Formal Power Series and Algebraic Combinatorics
Nankai University, Tianjin, China, 2007

# The Automorphism Group of a Finite $p$-Group is Almost Always a $p$-Group

Geir T. Helleloid and Ursula Martin

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 whose automorphism group is a $p$-group. Yet the main theorem in this paper shows that the automorphism group of a finite $p$-group is almost always a $p$-group. The asymptotics in our theorem involve fixing any two of the following parameters and letting the third go to infinity: the lower $p$-length, the number of generators, and $p$. The proof of this theorem depends on a variety of topics: counting subgroups of a $p$-group; analyzing the lower $p$-series of a free group via its connection with the free Lie algebra; counting submodules of a module via Hall polynomials; and using numerical estimates on Gaussian coefficients.

## 1. Introduction

The main theorem of this paper shows that, in a certain asymptotic sense, the automorphism group of a finite $p$-group is almost always a $p$-group. A complete proof can be found in [**HM07**]; this paper outlines the arguments. A weaker version of this result was announced by the second author in [**Mar86**], but [**HM07**] contains the first published proof.

The result may not seem entirely plausible at first, as many common finite $p$-groups have an automorphism group that is not a $p$-group. Examples include: abelian $p$-groups, unless $p = 2$ and the type of the group does not have repeated parts (see Macdonald [**Mac95**, Chapter II, Theorem 1.6]); the Sylow-$p$ subgroup of $\mathrm{GL}(n, \mathbb{F}_p)$ for $p$ odd (see Gibbs [**Gib70**]); and the extraspecial $p$-groups (see Winter [**Win72**]). Furthermore, Bryant and Kovács [**BK78**] 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 below. Our result seems to say 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 whose automorphism group is a 2-group: $\mathbb{Z}_{2^n}$, the dihedral 2-group $D_{2^n}$ $(n \geq 3)$, and the generalized quaternion group $Q_{2^n}$ $(n \geq 4)$ are common examples, while Newman and O'Brien [**NO89**] offer three more infinite families. It is more difficult to find finite $p$-groups whose automorphism groups are $p$-groups when $p$ is odd. In [**Hor71**], 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 [**Hor71**] and [**Hor73**] that for any prime $p$, if $H_1, H_2, \ldots, H_n$ are finite $p$-groups whose automorphism groups are $p$-groups, then the automorphism group of the iterated wreath product $H_1 \wr H_2 \wr \cdots \wr H_n$ is also a $p$-group. Otherwise, most known examples arise from complicated and unnatural-looking constructions (see Webb [**Web81**]). A survey on the automorphism groups of finite $p$-groups, including a comprehensive list of examples in the literature of finite $p$-groups whose automorphism groups are $p$-groups, can be found in [**Helb**].

Compiled with the gracious help of Eamonn O'Brien (personal communication) and the GAP packages AutPGroup and SmallGroups [**GAP05**], Table 1 summarizes data on the proportion of small $p$-groups whose automorphism group is a $p$-group.

2000 *Mathematics Subject Classification.* Primary 20E36; Secondary 05A16.

*Key words and phrases.* $p$-group, automorphism group, lower $p$-series, Frattini subgroup, lower central $p$-series.

The first author was partially supported by a Department of Defense National Defense Science and Engineering Graduate Fellowship.

| 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 | 65 of 685 |
| $p^7$ | 2067 of 2328 | 2119 of 9310 | 11895 of 34297 |

TABLE 1. The proportion of $p$-groups of a given order whose automorphism group is a $p$-group

Of course, the meaning of the statement "The automorphism group of a finite $p$-group is almost always a $p$-group" depends on the asymptotic interpretation of "almost always." Probably the most natural interpretation is to consider all $p$-groups of order at most $p^n$ and let $n$ go to infinity. However, this is not the sense of our result, and indeed, the question remains open for this interpretation (see Mann [**Man99**, Question 9]). The precise statement of our main theorem depends on the *lower $p$-series* of a group. While this series is not as well-studied or widely used as, say, the lower central series, this is not the first context in which it has proven useful; see the beginning of Section 2 for references. The lower $p$-series will be defined in Section 2; for the moment, it suffices to say that it is a central series with elementary abelian factors and that the *lower $p$-length* of a group is the number of non-identity terms in the associated lower $p$-series. The main theorem of this paper may be concisely stated as follows.

THEOREM 1.1. *Fix a prime $p$ and positive integers $d$ and $n$. Let $r_{d,n}$ be the proportion of $p$-groups minimally generated by $d$ elements and with lower $p$-length at most $n$ whose automorphism group is a $p$-group. If $n \geq 2$, then*

$$\lim_{d\to\infty} r_{d,n} = 1.$$

*If $d \geq 5$, then*

$$\lim_{n\to\infty} r_{d,n} = 1.$$

*If $n = 2$ and $d \geq 10$, or $n \geq 3$ and $d \geq 6$, or $n \geq 10$ and $d \geq 5$, then*

$$\lim_{p\to\infty} r_{d,n} = 1.$$

The proof of Theorem 1.1 breaks down into three parts, which are presented in Sections 2, 4, and 5, and are assembled to prove Theorem 1.1 in Section 6. In the remainder of this section, we will outline the structure of the proof.

The first step is to connect the enumeration of finite $p$-groups to an analysis of certain subgroups and quotients of free groups. Let $F$ be the free group on $d$ generators and let $F_n$ be the $n$-th term in the lower $p$-series of $F$. It turns out that the action of $\mathrm{Aut}(F/F_{n+1})$ on $F_n/F_{n+1}$ induces an action of $\mathrm{GL}(d,\mathbb{F}_p)$ on $F_n/F_{n+1}$, and the $\mathrm{Aut}(F/F_{n+1})$-orbits on the normal subgroups of $F_n/F_{n+1}$ are also the $\mathrm{GL}(d,\mathbb{F}_p)$-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 lower $p$-series, we prove the following theorem.

