TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 348, Number 9, September 1996

MAXIMAL SUBGROUPS IN FINITE AND PROFINITE GROUPS

ALEXANDRE V. BOROVIK, LASZLO PYBER, AND ANER SHALEV

ABSTRACT. We prove that if a finitely generated profinite group G is not generated with positive probability by finitely many random elements, then every finite group F is obtained as a quotient of an open subgroup of G. The proof involves the study of maximal subgroups of profinite groups, as well as techniques from finite permutation groups and finite Chevalley groups. Confirming a conjecture from Ann. of Math. **137** (1993), 203–220, we then prove that a finite group G has at most $|G|^c$ maximal soluble subgroups, and show that this result is rather useful in various enumeration problems.

1. INTRODUCTION

Let G be a finitely generated profinite group, and let $m_n = m_n(G)$ denote the number of maximal subgroups of index n in G. The series $\{m_n\}$, referred to as the *maximal subgroup growth* of G, has recently been investigated in [14, 16]. We say that G has *polynomial maximal subgroup growth* if for some c and for all n we have $m_n(G) \leqslant n^c$. Such groups are called *PMSG groups*. The class of PMSG groups is a natural extension of the class of PSG groups (namely of groups with polynomial subgroup growth) which was studied extensively by Lubotzky, Mann, Segal and others (see for instance [13]). The interest in these groups partially stems from some probabilistic questions. Let us say that G is *positively finitely generated* (PFG for short) if there exists k such that k elements chosen at random from G will generate G with positive probability. Here we view G (and its Cartesian power G^k) as a probability space, with respect to a normalized Haar measure. For example, by results of [7], abelian profinite groups are PFG, while nonabelian free profinite groups are not PFG. An elementary probabilistic argument, given in [14], shows that every PMSG group is a PFG group. This is used to show that prosoluble groups are PFG [14, Theorem 10]. Here we establish similar results for a larger class of profinite groups.

Our main result is as follows.

Theorem 1.1. *Let G be a finitely generated profinite group, and suppose there is a finite group F which is not obtained as a quotient of an open subgroup of G. Then G has polynomial maximal subgroup growth. Consequently, G is positively finitely generated.*

Received by the editors September 21, 1995.
1991 *Mathematics Subject Classification.* Primary 20E28, 20D99; Secondary 20B35, 20D06.
The second author acknowledges support of the Hungarian National Foundation for Scientific Research, Grant No. T7441.
The third author acknowledges support of the Basic Research Foundation, administrated by the Israel Academy of Sciences and Humanities.

Theorem 1.1 has the following finitary version: *for every finite group F there is a constant $c(F)$ such that if G is a finite d-generated group which does not have sections isomorphic to F, then $m_n(G) \leqslant n^{c(F)d}$ for all n. This implies that if $s > 1$ and $k = c(F)d + s$ is an integer, then k randomly chosen elements of G generate G with probability $\geqslant 1 - \zeta(s)$, where ζ is the Riemann zeta function.*

It is not known whether the subgroup growth of PMSG groups is at most exponential. However, the finitary version of Theorem 1.1 can be used to show that the subgroup growth of groups satisfying the assumptions of this theorem is at most exponential (see the second proof of [14, Theorem 12]). A similar but somewhat stronger result is obtained in [18].

While Theorem 1.1 extends [14, Theorem 10] stated above, it also generalizes [14, Theorem 15] and [16, Proposition 3], showing that $SL_n(\mathbb{Z})$ ($n \geqslant 3$) and similar arithmetic groups (in arbitrary characteristic) with the congruence subgroup property are PMSG. Indeed, these arithmetic groups (more precisely, their profinite completions) are easily seen to satisfy the assumption of Theorem 1.1.

We note that Theorem 1.1 does not characterize PMSG groups. For instance, using iterated wreath products of alternating groups, Bhattacharjee [4] has constructed PMSG profinite groups which have all alternating groups—hence all finite groups—as upper sections (i.e. as quotients of finite index subgroups). The question of characterizing finitely generated PMSG profinite groups is still very much open. It is shown in [16] (using the Classification Theorem) that a finitely generated profinite group is PMSG if and only if it is PFG. This provides some sort of characterization without clearing the mystery around the structure of PMSG groups.

The proof of Theorem 1.1 consists of several stages. We first need some notation. Let $\mathcal{F}$ denote a class of finite groups satisfying the following conditions:

> *The class $\mathcal{F}$ is closed under taking quotients, subgroups, and extensions, contains all finite soluble groups and does not contain all finite groups.*

A typical example is the class $\mathcal{S}$ of all finite soluble groups, or the class $\mathcal{F}_d$ ($d \geqslant 5$) of all finite groups not involving the alternating group Alt_d as a section; we call such groups *Alt_d-free*. In general, if $\mathcal{F}$ is as above, then the groups in $\mathcal{F}$ satisfy the well-known Babai-Cameron-Pálfy restrictions on their nonabelian composition factors [3]. We say that a subgroup $G \leqslant Sym_n$ is a maximal transitive (or primitive) $\mathcal{F}$-subgroup if G is transitive (primitive), $G \in \mathcal{F}$, and G is maximal with respect to these properties.

The first step in proving Theorem 1.1 is to reduce it to the following result on finite permutation groups.

Theorem 1.2. *Sym_n has at most $n^{c(\mathcal{F})}$ conjugacy classes of maximal transitive $\mathcal{F}$-subgroups.*

The reduction is based on the Babai-Cameron-Pálfy polynomial bound on the orders of Alt_d-free primitive permutation groups [3]. Now, using the O'Nan-Scott Theorem [10] and [16, Theorem 1.1], we reduce Theorem 1.2 to the following result in finite linear groups.

Theorem 1.3. *$GL_n(q)$ has at most $q^{c(\mathcal{F})n}$ conjugacy classes of maximal irreducible $\mathcal{F}$-subgroups.*

The proof of Theorem 1.3 relies heavily on Aschbacher's Theorem on the subgroup structure of the classical groups [1]. We note that merely invoking Asch-

bacher's Theorem does not seem to be enough, since the subgroups we are counting need not be maximal in $GL_n(q)$; consequently, we embark on a rather complicated inductive process which eventually yields the required result.

