfrak{D}_{d,n} \subseteq \mathfrak{C}_{d,n}$ is contained in the subset of $\mathfrak{A}_{d,n}$ of p-groups with automorphism group a p-group. By Theorem 1.4(b),

$$\lim_{d\to\infty} \frac{|\mathfrak{C}_{d,n}|}{|\mathfrak{D}_{d,n}|} = 1.$$

It follows that

$$\lim_{d\to\infty} \frac{|\mathfrak{A}_{d,n}|}{|\mathfrak{D}_{d,n}|} = 1,$$

and hence that $\lim_{d\to\infty} s_{d,n} = 1$. □

Corollary 7.2 (Theorem 1.1). *Fix an odd prime p and $n \geq 2$. If $r_{d,n}$ is the proportion of p-groups generated by at most d elements and with Frattini length at most n whose automorphism group is a p-group, then* $\lim_{d\to\infty} r_{d,n} = 1$.

Proof. This follows directly from Theorem 7.1 and the trivial observation that the number of p-groups generated by at most d elements and with Frattini length at most n is finite, while the number of p-groups with Frattini length at most n is infinite. □

Corollary 7.3. *Fix an odd prime p and $n \geq 2$. If $t_{d,n}$ is the proportion of p-groups generated by d elements and with Frattini length n whose automorphism group is a p-group, then* $\lim_{d\to\infty} t_{d,n} = 1$.

Proof. As $\mathfrak{D}_{d,n} \subseteq \mathfrak{B}_{d,n} \cup \{F_n/F_{n+1}\} \subseteq \mathfrak{A}_{d,n}$, it follows from Theorem 7.1 that

$$\lim_{d\to\infty} \frac{|\mathfrak{B}_{d,n}| + 1}{|\mathfrak{D}_{d,n}|} = 1.$$

Since $|\mathfrak{A}_{d,n}| \to \infty$ as $d \to \infty$, Theorem 7.1 implies that $|\mathfrak{D}_{d,n}| \to \infty$ as $d \to \infty$, proving that

$$\lim_{d\to\infty} \frac{|\mathfrak{B}_{d,n}|}{|\mathfrak{D}_{d,n}|} = 1.$$

□

Using Theorem 1.1, Henn and Priddy [6] prove the following theorem.

Theorem 7.4 (Henn and Priddy [6]). *Fix an odd prime p and $n \geq 2$. Let $u_{d,n}$ be the proportion of p-groups P generated by at most d elements and with Frattini length at most n that satisfy the following property: if H is a finite group with Sylow p-subgroup P, then H has a normal p-complement. Then* $\lim_{d\to\infty} u_{d,n} = 1$.

When $p = 2$, the analogues of Theorems 1.1 and 7.1 and Corollary 7.3 are open (and, presumably, the analogue of Theorem 7.4). Also, as mentioned in the introduction, the following question remains unanswered.

Question. *Fix a prime p. Let v_n be the proportion of p-groups with order less p^n whose automorphism group is a p-group. Is it true that* $\lim_{n\to\infty} v_n = 1$*?*

8 Acknowledgements

We would like to thank Persi Diaconis for introducing us to each other and for his continued support of this project. We would also like to thank Charles Leedham-Green for his help with the examples in the introduction. In the course of this research, the first author was partially supported by a Department of Defense National Defense Science and Engineering Graduate Fellowship.

References

[1] R. M. Bryant and L. G. Kovács, *Lie representations and groups of prime power order*, J. London Math. Soc. (2) **17** (1978), 415–421.

[2] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4*, 2005, package AutPGrp (`http://www.gap-system.org`).

[3] Adriano M. Garsia, *Combinatorics of the free Lie algebra and the symmetric group*, Analysis, et cetera, Academic Press, Boston, MA, 1990, pp. 309–382.

[4] Jay Goldman and Gian-Carlo Rota, *On the foundations of combinatorial theory. IV. Finite vector spaces and Eulerian generating functions*, Studies in Appl. Math. **49** (1970), 239–258.

[5] Philip Hall, *A contribution to the theory of groups of prime-power order*, Proc. London Math. Soc. **36** (1934), 29–95.

[6] Hans-Werner Henn and Stewart Priddy, *p-nilpotence, classifying space indecomposability, and other properties of almost all finite groups*, Comment. Math. Helv. **69** (1994), no. 3, 335–350.

[7] M. V. Horoševskiĭ, *The automorphism groups of finite p-groups*, Algebra i Logika **10** (1971), 81–86, English translation in Algebra and Logic **10** (1971), 54–57.

[8] M. V. Horoševskiĭ, *The automorphism group of wreath products of finite groups*, Sibirsk. Mat. Ž. **14** (1973), 651–659, 695, English translation in Siberian Math. J. **14** (1973), 453–458.

[9] B. Huppert, *Endliche Gruppen. I*, Die Grundlehren der Mathematischen Wissenschaften, Band 134, Springer-Verlag, Berlin, 1967.

[10] Bertram Huppert and Norman Blackburn, *Finite groups. II*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 242, Springer-Verlag, Berlin, 1982.

[11] Hans Kurzweil and Bernd Stellmacher, *The theory of finite groups*, Universitext, Springer-Verlag, New York, 2004.

[12] Michel Lazard, *Sur les groupes nilpotents et les anneaux de Lie*, Ann. Sci. Ecole Norm. Sup. (3) **71** (1954), 101–190.

[13] Alexander Lubotzky and Dan Segal, *Subgroup growth*, Progress in Mathematics, vol. 212, Birkhäuser Verlag, Basel, 2003.

[14] I. D. Macdonald, *A computer application to finite p-groups*, J. Austral. Math. Soc. **17** (1974), 102–112.

[15] I. G. Macdonald, *Symmetric functions and Hall polynomials*, second ed., Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, 1995.

[16] Avinoam Mann, *Some questions about p-groups*, J. Austral. Math. Soc. Ser. A **67** (1999), no. 3, 356–379.

[17] Ursula Martin, *Almost all p-groups have automorphism group a p-group*, Bull. Amer. Math. Soc. (N.S.) **15** (1986), no. 1, 78–82.

[18] G. A. Miller, *On the subgroups of an abelian group*, Ann. of Math. (2) **6** (1904), no. 1, 1–6.

[19] Hanna Neumann, *Varieties of groups*, Springer-Verlag New York, Inc., New York, 1967.

[20] A. I. Skopin, *The factor groups of an upper central series of free groups*, Doklady Akad. Nauk SSSR (N.S.) **74** (1950), 425–428.

[21] U. H. M. Webb, *The occurrence of groups as automorphisms of nilpotent p-groups*, Arch. Math. (Basel) **37** (1981), no. 6, 481–498.

[22] E. T. Whittaker and G. N. Watson, *A course of modern analysis. An introduction to the general theory of infinite processes and of analytic functions: with an account of the principal transcendental functions*, Fourth edition. Reprinted, Cambridge University Press, New York, 1962.

[23] Herbert S. Wilf, *Three problems in combinatorial asymptotics*, J. Combin. Theory Ser. A **35** (1983), no. 2, 199–207.