THEOREM 1.2. *Fix a prime $p$ and integers $d, n \geq 2$. Let $F$ be the free group on $d$ generators and define the following sets:*

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

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

$$\mathfrak{D}_{d,n} \quad = \quad \{\textit{regular } \mathrm{GL}(d,\mathbb{F}_p)\textit{-orbits in } \mathcal{C}_{d,n}\}.$$

*Then there is a well-defined map* $\pi_{d,n} : \mathfrak{A}_{d,n} \to \{$*finite p-groups*$\}$ *given by* $L/F_{n+1} \mapsto F/L$*, where* $L/F_{n+1} \in \mathcal{A}_{d,n}$*. Furthermore* $\pi_{d,n}$ *induces bijections*

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

Recall that a regular orbit is one in which every point has trivial stabilizer. Note that as a result of Theorem 1.2, it is enough to show that $|\mathfrak{A}_{d,n}|/|\mathfrak{D}_{d,n}|$ goes to 1 under the relevant limits.

Section 3 follows with an examination of the structure of $F_n/F_{n+1}$ that will be needed in Sections 4 and 5. The second and third steps of the proof of Theorem 1.1 are summarized in Theorems 1.3 and 1.4 and are discussed in Sections 4 and 5. The terms $C(p)$ and $D(p)$ that appear in Theorems 1.3 and 1.4 are functions of $p$ which tend to 1 as $p \to \infty$. Both theorems depend on some combinatorial estimates, including bounds on Gaussian coefficients, many of which are contained in Wilf [**Wil83**].

THEOREM 1.3. *Fix a prime* $p$ *and integers* $d$ *and* $n$ *so that either* $n \geq 3$ *and* $d \geq 6$ *or* $n \geq 10$ *and* $d \geq 5$*. Let* $F$ *be the free group on* $d$ *generators and let* $d_n$ *be the rank of* $F_n/F_{n+1}$*. Then*

$$1 \leq \frac{|\mathfrak{A}_{d,n}|}{|\mathfrak{C}_{d,n}|} \leq 1 + C(p)^{n-1} D(p)^{n-2} p^{d_{n-1} - d_n/4 + d^2}.$$

The proof of Theorem 1.3 uses a theorem estimating the number of normal subgroups of an arbitrary finite $p$-group, applying it to quotients of free groups.

THEOREM 1.4. *Fix a prime* $p$ *and integers* $d$ *and* $n$ *so that either* $n = 2$ *and* $d \geq 10$ *or* $n \geq 3$ *and* $d \geq 3$*. Let* $F$ *be the free group on* $d$ *generators and let* $d_n$ *be the rank of* $F_n/F_{n+1}$*. Let*

$$K = \begin{cases} C(p)^5 D(p)^4 p^{17/4} & : \quad n = 2 \textit{ and } d \geq 10 \\ C(p)^2 D(p) p^{3/4} & : \quad n \geq 3. \end{cases}$$

*Let*

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

*Then*

*(a)*

$$1 \leq \frac{|\mathfrak{C}_{d,n}| \cdot |\mathrm{GL}(d,\mathbb{F}_p)|}{|\mathcal{C}_{d,n}|} \leq 1 + Kp^x.$$

*(b)*

$$1 \leq \frac{|\mathfrak{C}_{d,n}|}{|\mathfrak{D}_{d,n}|} \leq \frac{1 + Kp^x}{1 - Kp^x}.$$

In stating Theorems 1.3 and 1.4, we have judged it more satisfactory to give explicit numerical bounds, even though the proof of Theorem 1.1 requires only asymptotic bounds. However, since we have no expectation that our proof method gives bounds that are sharp, we have opted for clean explicit bounds rather than the best possible.

As we will show in Section 6, Theorem 1.1 follows easily from Theorems 1.2, 1.3, and 1.4. We close Section 6 with some observations and open questions.

## 2. The Lower $p$-Series

In this section, we define and discuss the *lower p-series* of a group (also called the *lower central p-series* or the *lower exponent-p central series*). Then, in Theorems 2.5 and 2.6, we describe how isomorphism classes of finite $p$-groups in a variety may be enumerated, obtaining Theorem 1.2 as a corollary.

**2.1. Preliminaries.** The lower $p$-series was introduced by Skopin [**Sko50**] and Lazard [**Laz54**], and it is described in detail by Huppert and Blackburn [**HB82**, Chapter VIII] (under the name $\lambda$-series) and by Bryant and Kovács [**BK78**]. The lower $p$-series is particularly suited to computer analysis of finite $p$-groups and forms the basis of the $p$-group generation algorithm of M. F. Newman [**New77**] (this algorithm is described in greater detail in, for example, O'Brien [**O'B90**]). This algorithm was modified in [**O'B95**] and [**ELGO02**] to construct automorphism groups of finite $p$-groups. It should also be mentioned that some information about the lower $p$-series has appeared in [**O'B90**] and [**ELGO02**], while the link between the lower $p$-series and automorphisms described later in this section is an extension of results that Higman [**Hig60**] and Sims [**Sim65**] used to count finite $p$-groups.

DEFINITION 2.1. Fix a prime $p$. For any group $H$, the *lower $p$-series* $H = H_1 \geq H_2 \geq \cdots$ of $H$ is defined by $H_{i+1} = H_i^p[H_i, H]$ for $i \geq 1$. $H$ is said to have *lower $p$-length* $n$ if $H_n$ is the last non-identity element of the lower $p$-series.