Theorem 1.2 for the class of soluble groups improves Lemma 3.2 of [17], where it is shown that Sym_n has at most $n^{c\log^2 n}$ maximal transitive soluble subgroups up to conjugacy (where c is approximately 3). As for non-transitive groups, we show that Sym_n has at most c^n conjugacy classes of maximal $\mathcal{F}$-subgroups (see Lemma 2.2 below).

As a by-product of our methods we obtain the following result which is of independent interest.

Theorem 1.4. *There exists an absolute constant $c > 0$ such that a finite group G has at most $|G|^c$ maximal soluble subgroups.*

This settles a conjecture from [17]. While we do not obtain sharp bounds on the exponent c in Theorem 1.4, we conjecture that $c = 1$ will do. Theorem 1.4 seems to be quite useful in various enumeration problems; for example, it can be used to give a streamlined proof of the main result of [17] and of [12, Theorem F]. More applications are given below. Denote by $s(G)$ the number of subgroups of a finite group G. For a prime p, let G_p denote a Sylow p-subgroup of G.

Corollary 1.5. *Let c be as in Theorem 1.4, and let G be a finite group. Then*

$$s(G) \leqslant |G|^{c+1} \prod_p s(G_p).$$

The next result, which applies Corollary 1.5, provides an upper bound on $s(G)$ in terms of $|G|$ alone. It improves the crude and frequently used bound

$$s(G) \leqslant |G|^{\log_2 |G|}.$$

Corollary 1.6. *Let G be a finite group. Then*

$$s(G) \leqslant |G|^{(1/4+o(1))\log_2 |G|}.$$

This bound is essentially the best possible, as the example of elementary abelian 2-groups demonstrates. In fact, using Corollary 1.5 it can also be shown that groups G for which $s(G)$ is close to $|G|^{1/4\log_2 |G|}$ are in a sense almost elementary abelian 2-groups.

We conclude the introduction with some words on the structure of this paper. In Section 2 we reduce Theorem 1.1 to Theorem 1.2, and Theorem 1.2 to Theorem 1.3. In Section 3 we essentially reduce the enumeration of maximal $\mathcal{F}$-subgroups of a finite group G to the case where G is almost simple. In Section 4 we enumerate maximal irreducible $\mathcal{F}$-subgroups of the group $\Gamma L_n(q)$ of semi-linear transformations, using Aschbacher's Theorem [1] as our main tool. This is where Theorem 1.3—and with it Theorems 1.2 and 1.1—are proved. Section 5 is devoted to the proof of Theorem 1.4 and Corollaries 1.5 and 1.6.

Notation

Let $q = p^n$, p a prime, let $\Gamma L_n(q)$ denote the extension of $GL_n(q)$ by the group of field automorphisms, and let $P\Gamma L_n(q)$ be the corresponding projective group. Then $\Gamma L_n(q)$ acts by semi-linear transformations on the vector space V of dimension n over $\mathbb{F}_q$.

For a finite group G, let $\mathcal{M}_{\mathcal{F}} = \mathcal{M}_{\mathcal{F}}(G)$ denote the set of maximal $\mathcal{F}$-subgroups of G, and let $\mu_{\mathcal{F}}(G) = |\mathcal{M}_{\mathcal{F}}|$ denote their number. When G is considered as a group of semi-linear transformations of a vector space or a permutation group (in some fixed representation) we denote by $\nu_{\mathcal{F}}(G)$ the number of maximal *irreducible* $\mathcal{F}$-subgroups in a semi-linear group G or the number of maximal *transitive* $\mathcal{F}$-subgroups in a permutation group G. This ambiguous convention will be used in a non-ambiguous way and it will always be clear from context which particular representation of G we are considering.

We will frequently use the following trivial observation: if $H \leqslant G$, then we have $\mu_{\mathcal{F}}(H) \leqslant \mu_{\mathcal{F}}(G)$. Indeed, with each subgroup $M \in \mathcal{M}_{\mathcal{F}}(H)$ we can associate a subgroup $N \in \mathcal{M}_{\mathcal{F}}(G)$ such that $N \geqslant M$. Then $M \leqslant H \cap N$ and since $H \cap N$ is an $\mathcal{F}$-subgroup we have equality (by the maximality of M). It follows that the correspondence $M \mapsto N$ is injective, which implies the claim. A similar observation holds when $\mu_{\mathcal{F}}$ is replaced by $\nu_{\mathcal{F}}$.

We denote by $S_{\mathcal{F}}(G)$ the $\mathcal{F}$-radical of G, i.e. the maximal normal $\mathcal{F}$-subgroup. Certainly when $\mathcal{F}$ is a class of all soluble groups, $S_{\mathcal{F}}(G) = S(G)$ is the usual soluble radical of G.

By a simple group we mean a nonabelian simple group. A quasi-simple group is a perfect group which is simple modulo its centre. An almost simple group is a group lying between a simple group and its group of automorphisms. The layer of G (the product of all quasisimple subnormal subgroups of G) is denoted by $L(G)$. Throughout this paper b, B, c, C represent constants (which sometimes depend on class $\mathcal{F}$), but their values may change according to the context.

2. Some reductions

In this section we reduce Theorem 1.1 to Theorem 1.3.

Given the class $\mathcal{F}$ (as in the introduction), let $\mathrm{Conj}_{\mathcal{F}}(n)$ be the number of conjugacy classes of maximal primitive $\mathcal{F}$-subgroups of Sym_n, and let $\mathrm{Ord}_{\mathcal{F}}(n)$ be the maximal order of such a subgroup. Let us say that an infinite group G is *an $\mathcal{F}$-group* if all finite images of G belong to $\mathcal{F}$.