Note that if $H$ is a finite $p$-group, then $H_2 = \Phi(H)$, the Frattini subgroup of $H$. Before we list some basic facts about the lower $p$-series, recall that a subgroup is *fully invariant* if every endomorphism of the group restricts to an endomorphism of the subgroup. Also, we will write $H = \gamma_1(H) \geq \gamma_2(H) \geq \cdots$ to denote the *lower central series* of $H$, where $\gamma_{i+1}(H) = [\gamma_i(H), H]$. The following proposition states five fundamental properties of the lower $p$-series.

PROPOSITION 2.2. *For all positive integers $i$ and $j$,*

(1) $[H_i, H_j] \leq H_{i+j}$.
(2) $H_i^{p^j} \leq H_{i+j}$.
(3) $H_i = \gamma_1(H)^{p^{i-1}}\gamma_2(H)^{p^{i-2}} \cdots \gamma_i(H)$.
(4) *$H_{i+1}$ is the smallest normal subgroup of $H$ lying in $H_i$ such that $H_i/H_{i+1}$ is an elementary abelian $p$-group and is central in $H/H_{i+1}$.*
(5) *$H_i$ is fully invariant in $H$.*

As we will see, the fact that $H_i/H_{i+1}$ is elementary abelian, and therefore an $\mathbb{F}_p$-vector space, is a key reason we are able to prove the main theorem. It is easy to see the following proposition.

PROPOSITION 2.3. *Let $H$ be a finite group. Then $H$ is a $p$-group if and only if $H$ has finite lower $p$-length.*

The lower $p$-length of a finite $p$-group is related to the lower $p$-series of a free group in the following way. Let $F$ be the free group on $d$ generators; then any finite $p$-group $H$ that is minimally generated by $d$ elements is isomorphic to $F/U$ for some normal subgroup $U$ of $F$. By induction, $H_i = F_iU/U$. So the lower $p$-length of $H$ is $n$, where $F_{n+1}$ is the first term in the lower $p$-series of $F$ that is contained in $U$.

There is a link between the lower $p$-series and automorphisms. First, suppose that $H$ is a finite $p$-group that is minimally generated by $d$ elements. Of course, every automorphism of $H$ induces an automorphism of $H_i/H_{i+1}$ for each $i$. In particular, any automorphism of $H$ induces an element of $\mathrm{Aut}(H/H_2) \cong \mathrm{GL}(d, \mathbb{F}_p)$ (by the Burnside Basis Theorem, the rank of $H/H_2$ is $d$). Thus we obtain a map from $\mathrm{Aut}(H)$ to $\mathrm{GL}(d, \mathbb{F}_p)$, and an exact sequence

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

where $A(H)$ is a subgroup of $\mathrm{GL}(d, \mathbb{F}_p)$. The group $K(H)$ acts trivially on $H/H_2$, and hence on each factor $H_i/H_{i+1}$ (see Huppert and Blackburn [**HB82**, 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 $H_i/H_{i+1}$. The following key proposition is due to P. Hall [**Hal34**, Section 1.3].

PROPOSITION 2.4. *If $H$ is a finite $p$-group, then so is $K(H)$.*

We also note that by Huppert and Blackburn [**HB82**, Chapter VIII, Theorem 11.15], the rank of $F/[F, F]$, and hence of $F/F_2$, is $d$, and the rank of $F_n/F_{n+1}$ is finite for each $n$ (in Section 3, we will compute the rank of $F_n/F_{n+1}$ in general).

**2.2. Enumerating Groups in a Variety.** A *variety of groups* $V$ consists of all groups $G$ satisfying a set of relations $w = 1$, where $w$ ranges over a fixed set $W$ of group words (see Neumann [**Neu67**]). Let $F$ be the free group on $d$ generators. The variety $V$ contains a *relatively free group* on $d$ generators, namely

$F/U$, where $U$ is the *verbal subgroup* of $F$ generated by all the values of $w \in W$. For example, all abelian groups form 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 lower $p$-length at most $n$, but the theorems in this subsection hold in more general situations.

Let $U$ be a fully invariant subgroup of $F$. Then $G = F/U$ is a relatively free group in some variety $V$ minimally generated by $d$ elements. The relations defining $V$ come from setting each word in $U$ equal to the identity element. Suppose that $G$ is a finite non-trivial $p$-group. In this setting, we can describe $A(G)$ and $K(G)$ more precisely.

THEOREM 2.5. *Suppose that $G$ is the relatively free group on $d$ generators in a variety of groups $V$ and that $|G| = p^g$. Then*

$$1 \to K(G) \to \mathrm{Aut}(G) \to \mathrm{GL}(d, \mathbb{F}_p) \to 1$$

*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 groups in $V$ minimally generated by $d$ elements. 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 $|B(L)| = p^{dm}$.*

THEOREM 2.6. *Suppose that $G$ is the relatively free group on $d$ generators in a variety of groups $V$ and suppose that $G$ has lower $p$-length $n$. The map $L \mapsto G/L$ defines a bijection between $\mathrm{GL}(d, \mathbb{F}_p)$-orbits on normal subgroups $L$ of $G$ lying in $G_n$ and groups $H$ in $V$ that are minimally generated by $d$ elements and satisfy $H/H_n \cong G/G_n$. If $H = G/L$, then*

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

*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 $\mathrm{Aut}(H)$.*

The proofs of these two theorems are relatively straightfoward, using only basic properties of relatively free groups and the lower $p$-series. It is now easy to prove Theorem 1.2.

PROOF OF THEOREM 1.2. Take $V$ to be the variety of $p$-groups of lower $p$-length at most $n$. Then $F/F_{n+1}$ is the relatively free group on $d$ generators in $V$. The $\mathrm{Aut}(F/F_{n+1})$- and $\mathrm{GL}(d, \mathbb{F}_p)$-orbits in $\mathcal{C}_{d,n}$ are the same because of the first exact sequence in Theorem 2.5 and the fact that $K(F/F_{n+1})$ acts trivially on $F_n/F_{n+1}$ as in Subsection 2.1.

The map $\pi_{d,n}$ is well-defined and defines bijections for $\mathfrak{A}_{d,n}$ and $\mathfrak{B}_{d,n}$ by Theorem 2.5. A normal subgroup $L$ of $F/F_{n+1}$ lying in $F_n/F_{n+1}$ is in a regular $\mathrm{GL}(d, \mathbb{F}_p)$-orbit if $N_{\mathrm{GL}(d,\mathbb{F}_p)}(L) = 1$. By Theorem 2.6, $L$ 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 Lower $p$-Series of a Free Group

Let $F$ be the free group on $d$ generators $y_1, y_2, \ldots, y_d$. To prepare for Sections 4 and 5, we need to analyze the $\mathbb{F}_p\mathrm{GL}(d, \mathbb{F}_p)$-module structure of $F_n/F_{n+1}$ along with power and commutator maps from $F_n/F_{n+1}$ to $F_{n+1}/F_{n+2}$. Our main tool will be the connection between the lower $p$-series of $F$ and the free Lie algebra described in Theorem 3.2. The results of Theorem 3.2 appear several times in the literature with varying degrees of correctness and detail. Our presentation follows Bryant and Kovács [**BK78**], while the most complete proof may be inferred from Huppert and Blackburn [**HB82**, Chapter VIII]. A complete proof will be available in [**Hela**].

Let $K$ be any field and let $A = \{x_1, \ldots, x_d\}$ be an alphabet on $d$ letters. Write $A^*$ for the collection of all $A$-words and $A^n$ for the collection of all $A$-words of length $n$. Let $K[A^*]$ denote the non-commutative algebra of polynomials

$$f = \sum_{w \in A^*} f_w w$$

with coefficients $f_w \in K$. The algebra $K[A^*]$ is graded by degree; let $K[A^n]$ denote the homogeneous component of degree $n$. Also, $K[A^*]$ is a Lie algebra under the Lie bracket $[f,g] = fg - gf$. Let $K[\Lambda^*]$ denote the Lie subalgebra of $K[A^*]$ generated by $x_1, \ldots, x_d$ and the Lie bracket. Then $K[\Lambda^*]$ is the *free Lie algebra* over $K$ on $x_1, \ldots, x_d$. It is also graded by degree; let $K[\Lambda^n]$ be the homogeneous component of $K[\Lambda^*]$ of degree $n$.

The results in this section require several maps; in an attempt to clarify matters, we will define all the maps now, using suggestive names, and postpone stating their properties until necessary.

DEFINITION 3.1. Fix a prime $p$. Fix integers $n \geq 1$, $d \geq 2$, and $1 \leq j \leq d$. Let $f_i \in F_i$ for each $i \geq 1$.

- $\mathrm{pow}_n : F_n/F_{n+1} \to F_{n+1}/F_{n+2}$
  (*a power map on $F$*)
  $\mathrm{pow}_n : f_n F_{n+1} \mapsto f_n^p F_{n+2}$
- $\mathrm{Fcom}_{j,n} : F_n/F_{n+1} \to F_{n+1}/F_{n+2}$
  (*a commutator map on $F$*)
  $\mathrm{Fcom}_{j,n} : f_n F_{n+1} \mapsto [f_n, y_j] F_{n+2}$
- $\mathrm{emb}_n : F_n \to \mathbb{F}_p[A^*]$
  (*an embedding of $F_n$ into $\mathbb{F}_p[A^*]$*)
  $\mathrm{emb}_1 : y_j \mapsto x_j$
  $\mathrm{emb}_n : f_{n-1}^p \mapsto \begin{cases} \mathrm{emb}_1(f_1) + \mathrm{emb}_1(f_1)^2 & : n = 2 \text{ and } p = 2 \\ \mathrm{emb}_{n-1}(f_{n-1}) & : \text{otherwise} \end{cases}$
  $\mathrm{emb}_n : [f_{n-1}, f_1] \mapsto [\mathrm{emb}_{n-1}(f_{n-1}), \mathrm{emb}_1(f_1)]$
  $\mathrm{emb}_n : f_{n+1} \mapsto 0$
- $\mathrm{qemb}_n : F_n/F_{n+1} \to \mathbb{F}_p[A^*]$
  (*an embedding of the quotient $F_n/F_{n+1}$ into $\mathbb{F}_p[A^*]$*)
  $\mathrm{qemb}_n$ is induced by $\mathrm{emb}_n$
- $\mathrm{com}_j : \mathbb{F}_p[A^*] \to \mathbb{F}_p[A^*]$
  (*a commutator map on $\mathbb{F}_p[A^*]$*)
  $\mathrm{com}_j : f \mapsto [f, x_j]$

THEOREM 3.2. *The map* $\mathrm{emb}_n$ *is a well-defined homomorphism. The map* $\mathrm{qemb}_n$ *is an* $\mathbb{F}_p\mathrm{GL}(d,\mathbb{F}_p)$*-module embedding of* $F_n/F_{n+1}$ *into* $\mathbb{F}_p[A^*]$*. If* $p$ *is odd, the image of* $\mathrm{qemb}_n$ *is* $\mathbb{F}_p[\Lambda^1] \oplus \cdots \oplus \mathbb{F}_p[\Lambda^n]$*, and hence*

$$F_n/F_{n+1} \cong \mathbb{F}_p[\Lambda^1] \oplus \cdots \oplus \mathbb{F}_p[\Lambda^n]$$