Lemma 2.1. *With the above notation, let G be an r-generated $\mathcal{F}$-group. Then*

$$m_n(G) \leqslant n \cdot \mathrm{Conj}_{\mathcal{F}}(n) \cdot \mathrm{Ord}_{\mathcal{F}}(n)^{r-1}.$$

Proof. It is well known that $m_n(G)$ is equal to the number of homomorphisms $\phi : G \longrightarrow Sym_n$ with primitive image divided by $(n-1)!$. The image of any such homomorphism is a primitive $\mathcal{F}$-subgroup of Sym_n, which can be extended to a maximal primitive $\mathcal{F}$-subgroup. In order to bound m_n it therefore suffices to count homomorphisms from G to M, where M ranges over all maximal primitive $\mathcal{F}$-subgroups of Sym_n. Fix a conjugacy class C of such subgroups, and let m be the order of the subgroups in C. Then $M \in C$ can be chosen in at most $n!/m$ ways, and given M there are at most m^r homomorphisms from G to M. Since $n!/m \cdot m^r \leqslant n! \cdot \mathrm{Ord}_{\mathcal{F}}(n)^{r-1}$ we see that the number of homomorphisms from G to some maximal primitive $\mathcal{F}$-subgroup is at most $n!\mathrm{Conj}_{\mathcal{F}}(n)\mathrm{Ord}_{\mathcal{F}}(n)^{r-1}$. The result follows. □

Note that since every finite group is a subgroup of some alternating group Alt_n, there is a natural number d such that all groups in our class $\mathcal{F}$ are Alt_d-free. By the main result of Babai-Cameron-Pálfy [3] we have

$$\mathrm{Ord}_{\mathcal{F}}(n) \leqslant n^{c_1},$$

where c_1 depends on d (and thus on $\mathcal{F}$). Now, assuming $\mathrm{Conj}_{\mathcal{F}}(n) \leqslant n^{c_2}$ (where $c_2 = c_2(\mathcal{F})$ depends on $\mathcal{F}$), we obtain

$$m_n(G) \leqslant n \cdot n^{c_2} \cdot (n^{c_1})^{r-1} \leqslant n^{c_3},$$

for a suitable constant c_3. This completes the reduction of Theorem 1.1 to Theorem 1.2.

The following preliminary result, which enumerates maximal (possibly intransitive) $\mathcal{F}$-subgroups of Sym_n, will be needed in what follows.

Lemma 2.2. *Sym_n has at most C^n conjugacy classes of maximal $\mathcal{F}$-subgroups, where C is some absolute constant (not depending on $\mathcal{F}$).*

Proof. By [18, Lemma 2.1], Sym_n has at most $c_1^{\sqrt{n}\log^2 n}$ primitive subgroups up to conjugacy. In particular, this yields an exponential bound (say, c_2^n) on the number of conjugacy classes of maximal primitive $\mathcal{F}$-subgroups of S_n.

Now, if $H \leqslant Sym_n$ is a maximal $\mathcal{F}$-subgroup which is transitive but imprimitive, then H is a wreath product of maximal primitive $\mathcal{F}$-subgroups $P_1, \ldots, P_t$ where $P_i \leqslant S_{n_i}$ and $n_1 \cdots n_t = n$ (this can be seen by adapting the proof of [20, Ch. 4, §15, Theorem 4]). By the primitive case there are at most $c_2^{n_i}$ choices for $P_i \leqslant Sym_{n_i}$ up to conjugacy, and so, given the multiplicative partition $n_1, \ldots, n_t$ of n, H can be chosen in at most $\prod c_2^{n_i} = c_2^{\sum n_i} \leqslant c_2^n$ ways up to conjugacy. Since n has no more than n^2 multiplicative partitions, we obtain an $n^2 c_2^n \leqslant c_3^n$ bound on the number of choices for H up to conjugacy.

It remains to count $\mathcal{F}$-maximal subgroups H which are intransitive. By maximality we have $H = H_1 \times \cdots \times H_t$ where $n = n_1 + \cdots + n_t$ and for each i, $H_i \leqslant Sym_{n_i}$ is a maximal transitive $\mathcal{F}$-subgroup. Since each H_i can be chosen in at most $c_3^{n_i}$ ways up to conjugacy, we see that given the additive partition $n_1, \ldots, n_t$ of n, there are at most $c_3^{(n_1+\cdots+n_t)} = c_3^n$ choices for H up to conjugacy. Since n has less than 2^n additive partitions, we get a c_4^n upper bound on the number of choices for H up to conjugacy, where $c_4 = 2c_3$.

The result follows. □

Note that Lemma 2.2 extends [17, Lemma 3.2(iii)], yielding an exponential bound on the number of conjugacy classes of maximal soluble subgroups of Sym_n.

Let us now reduce Theorem 1.2 to Theorem 1.3. We first show that it suffices to count maximal *primitive* $\mathcal{F}$-subgroups of Sym_n. Our arguments are similar to those used in the proof of Lemma 2.1. Indeed, fix n and let H be a maximal transitive $\mathcal{F}$-subgroup of Sym_n. If H is imprimitive then it is the wreath product of maximal primitive $\mathcal{F}$-groups $P_1, \ldots, P_t$ where $P_i \leqslant S_{n_i}$ and $n_1 \cdots n_t = n$. Assuming Theorem 1.2 holds for primitive groups with an exponent c, we see that, given the multiplicative partition $n_1, \ldots, n_t$, each $P_i \leqslant Sym_{n_i}$ can be chosen in at most n_i^c ways up to conjugacy, and so H can be chosen in $n_1^c \cdots n_t^c = n^c$ ways up to conjugacy. Since n has no more than n^2 multiplicative partitions, it follows from the primitive case that H can be chosen in at most n^{c+2} ways up to conjugacy.

We need the following.