*as* $\mathbb{F}_p\mathrm{GL}(d,\mathbb{F}_p)$*-modules.*

*If* $p = 2$*, the image of* $\mathrm{qemb}_1$ *is* $\mathbb{F}_2[\Lambda^1]$*. The image* $E$ *of* $\mathrm{qemb}_2$ *satisfies*

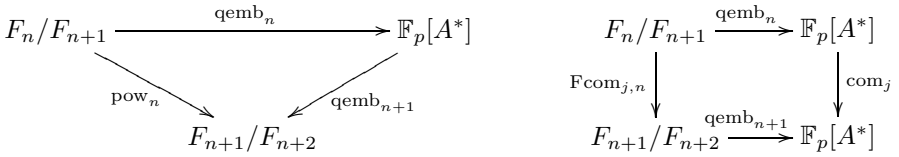
$$E + \mathbb{F}_2[A^2] = \mathbb{F}_2[A^1] \oplus \mathbb{F}_2[A^2] \quad \text{and} \quad E \cap \mathbb{F}_2[A^2] = \mathbb{F}_2[\Lambda^2],$$

*so* $E$ *is an extension of* $\mathbb{F}_2[\Lambda^2]$ *by* $\mathbb{F}_2[\Lambda^1]$*. For* $n \geq 3$*, the image of* $\mathrm{qemb}_n$ *is* $E \oplus \mathbb{F}_2[\Lambda^3] \oplus \cdots \oplus \mathbb{F}_2[\Lambda^n]$*, and hence*

$$F_n/F_{n+1} \cong E \oplus \mathbb{F}_2[\Lambda^3] \oplus \cdots \oplus \mathbb{F}_2[\Lambda^n].$$

Note that as a $\mathbb{F}_p\mathrm{GL}(d,\mathbb{F}_p)$-module, $\mathbb{F}_p[\Lambda^n] \cong V \wedge V \wedge \cdots \wedge V$, the $n$-fold wedge product where $V$ is the natural $\mathbb{F}_p\mathrm{GL}(d,\mathbb{F}_p)$-module.

COROLLARY 3.3. *Unless* $p = 2$ *and* $n = 1$*, the diagram on the left commutes and* $\mathrm{pow}_n$ *is an injective homomorphism. The diagram on the right commutes and* $\mathrm{Fcom}_{j,n}$ *is a homomorphism.*




The dimension of $K[\Lambda^i]$ is given by Witt's formula:

$$\dim(K[\Lambda^i]) = \frac{1}{i} \sum_{j|i} \mu(i/j) \cdot d^j,$$

where $\mu$ is the Möbius function (see [**Reu93**, Appendix 0.4.2]). Thus Theorem 3.2 tells us the rank of $F_n/F_{n+1}$.

COROLLARY 3.4. *The rank of $F_n/F_{n+1}$ is*

$$\sum_{i=1}^{n} \frac{1}{i} \sum_{j|i} \mu(i/j) \cdot d^j.$$

A close analysis of the free Lie algebra lets us prove a lemma about the dimensions of subspaces and the map com.

LEMMA 3.5. *Fix $d \geq 3$. Let $U_n = \mathbb{F}_p[\Lambda^1] \oplus \cdots \oplus \mathbb{F}_p[\Lambda^n]$ if $p$ is odd or $U_n = E \oplus \mathbb{F}_2[\Lambda^3] \oplus \cdots \oplus \mathbb{F}_2[\Lambda^n]$ if $p = 2$. Suppose that $W$ is a subspace of $\mathbb{F}_p[A^*]$ contained in $U_n$. Then $\dim(W + \mathrm{com}(W)) \geq (3/2)\dim(W)$.*

Since the free Lie algebra and the lower $p$-series of $F$ are so intimately connected, Lemma 3.5 almost directly implies the following theorem and corollary about $F/F_{n+1}$.

THEOREM 3.6. *Fix a prime $p$ and integers $d \geq 3$ and $n \geq 2$. Suppose that $U$ is a normal subgroup of $F$ lying in $F_2$. Let*

$$\begin{aligned} Q &= (U \cap F_n)F_{n+1}/F_{n+1} \\ R &= (U_2 \cap F_{n+1})F_{n+2}/F_{n+2} \\ S &= (U^p[U,F] \cap F_{n+1})F_{n+2}/F_{n+2}. \end{aligned}$$

*Then $\mathrm{rank}(R) \geq \mathrm{rank}(Q)$ and $\mathrm{rank}(S) \geq (3/2)\,\mathrm{rank}(Q)$.*

The third isomorphism theorem lets us replace $F$ by $F/F_n$, giving the following corollary.

COROLLARY 3.7. *Fix a prime $p$ and integers $d \geq 3$, $n \geq 3$, and $2 \leq i < n$. Let $G = F/F_{n+1}$. Suppose that $U$ is a normal subgroup of $G$ lying in $G_2$. Let*

$$\begin{aligned} Q &= (U \cap G_i)G_{i+1}/G_{i+1} \\ R &= (U_2 \cap G_{i+1})G_{i+2}/G_{i+2} \\ S &= (U^p[U,F] \cap G_{i+1})G_{i+2}/G_{i+2}. \end{aligned}$$

*Then $\mathrm{rank}(R) \geq \mathrm{rank}(Q)$ and $\mathrm{rank}(S) \geq (3/2)\,\mathrm{rank}(Q)$.*

Corollary 3.7 will allow us to count normal subgroups of $F/F_{n+1}$ when combined with Theorem 4.1.

## 4. From Subgroups in $F_2/F_{n+1}$ to Subgroups in $F_n/F_{n+1}$

The goal of this section is to outline a proof of Theorem 1.3, essentially showing that most $\mathrm{GL}(d,\mathbb{F}_p)$-orbits of normal subgroups of $F/F_{n+1}$ contained in $F_2/F_{n+1}$ are $\mathrm{GL}(d,\mathbb{F}_p)$-orbits of normal subgroups of $F/F_{n+1}$ contained in $F_n/F_{n+1}$. The theorem is obtained by estimating the number of normal subgroups of $F/F_{n+1}$ contained in $F_2/F_{n+1}$. Theorem 4.1 offers a refined estimate on the number of normal subgroups of an arbitrary finite $p$-group. Our estimate depends on certain parameters which are difficult to work out in general, but have been calculated for $F/F_{n+1}$ in Corollary 3.7. This gives us the tools to prove Theorem 1.3.

Let $H$ be a finite $p$-group of lower $p$-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

$$S(H,\vec{u}) = \{U \lhd H \ : \ \dim((U \cap H_i)H_{i+1}/H_{i+1}) = u_i\},$$

where $\vec{u} = (u_1, \ldots, u_n)$ and each integer $u_i$ satisfies

$$0 \leq u_i \leq h_i = \dim(H_i/H_{i+1}).$$

THEOREM 4.1. *Suppose that for each $U \in S(H,\vec{u})$,*

$$\dim((U_2 \cap H_i)H_{i+1}/H_{i+1}) \geq v_i$$

*and*

$$\dim((U^p[U,H] \cap H_i)H_{i+1}/H_{i+1}) \geq w_i.$$

*Then*

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

Applying Theorem 4.1 and Corollary 3.7 and using combinatorial estimates for Gaussian coefficients from Wilf [**Wil83**] proves Theorem 1.3.

## 5. Most Orbits on Subgroups of $F_n/F_{n+1}$ are Regular

The proof of Theorem 1.4 depends on estimating $|\mathfrak{C}_{d,n}|$, the number of $\mathrm{GL}(d,\mathbb{F}_p)$-orbits on subspaces of $F_n/F_{n+1}$, via the Cauchy-Frobenius Lemma. To do this, we obtain in Theorem 5.2 an upper bound for the number of subspaces of $F_n/F_{n+1}$ fixed by an element of $\mathrm{GL}(d,\mathbb{F}_p)$, and refine this in Theorem 5.3 to obtain a stronger bound in the case $n = 2$.

Suppose $M$ is an $\mathbb{F}_p\mathrm{GL}(d,\mathbb{F}_p)$-module. Let $g \in \mathrm{GL}(d,\mathbb{F}_p)$. We want to count the number of subspaces of $M$ (viewed as an $\mathbb{F}_p$-vector space) fixed by $g$, which is the number of submodules of $M$ as a $\mathbb{F}_p\langle g\rangle$-module. We note that when $M$ is the natural $\mathbb{F}_p\mathrm{GL}(d,\mathbb{F}_p)$-module, Eick and O'Brien [**EO99**] give an explicit formula for this number. The following preliminaries are based on Macdonald [**Mac95**, Chapter IV, Section 2].

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

$$M \cong \bigoplus_{f\in\Phi} \bigoplus_i \frac{\mathbb{F}_p[t]}{(f)^{\mu_i(f)}},$$

where $\mu_i(f)$ is the $i$-th part of $\mu(f)$, $(f)$ is the ideal of $\mathbb{F}_p[t]$ generated by $f$, and $g$ acts upon $\mathbb{F}_p[t]/(f)^s$ as multiplication by $t$.

Let

$$M_f = \bigoplus_i \frac{\mathbb{F}_p[t]}{(f)^{\mu_i(f)}}.$$

We call $\mu(f)$ the *type* of $M_f$. Any submodule $N$ of $M$ can be written $N = \oplus_{f\in\Phi} N_f$ with $N_f \subseteq M_f$ for each $f \in \Phi$. That is, every submodule of $M$ is the direct sum of submodules of the summands $M_f$. By Macdonald [**Mac95**, Chapter II, 3.1] the type $\lambda$ of any $\mathbb{F}_p\langle g\rangle$-submodule or quotient module of $M_f$ satisfies $\lambda \subseteq \mu(f)$.

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

Both Theorems 5.2 and 5.3 depend on Theorem 5.1, where we calculate the number of submodules of fixed type in a module of fixed type over a discrete valuation ring. This generalizes the formula for the number of subgroups of a finite abelian $p$-group (see Birkhoff [**Bir35**]).

THEOREM 5.1. *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 $\alpha'$. Then the number of submodules of $M$ of type $\beta'$ is*

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

Theorem 5.1 and some combinatorial estimates give the following upper bound on the number of subspaces of $F_n/F_{n+1}$ fixed by an element of $\mathrm{GL}(d,\mathbb{F}_p)$.

THEOREM 5.2. *Fix $d \geq 2$ and $g \in \mathrm{GL}(d,\mathbb{F}_p)$. Suppose that $M$ is an $\mathbb{F}_p\langle g\rangle$-module. Let $m = \dim_{\mathbb{F}_p}(M)$ and let $S_M$ be the number of submodules of $M$. Then either $g$ acts as a scalar on $M$ and $S_M$ equals the total number of subspaces of an $m$-dimensional $\mathbb{F}_p$-vector space, or $g$ does not act as a scalar and*

$$\log_p S_M \leq (m^2 - 2m + 2)/4 + 2\varepsilon,$$

*where $\varepsilon = \log_p(C(p)D(p))$.*

The next theorem strengthens this result when the module structure is known more precisely and is needed to deal with groups of lower $p$-length 2.