Lemma 2.3. (i) *Sym_n has at most $O(n)$ simple subgroups up to isomorphism.*

(ii) *Sym_n has at most $O(n \log^6 n)$ almost simple subgroups up to isomorphism.*

Proof. Clearly, Sym_n has at most $(n-4)+26$ simple subgroup of alternating or sporadic type. So it remains to count simple subgroups of Lie type. We use the

information on the minimal degrees of permutation representations of such groups, as presented in [8, p. 175] for the classical groups, and in [9] for exceptional groups. Let $T = X_k(q)$ be a group of Lie type of rank k over $\mathbb{F}_q$, and suppose $T \leqslant Sym_n$. Since the minimal degree of a permutation representation of G is at least bq^k, we obtain $n \geqslant bq^k$. It follows that $k \leqslant O(\log n)$ and that, given k, there are $O(n^{1/k})$ possibilities for q. Now, if q and k are given, there are at most 7 possibilities for the simple group T (up to isomorphism). We conclude that the number of simple subgroups $T \leqslant Sym_n$ of Lie type is of the form

$$O(\sum_{k=1}^{\log n} n^{1/k}) \leqslant O(n + \sqrt{n}\log n) = O(n).$$

Part (i) follows.

To prove part (ii), let $H \leqslant Sym_n$ be almost simple, and let $T = Soc(H)$. Suppose T is given. If T is alternating, then there are only 2 choices for H. Suppose T is of Lie type, then the information on the minimal degree of T yields $|T| \leqslant C^{\log^2 n}$, so $|Out(T)| \leqslant \log|T| \leqslant O(\log^2 n)$. By [6], every subgroup of $Out(T)$ can be generated by 3 elements. It follows that $Out(T)$ has at most $|Out(T)|^3 \leqslant O(\log^6 n)$ subgroups. This shows that given T, there are at most $O(\log^6 n)$ choices for H. Part (ii) now follows by applying part (i). □

We now reduce Theorem 1.2 for primitive groups to Theorem 1.3, using [16] as the main tool. Let $H \leqslant Sym_n$ be a maximal primitive $\mathcal{F}$-subgroup. We distinguish between the following possibilities, according to the O'Nan-Scott Theorem (see [10]).

Case 1. H is of affine type.

Then $n = p^k$ and the socle of H is an elementary abelian p-group of rank k. Counting the possibilities for H up to conjugacy in Sym_n is equivalent to counting conjugacy classes of maximal irreducible $\mathcal{F}$-subgroups of $GL_k(p)$. Assuming Theorem 1.3 holds, there are at most $p^{ck} = n^c$ such conjugacy classes (where $c = c(\mathcal{F})$). This concludes the argument in the affine case.

In the remaining cases H has nonabelian socle, say $Soc(H) = T^k$ for some $k \geqslant 1$ and a nonabelian simple group T.

Case 2. H is of a wreath product type (with the product action).

Then, by maximality, $H = H_1 \wr H_2$ where $H_i \leqslant Sym_{n_i}$ and $n_1^{n_2} = n$. Moreover, H_1 is a maximal primitive $\mathcal{F}$-subgroup of Sym_{n_1} and so by induction it can be chosen in at most n_1^c ways up to conjugacy in Sym_{n_1}. Now, H_2 is a maximal transitive $\mathcal{F}$-subgroup of Sym_{n_2}, so by induction on n and by the above reduction to the primitive case, H_1 has at most n_2^{c+2} possibilities up to conjugacy. It follows that given $n_1, n_2 > 1$ with $n_1^{n_2} = n$, H can be chosen in at most $n_1^c n_2^{c+2}$ ways up to conjugacy. Clearly, $n_2 \leqslant \log n$ and $n_1 \leqslant n^{1/2}$. Thus

$$n_1^c n_2^{c+2} \leqslant n^{c/2}(\log n)^{c+2} \leqslant n^c/\log n,$$

if we assume c is large enough. Since there are no more than $\log n$ choices for n_1, n_2, we see that there are at most n^c choices for H up to conjugacy.

Case 3. H is of a diagonal type.

Recall that $Soc(H) = T^k$. By Lemma 2.3, Sym_n has at most $O(n)$ simple subgroups up to isomorphism. Thus T can be chosen in at most $O(n)$ ways. Given T, k is determined since $|T|^{k-1} = n$. So suppose $Soc(H) = T^k$ is given as an abstract

group. Then T^k has $|Out(T)^{k-1}| \leqslant |T|^{k-1} = n$ conjugacy classes of diagonal subgroups D. Given the conjugacy class of D, the permutation representation of T^k in Sym_n (with D as a point-stabilizer) is determined up to conjugacy. This shows that there are at most $O(n^2)$ choices for $Soc(H) \leqslant Sym_n$ up to conjugacy. Given the embedding of $Soc(H)$ in Sym_n we have $T^k \leqslant H \leqslant N_{Sym_n}(T^k) = T^k.(Sym_k \times Out(T))$, and so it remains to bound the number of conjugacy classes of maximal $\mathcal{F}$-subgroups of $Sym_k \times Out(T)$. Since $Out(T)$ is soluble, and $\mathcal{F}$ is extension-closed and contains all finite soluble groups, every maximal $\mathcal{F}$-subgroup of $Sym_k \times Out(T)$ contains $Out(T)$, and so we are reduced to counting maximal $\mathcal{F}$-subgroups of Sym_k up to conjugacy. By Lemma 2.2 there are at most C^k such subgroups up to conjugacy where C is an absolute constant. Note that $k \leqslant \log n$. Putting everything together it follows that there are $O(n^2 C^{\log n})$ choices for H up to conjugacy, and this expression is bounded above by n^c for large enough c.

Case 4. H is of a twisted wreath product type.

Then G has a unique minimal normal subgroup, say N, and N is regular and nonabelian. Set $C = C_{S_n}(N)$. Note that the normalizer of N in Sym_n normalizes C, and so G normalizes C. Now, $C \cong N$ and so $C \in \mathcal{F}$. It follows GC is an $\mathcal{F}$-subgroup of Sym_n, so $G = GC$ by maximality. This shows that $C \leqslant G$. Clearly, N and C are minimal normal subgroups of G, and $N \neq C$ (since N is nonabelian). This contradicts the fact that N is the unique minimal normal subgroup of G. In other words, we have shown that maximal primitive $\mathcal{F}$-subgroups of Sym_n cannot be of twisted wreath product type.