THEOREM 5.3. *Fix $d \geq 2$ and $g \in \mathrm{GL}(d, \mathbb{F}_p)$ with $g \neq 1$. Suppose that $V$ is an $\mathbb{F}_p\langle g\rangle$-module on which $g$ acts non-trivially and that $M$ is an $\mathbb{F}_p\langle g\rangle$-module extension of $V \wedge V$ by $V$. Let $v = \dim_{\mathbb{F}_p}(V)$, let $m = \dim_{\mathbb{F}_p}(M) = v(v+1)/2$, and let $S_M$ be the number of submodules of $M$. Then*

$$\log_p S_M \leq (m-4)^2/4 + C,$$

*where $\varepsilon = \log_p(C(p)D(p))$ and*

$$C = \begin{cases} \varepsilon + 2m - 4 & : \quad m \leq 45 \\ 5\varepsilon + 4 & : \quad \text{otherwise.} \end{cases}$$

Recall that $\mathfrak{C}_{d,n}$ is the set of $\mathrm{GL}(d,\mathbb{F}_p)$-orbits in $\mathcal{C}_{d,n}$, $\mathfrak{D}_{d,n}$ is the set of regular orbits in $\mathfrak{C}_{d,n}$ (that is, the orbits in which every point has trivial stabilizer), and $|\mathcal{C}_{d,n}| = \mathcal{G}_{d_n}(p)$. If $g \in \mathrm{GL}(d,\mathbb{F}_p)$, 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 $\mathbb{F}_p\langle g\rangle$-module, which we estimated in Theorems 5.2 and 5.3. Theorem 1.4 then follows from the Cauchy-Frobenius Theorem.

## 6. Summary

In this section we use Theorems 1.2, 1.3, and 1.4 to prove Theorem 1.1 along with two corollaries.

**Theorem 1.1** *Fix a prime $p$ and positive integers $d$ and $n$. Let $r_{d,n}$ be the proportion of $p$-groups minimally generated by $d$ elements and with lower $p$-length at most $n$ whose automorphism group is a $p$-group. If $n \geq 2$, then*

$$\lim_{d\to\infty} r_{d,n} = 1.$$

*If $d \geq 5$, then*

$$\lim_{n\to\infty} r_{d,n} = 1.$$

*If*

$$n = 2 \text{ and } d \geq 10, \text{ or } n \geq 3 \text{ and } d \geq 6, \text{ or } n \geq 10 \text{ and } d \geq 5, \tag{6.1}$$

*then*

$$\lim_{p\to\infty} r_{d,n} = 1.$$

PROOF. The set of $p$-groups minimally generated by $d$ elements and with lower $p$-length at most $n$ is $\mathfrak{A}_{d,n}$. When $n = 2$, $\mathfrak{A}_{d,n} = \mathfrak{C}_{d,n}$. The expression

$$C(p)^{n-1}D(p)^{n-2}p^{d_{n-1}-d_n/4+1/4+d^2}$$

goes to 0 as $d \to \infty$ if $n \geq 3$ or as $n \to \infty$ if $d \geq 5$. If $d$ and $n$ satisfy one of the conditions of Equation 6.1, then the exponent of $p$ is negative. By Theorem 1.3, it follows that

$$\begin{aligned} \lim_{d\to\infty} \frac{|\mathfrak{A}_{d,n}|}{|\mathfrak{C}_{d,n}|} &= 1 \quad \text{if } n \geq 2, \\ \lim_{n\to\infty} \frac{|\mathfrak{A}_{d,n}|}{|\mathfrak{C}_{d,n}|} &= 1 \quad \text{if } d \geq 5, \text{ and} \\ \lim_{p\to\infty} \frac{|\mathfrak{A}_{d,n}|}{|\mathfrak{C}_{d,n}|} &= 1 \quad \text{if one of the conditions in Equation 6.1 holds.} \end{aligned}$$

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

$$\begin{aligned} \lim_{d\to\infty} \frac{|\mathfrak{C}_{d,n}|}{|\mathfrak{D}_{d,n}|} &= 1 \quad \text{if } n \geq 2, \\ \lim_{n\to\infty} \frac{|\mathfrak{C}_{d,n}|}{|\mathfrak{D}_{d,n}|} &= 1 \quad \text{if } d \geq 5, \text{ and} \\ \lim_{p\to\infty} \frac{|\mathfrak{C}_{d,n}|}{|\mathfrak{D}_{d,n}|} &= 1 \quad \text{if one of the conditions in Equation 6.1 holds.} \end{aligned}$$

It follows that $|\mathfrak{A}_{d,n}|/|\mathfrak{D}_{d,n}|$ goes to 1 under the specified limits, and the theorem follows. □

COROLLARY 6.1. *Fix a prime $p$ and $n \geq 2$. Let $s_{d,n}$ be the proportion of $p$-groups generated by at most $d$ elements and with lower $p$-length at most $n$ whose automorphism group is a $p$-group. Then*

$$\lim_{d\to\infty} s_{d,n} = 1.$$

PROOF. This follows directly from Theorem 1.1 and the trivial observation that the number of $p$-groups generated by at most $d$ elements and with lower $p$-length at most $n$ is finite, while the number of $p$-groups with lower $p$-length at most $n$ is infinite. □

COROLLARY 6.2. *Fix a prime $p$ and $n \geq 2$. Let $t_{d,n}$ be the proportion of $p$-groups minimally generated by $d$ elements and with lower $p$-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 1.1 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 1.1 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 [**HP94**] prove the following theorem.