Case 5. H is almost simple.

Lemma 2.3 implies that as an abstract group, $H \leqslant Sym_n$ can be chosen in at most n^{c_1} ways. Now, by Theorem 1.1 of [16], an almost simple group has at most n^{c_2} maximal subgroups of index n. This shows that the abstract group H has at most n^{c_2} primitive representations of degree n, and so the number of choices for $H \leqslant Sym_n$ up to conjugacy is $\leqslant n^{c_1+c_2}$. This completes the proof.

3. Reduction Lemmas

For a subgroup H of a finite group G denote $Aut_G(H) = N_G(H)/C_G(H)$. Obviously $Aut_G(H)$ is naturally embedded into $Aut(H)$.

The following fact is well-known.

Lemma 3.1. *Let G be a finite group with $S(G) = 1$. Set $L = L(G)$. Then $L = L_1 \times \cdots \times L_k$, where L_i are simple and $C_G(L) = 1$, i.e. G has a natural embedding into $Aut(L)$. Denote $Aut_G(L_i)$ by A_i and $\prod_{i=1}^k Aut_G(L_i)$ by A. Then A is a subgroup of $Aut(L)$ normalized by $G \leqslant Aut(L)$ and the factor group AG/A acts faithfully as a group permuting the subgroups L_i.*

Lemma 3.2. *Suppose, under the assumptions of Lemma 3.1, that $G \geqslant A$ and G/A is a $\mathcal{F}$-group. Then for $M \in \mathcal{M}_{\mathcal{F}}(G)$ we have*

(i) $M_i = M \cap A_i \in \mathcal{M}_{\mathcal{F}}(A_i)$.
(ii) $M \cap A = \prod_{i=1}^k M_i$.
(iii) $M = N_G(M \cap A)$.

Proof. In its natural action by conjugation, M permutes the subgroups L_i. Take an orbit, say $L_1, \ldots, L_t$. Take elements $g_1 = 1, g_2, \ldots, g_t$ such that $L_i = L_1^{g_i}$, $i = 1, \ldots, t$. The subgroup $N_M(L_1)$ acts on L_1 by conjugation and induces a subgroup P_1 of $A_1 = Aut_G(L_1)$.

Let $M_1 \in \mathcal{M}_{\mathcal{F}}(A_1)$ contain P_1. Consider the subgroup

$$N = M_1 \times M_1^{g_2} \times \cdots \times M_1^{g_t}.$$

We claim that M normalizes N. Indeed, if $h \in N_M(L_1)$, then h acts on $Aut_G(L_1)$ as an element of P_1, therefore $M_1^h = M_1$. If now g is an arbitrary element of M, then it can be written as $g = hg_i$ for some $i = 1, \dots, t$, so $M_1^g = M_1^{hg_i} = M_1^{g_i} \leqslant N$. This means that the group N is generated by all subgroups conjugate to M_1 by elements from M, which proves the claim.

Now NM is an $\mathcal{F}$-subgroup, therefore $NM = M$ and $N \leqslant M$, which proves (i) and (ii).

The subgroup $M \cap A$ is a maximal $\mathcal{F}$-subgroup of A, hence is self-normalizing in A. As G/A is a $\mathcal{F}$-group, it follows that $N_G(M \cap A) \leqslant M$. But $M \cap A \trianglelefteq M$ and therefore (iii) follows. □

Corollary 3.3. *Assume that $S_{\mathcal{F}}(G) = 1$, $G/L(G)$ is an $\mathcal{F}$-group and also that $L(G) = L_1 \times \cdots \times L_k$ for simple subgroups L_i. Then*

$$\mu_{\mathcal{F}}(G) \leqslant \prod_{i=1}^{k} \mu_{\mathcal{F}}(Aut_G(L_i)).$$

Proof. Consider the subgroup AG of $Aut(L(G))$. It satisfies the conditions of Lemma 3.2, therefore

$$\mu_{\mathcal{F}}(AG) \leqslant \prod_{i=1}^{k} \mu_{\mathcal{F}}(Aut_G(L_i)).$$

But $\mu_{\mathcal{F}}(G) \leqslant \mu_{\mathcal{F}}(AG)$ and this proves our statement. □

Now, let T be a nonabelian composition factor of G and suppose T does not belong to $\mathcal{F}$. It is easy to see that T is naturally isomorphic to one of the sections of G obtained in the following process. Let $F_0 = H_0 = 1$, $H_1 = S_{\mathcal{F}}(G)$, F_1 the preimage in G of $L(G/S_{\mathcal{F}}(G))$ and for $i > 1$ set H_i to be equal to the preimage of $S_{\mathcal{F}}(G/F_{i-1})$ in G and F_i the preimage of $L(G/H_i(G))$ in G. The nonabelian simple normal subgroups of F_i/H_i are called *distinguished simple sections of G*. Clearly, every nonabelian composition factor which is not in $\mathcal{F}$ is naturally isomorphic to a distinguished simple section of G. If $T \trianglelefteq F_i/H_i$ is one of the distinguished simple sections we set $Aut_G(T) = Aut_{G/H_i}(T)$.

Lemma 3.4 (Reduction Lemma)**.** *Let G be an arbitrary finite group. Then*

$$\mu_{\mathcal{F}}(G) \leqslant \prod \mu_{\mathcal{F}}(Aut_G(T_i)),$$

where T_i ranges over the set of all distinguished simple sections of G.

Proof. It suffices to show this for groups G with $S_{\mathcal{F}}(G) = 1$.

If $S_{\mathcal{F}}(G) = 1$, then $L(G) = F_1(G)$ and by induction the number of subgroups X in $\mathcal{M}_{\mathcal{F}}(G/L(G))$ is at most $\prod \mu_{\mathcal{F}}(Aut_G(T_i))$, where T_i ranges over all distinguished simple sections of $G/L(G)$ (which, together with simple normal subgroups of $L(G)$, constitute all the distinguished simple sections of G). If $\overline{X}$ is the preimage of X in G, then $\overline{X}$ satisfies the conditions of Corollary 3.3. Since each subgroup $M \in \mathcal{M}_{\mathcal{F}}(G)$ is mapped onto a subgroup of some $X \in \mathcal{M}_{\mathcal{F}}(G/L(G))$, Lemma 3.4 follows at once. □

On several occasions we shall use the Reduction Lemma in the following simplified form.

Lemma 3.5. *Let H be an almost simple group. Then*

$$\mu_{\mathcal{F}}(H \wr Sym_n) \leqslant \mu_{\mathcal{F}}(H)^n \cdot \mu_{\mathcal{F}}(Sym_n).$$

Proof. If $G = H \wr Sym_n$, then $L(G) = F^*(G) = L_1 \times \cdots \times L_n$, where, for all i, $L_i \cong L = L(H)$. Let $B \cong H \times \cdots \times H$ (n copies) be the base subgroups of the wreath product $B \wr Sym_n$, then $G = B \rtimes X$ for $X \cong Sym_n$. Since $N_G(L_i) = B \cdot X_i$, where $X_i \cong Sym_{n-1}$ is the stabilizer in $X = Sym_n$ of the point i, and $[L_i, X_i] = 1$, obviously $Aut_G(L_i) = N_G(L_i)/C_G(L_i) \cong H$.

If $Alt_n \notin \mathcal{F}$ then we have one more distinguished simple section of G, namely $T = L(G/B) \cong Alt_n$, and obviously $Aut_G(T) = G/B \cong Sym_n$. Now Lemma 3.5 follows at once from the Reduction Lemma. □

We need one more version of the Reduction Lemma, which deals with groups of semi-linear transformations. Let $\Gamma = \Gamma L_n(q)$. We are interested in the number $\nu_{\mathcal{F}}(G)$ of maximal irreducible $\mathcal{F}$-subgroups in certain subgroups G of Γ. Namely, consider the decomposition $V = V_1 \oplus \cdots \oplus V_t$ or $V = V_1 \otimes \cdots \otimes V_t$ into a direct or tensor product of isomorphic subspaces V_i, $i = 1, 2, \ldots, t$, of dimension a over $\mathbb{F}_q$ (correspondingly $n = at$ or $n = a^t$). The stabilizer G of this decomposition in Γ is isomorphic to

$$(GL_a(q) \circ \cdots \circ GL_a(q)) \rtimes (Sym_t \times \Lambda),$$

where Sym_t permutes t copies of $GL_a(q)$ in the central product and $\Lambda = Aut(\mathbb{F}_q)$ acts as the group of field automorphisms simultaneously on each copy of $GL_a(q)$.

Lemma 3.6. *Under the above assumptions,*

$$\nu_{\mathcal{F}}(G) \leqslant \nu_{\mathcal{F}}(\Gamma L_a(q))^t \cdot \nu_{\mathcal{F}}(Sym_t).$$

Proof. Follows the lines of the proof for Lemma 3.2. Obviously $L(G) = L_1 \circ \cdots \circ L_t$, where $L_i \cong SL_a(q)$ acts on V_i. Notice that $Aut_G(L_i) \cong P\Gamma L_a(q)$. Let K be the kernel of the action of G by permutation on the set $\{V_1, \ldots, V_t\}$. Then, obviously, $G/K \cong Sym_t$. Now if M is a maximal irreducible $\mathcal{F}$-subgroup of G, then its image in G/K is a transitive subgroup of Sym_t and the group P_1 induced on L_1 by the action of $N_M(L_1)$ is an irreducible (in the sense of semi-linear action) subgroup of $P\Gamma L_a(q)$. In view of these remarks we can easily adopt the arguments from Lemma 3.2, Corollary 3.3, the Reduction Lemma and Lemma 3.5. □

4. Proof of Theorem 1.3

The main result of this section is as follows.

Theorem 4.1. *There is a constant C which depends only on $\mathcal{F}$ such that, for $G = \Gamma L_n(q)$,*

$$\nu_{\mathcal{F}}(G) \leqslant q^{Cn} \cdot |GL_n(q)|.$$

The following result, which is our main tool in this section, is a simplified version of Aschbacher's Reduction Theorem for subgroups of finite classical groups [1]. Its proof can be easily extracted from the proof of Theorem Γ in [1]; our notation is slightly different from that of [1].

Theorem 4.2. *Let H be an irreducible subgroup of $G = \Gamma L_n(q)$, $q = p^e$, p prime. Denote by V the underlying vector space over $\mathbb{F}_q$ for $GL_n(q)$. Notice that G acts on V by semi-linear transformations. Then either*

(S): $S \leqslant H \leqslant N_G(S)$ for a quasi-simple irreducible subgroup S.

or H lies in a subgroup M of one of the following types.

(C2): *The stabilizer of a direct sum decomposition:*

$$M = (GL_a(q) \wr Sym_t).\Lambda,$$

where $n = at$ and $\Lambda \cong \mathbb{Z}_e$ is the group of field automorphisms.

(C4): *The stabilizer of a tensor product decomposition $V = V_1 \otimes V_2$:*

$$M = (GL_a(q) \circ GL_b(q)).\Lambda,$$

where $n = ab$ and a cyclic group Λ is induced by the field automorphisms of $GL_n(q)$.

(C6): *The group M is either the normalizer of a symplectic-type r-group (r prime) in an irreducible representation over $\mathbb{F}_{q^k}$,*

$$M = (\mathbb{Z}_{q^k-1} \circ r^{1+2a}).Sp_{2a}(r).C$$

where $n = r^a k$ and C is a cyclic subgroup of field automorphisms of $\mathbb{F}_{q^k}$, or the normalizer of the Zinger cycle $Z = \mathbb{Z}_{q^n-1}$; in the latter case M is a soluble group.