THEOREM 6.3 (Henn and Priddy [**HP94**]). *Fix a prime $p$ and integers $d, n \geq 2$. Let $u_{d,n}$ be the proportion of $p$-groups $P$ generated by at most $d$ elements and with lower $p$-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* $\lim_{d\to\infty} u_{d,n} = 1$.

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 at most $p^n$ whose automorphism group is a $p$-group. Is it true that* $\lim_{n\to\infty} v_n = 1$*?*

## 7. 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 several illuminating conversations and for his help with the examples in the introduction. Finally, we would like to thank Eamonn O'Brien for his help with references and computational data. For part of this research, the first author was supported by a Department of Defense National Defense Science and Engineering Graduate Fellowship.

## References

[Bir35] G. Birkhoff, *Subgroups of abelian groups*, Proc. London Math. Soc. (2) **38** (1934–35), 387–401.

[BK78] R. M. Bryant and L. G. Kovács, *Lie representations and groups of prime power order*, J. London Math. Soc. (2) **17** (1978), 415–421.

[ELGO02] B. Eick, C. R. Leedham-Green, and E. A. O'Brien, *Constructing automorphism groups of $p$-groups*, Comm. Algebra **30** (2002), no. 5, 2271–2295.

[EO99] B. Eick and E. A. O'Brien, *Enumerating $p$-groups*, J. Austral. Math. Soc. Ser. A **67** (1999), no. 2, 191–205.

[GAP05] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4*, 2005, packages AutPGrp and SmallGroups (`http://www.gap-system.org`).

[Gib70] J. A. Gibbs, *Automorphisms of certain unipotent groups*, J. Algebra **14** (1970), 203–228.

[Hal34] P. Hall, *A contribution to the theory of groups of prime-power order*, Proc. London Math. Soc. **36** (1934), 29–95.

[HB82] B. Huppert and N. Blackburn, *Finite groups. II*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 242, Springer-Verlag, Berlin, 1982.

[Hela] G. T. Helleloid, *Automorphism groups of finite $p$-groups: Structure and applications*, Ph.D. Thesis, Stanford University, forthcoming.

[Helb] ———, *A survey on automorphism groups of finite $p$-groups*, available at arXiv:math.GR/0610294.

[Hig60] G. Higman, *Enumerating $p$-groups. I. Inequalities*, Proc. London Math. Soc. (3) **10** (1960), 24–30.

[HM07] G. T. Helleloid and U. Martin, *The automorphism group of a finite p-group is almost always a p-group*, J. Algebra **312** (2007), no. 1, 294–329, available at arXiv:math.GR/0602039.

[Hor71] 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.

[Hor73] ———, *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.

[HP94] H.-W. Henn and S. Priddy, *p-nilpotence, classifying space indecomposability, and other properties of almost all finite groups*, Comment. Math. Helv. **69** (1994), no. 3, 335–350.

[Laz54] M. Lazard, *Sur les groupes nilpotents et les anneaux de Lie*, Ann. Sci. Ecole Norm. Sup. (3) **71** (1954), 101–190.

[Mac95] I. G. Macdonald, *Symmetric functions and Hall polynomials*, second ed., Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, 1995.

[Man99] A. Mann, *Some questions about p-groups*, J. Austral. Math. Soc. Ser. A **67** (1999), no. 3, 356–379.

[Mar86] U. Martin, *Almost all p-groups have automorphism group a p-group*, Bull. Amer. Math. Soc. (N.S.) **15** (1986), no. 1, 78–82.

[Neu67] H. Neumann, *Varieties of groups*, Springer-Verlag New York, Inc., New York, 1967.

[New77] M. F. Newman, *Determination of groups of prime-power order*, Group theory (Proc. Miniconf., Australian Nat. Univ., Canberra, 1975), Springer, Berlin, 1977, pp. 73–84. Lecture Notes in Math., Vol. 573.

[NO89] M. F. Newman and E. A. O'Brien, *A CAYLEY library for the groups of order dividing* 128, Group Theory (Singapore, 1987), de Gruyter, Berlin, 1989, pp. 437–442.

[O'B90] E. A. O'Brien, *The p-group generation algorithm*, J. Symbolic Comput. **9** (1990), no. 5-6, 677–698, Computational group theory, Part 1.

[O'B95] ———, *Computing automorphism groups of p-groups*, Computational algebra and number theory (Sydney, 1992), Math. Appl., vol. 325, Kluwer Acad. Publ., Dordrecht, 1995, pp. 83–90.

[Reu93] C. Reutenauer, *Free Lie algebras*, London Mathematical Society Monographs. New Series, vol. 7, The Clarendon Press Oxford University Press, New York, 1993.

[Sim65] C. C. Sims, *Enumerating p-groups*, Proc. London Math. Soc. (3) **15** (1965), 151–166.

[Sko50] A. I. Skopin, *The factor groups of an upper central series of free groups*, Doklady Akad. Nauk SSSR (N.S.) **74** (1950), 425–428.

[Web81] U. H. M. Webb, *The occurrence of groups as automorphisms of nilpotent p-groups*, Arch. Math. (Basel) **37** (1981), no. 6, 481–498.

[Wil83] H. S. Wilf, *Three problems in combinatorial asymptotics*, J. Combin. Theory Ser. A **35** (1983), no. 2, 199–207.

[Win72] D. L. Winter, *The automorphism group of an extraspecial p-group*, Rocky Mountain J. Math. **2** (1972), no. 2, 159–168.

Department of Mathematics, Stanford University, Stanford, CA 94305-2125
*E-mail address*: geir@math.stanford.edu

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