(C7): *Stabilizer of a tensor decomposition $V = \bigotimes_{i=1}^{t} V_i$:*

$$M = (GL_a(q) \circ \cdots \circ GL_a(q)) \rtimes (Sym_t \times \Lambda),$$

where $n = a^t$ and Λ is induced by field automorphisms of $GL_n(q)$.

Remark 4.1. Note that since we deal with irreducible subgroups, Aschbacher's class (C1) of parabolic subgroups does not occur. Also we require from the groups of our class (S) no further properties but irreducibility. This allows us to ignore the further subdivision of our class (S) and make redundant cases (C3), (C5) and (C8) in Aschbacher's Theorem.

Lemma 4.3 is a version of an estimate from [7] (see also Theorem 5.2.4 in [8]).

Lemma 4.3. *Let ν_{except} denote the number of irreducible projectively simple $\mathcal{F}$-subgroups S of $G = P\Gamma L_n(q)$. Then there exists a constant c_{except} which depends only on $\mathcal{F}$ such that*

$$\nu_{except} \leqslant q^{c_{except} n}|G|.$$

Proof. Recall that there is a constant d such that all groups in $\mathcal{F}$ are Alt_d-free. By [3] there is a constant c' which depends only on d and such that $|S| \leqslant q^{c'n}$. Now we can repeat the arguments of [7, p. 69]. Indeed, the number of possible simple subgroups S of a given order s is itself $\leqslant 2$ (by the classification of finite simple groups). Fix such a simple group S. Let $\overline{S}$ be its covering group. Then $|\overline{S}| \leqslant |S| \log |S|$ and the number of (equivalence classes of) absolutely irreducible projective representations of S in characteristic p is at most $|\overline{S}|$. Combining these inequalities we easily obtain that the number of absolutely irreducible projectively simple $\mathcal{F}$-subgroups of $P\Gamma L_n(q)$ is $\leqslant q^{cn}$ for some constant c. Irreducible, but not absolutely irreducible subgroups of $P\Gamma L_n(q)$ correspond to absolutely irreducible

subgroups of $P\Gamma L_a(q^b)$ with $ab = n$. Thus the desired estimate for the number of irreducible simple $\mathcal{F}$-subgroups boils down to

$$\sum_{ab=n} q^{b\cdot ca} = (\text{number of divisors of } n)\cdot q^{cn} \leqslant q^{c_{except}n}$$

for an appropriate constant c_{except}. □

Proof of Theorem 4.1. We will be looking for a bound for $\nu_{\mathcal{F}}(G)$ in the form

$$\nu_{\mathcal{F}}(G) \leqslant q^{f(n)}|G|$$

where f is some function. The idea is to obtain a recursive relation for $f(n)$ and then to conclude from it that f can actually be taken to be a linear function of the form $f(n) = B\cdot(n-1)$, where B is a large constant. Finally we notice that $|G| \leqslant |GL_n(q)|\cdot\log q$ and thus

$$\nu_{\mathcal{F}}(G) \leqslant q^{C\cdot n}|GL_n(q)|$$

for a slightly larger constant $C > B$.

Let H be a maximal irreducible $\mathcal{F}$-subgroup of $G = \Gamma L_n(q)$, $q = p^e$, p prime. Notice that H is self-normalizing, $H = N_G(H)$. Denote by V the underlying vector space over $\mathbb{F}_q$ for $GL_n(q)$. Notice that G acts on V by semi-linear transformations. Also H satisfies one of the clauses (S), (C2), (C4), (C6), (C7) of Theorem 4.2.

We start our analysis with the first possibility for H when it lies in the "exceptional class" (S). Since $H = N_G(S)$ in this case, it suffices to count the number of choices for the quasi-simple irreducible subgroup S, and this can be done using Lemma 4.3. It follows that the number ν_{except} of subgroups H satisfying (S) is bounded by

$$\nu_{except} \leqslant q^{c_{except}n}|G|$$

for some absolute constant c_{except}.

The next possibility is that H lies in the normalizer of one of the irreducible symplectic-type r-subgroups in G, or in the normalizer of a Zinger cycle $Z < G$ (as in case (C6)). Note that in the latter case we have $H = N_G(Z)$ by maximality (as the group on the right hand side is soluble), and so H can be chosen in at most $|G|$ ways.

We find that the number $\nu_{(C6)}$ of subgroups H in this case is bounded by

$$\begin{aligned}\nu_{(C6)} &\leqslant \sum_{r^a|n}\frac{|G|}{|M|}\cdot\mu_{\mathcal{F}}(Aut(Sp_{2a}(r))) + |G| \\ &\leqslant \sum_{r^a|n}\frac{|G|}{r^{2a+1}|Sp_{2a}(r)|}\cdot\mu_{\mathcal{F}}(Aut(Sp_{2a}(r))) + |G|.\end{aligned}$$

Now we can roughly estimate $\mu_{\mathcal{F}}(Aut(Sp_{2a}(r)))$. Since $r^a \leqslant n$, the order of $Aut(Sp_{2a}(r))$ is about $r^{(2a)^2} \sim n^{\log n}$. A finite group of order g has less than $g^{\log g}$ subgroups, therefore $Aut(Sp_{2a}(r))$ has less than $(n^{\log n})^{\log(n^{\log n})} = n^{\log^3 n}$ subgroups, which can be bounded by c^n for some absolute constant c. In view of our upper bound on $\nu_{(C6)}$ we easily conclude that

$$\nu_{(C6)} \leqslant c_{sympl}^n|G|$$

for some absolute constant c_{sympl}.

So we need only to consider the generic case when H is a proper subgroup in a subgroup M of one of the following types.

(C2): The stabilizer of a direct sum decomposition:

$$H \leqslant M = (GL_a(q) \wr Sym_t)\Lambda,$$

where $at = n$.

(C4): The stabilizer of a tensor product decomposition $V = V_1 \otimes V_2$:

$$H \leqslant M = (GL_a(q) \circ GL_b(q))\Lambda,$$

where $ab = n$.

(C7): The stabilizer of a tensor decomposition $V = \bigotimes_{i=1}^{t} V_i$:

$$H \leqslant M = (GL_a(q) \circ \cdots \circ GL_a(q)) \rtimes (Sym_t \times \Lambda),$$

where $a^t = n$.

One can easily notice that in the case (C2) the number $\nu_{(C2)}$ of the maximal irreducible $\mathcal{F}$-subgroups in G corresponding to one class of conjugate subgroups of type (C2) can be estimated by Lemma 3.6 and induction as

$$\begin{aligned}
\nu_{\mathcal{F}}(\Gamma L_a(q))^t \cdot \nu_{\mathcal{F}}(Sym_t) \cdot \frac{|G|}{|M|} &\leqslant (q^{f(a)} \cdot |\Gamma L_a(q)|)^t \cdot (c_{sym}^t |Sym_t|) \cdot \frac{|G|}{|M|} \\
&\leqslant (q^{f(a)t} c_{sym}^t (\log q)^t)|M| \frac{|G|}{|M|} \\
&\leqslant (q^{f(a)t} c_{sym}^t (\log q)^t)|G|.
\end{aligned}$$

We have used here a bound of the form

$$\nu_{\mathcal{F}}(Sym_t) \leqslant \mu_{\mathcal{F}}(Sym_t) \leqslant c_{sym}^t |Sym_t|,$$

which follows from Lemma 2.2. Thus the number $\nu_{(C2)}$ of maximal irreducible $\mathcal{F}$-subgroups in G produced by subgroups of type (C2) can be estimated as

$$\nu_{(C2)} \leqslant \sum_{at=n} (q^{f(a)t} c_{sym}^t (\log q)^t)|G|.$$

Analogously we have for types (C4) and (C7) the following share of maximal irreducible $\mathcal{F}$-subgroups:

$$\nu_{(C4)} \leqslant \sum_{ab=n} q^{f(a)+f(b)}|G|$$

and

$$\nu_{(C7)} \leqslant \sum_{a^t=n} q^{f(a)t} c_{sym}^t (\log q)^t |G|.$$

Combining these inequalities and summing up over all conjugacy classes of subgroups in the classes (S), (C2), (C4), (C6) and (C7), we obtain the following estimate.

$$\begin{aligned}\frac{\nu_{\mathcal{F}}(G)}{|G|} &\leqslant q^{c_{except}n} \\ &\quad + c^n_{sympl} \\ &\quad + \sum_{at=n} q^{f(a)t} c^t_{sym} (\log q)^t \\ &\quad + \sum_{ab=n} q^{f(a)+f(b)} \\ &\quad + \sum_{a^t=n} q^{f(a)t} c^t_{sym} (\log q)^t.\end{aligned}$$

We need to show that this sum is $\leqslant q^{f(n)}$. It is obvious that this inequality is satisfied by a large enough linear function $f(n) = B \cdot (n-1)$. □

Proof of Theorem 1.3. By [3] there is a constant $b = b(\mathcal{F})$ such that if H is any maximal irreducible $\mathcal{F}$-subgroup of $G = GL_n(q)$, then $|H| \leqslant q^{bn}$. Since H is self-normalizing, this implies that H has at least $|G|/q^{bn}$ conjugates in G. Now, in view of Theorem 4.1, we have $\nu_{\mathcal{F}}(\Gamma L_n(q)) \leqslant q^{Cn}|G|$, and we clearly have the bound $\nu_{\mathcal{F}}(G) \leqslant \nu_{\mathcal{F}}(\Gamma L_n(q))$. Therefore the group G has at most $q^{Cn}|G|$ maximal irreducible $\mathcal{F}$-subgroups. Since each conjugacy class of such subgroups has size at least $|G|/q^{bn}$, we deduce that G has at most $q^{(C+b)n}$ conjugacy classes of maximal irreducible $\mathcal{F}$-subgroups. This completes the proof. □

5. Applications

In this section we draw several important corollaries from Theorem 4.1 above. In particular, we prove that there is a constant c (which depends only on class $\mathcal{F}$) such that for any finite group G, $\mu_{\mathcal{F}}(G) \leqslant |G|^c$ (see Theorem 5.4 below).

Corollary 5.1. *There is a constant C such that*

$$\mu_{\mathcal{F}}(\Gamma L_n(q)) \leqslant q^{Cn^2}.$$

and

$$\mu_{\mathcal{F}}(Aut(PSL_n(q))) \leqslant q^{2Cn^2}.$$

Proof. To prove the first inequality we have to count maximal $\mathcal{F}$-subgroups of $G = \Gamma L_n(q)$ which are not necessarily irreducible. If H is such a subgroup, then H lies in some parabolic subgroup. Let P be a minimal parabolic subgroup containing H. Since H is a maximal $\mathcal{F}$-subgroup of P, it must contain the unipotent radical N of P, and H/N is a maximal $\mathcal{F}$-subgroup of the Levi factor $L = P/N$. If $V_1, \dots, V_t \leqslant V$ are the composition factors of the natural module V as a P-module, then H/N acts irreducibly on each V_i, and we have (in the usual notation)

$$L \cong (GL(V_1) \circ \cdots \circ GL(V_t)) \rtimes (\Lambda).$$

It is now easy to see that H/N has the form $N_L(K)$, where $K = K_1 \times \cdots \times K_t$, and each K_i is a maximal *irreducible* $\mathcal{F}$-subgroup of $GL(V_i)$. Using Theorem 4.1 we see that there are at most $q^{Cn_i}|GL_{n_i}(q)|$ choices for K_i, where $n_i = \dim V_i$, and since $\sum n_i = n$, H can be chosen in at most $q^{Cn}|G|$ ways, given P. Finally, it is well known that the number of conjugacy classes of parabolic subgroups of $G = \Gamma L_n(q)$ is bounded by an exponential function of n. Hence the total number of maximal

$\mathcal{F}$-subgroups of G is at most $c^n|G| \cdot q^{Cn}|G|$, which is bounded by a polynomial function of $|G|$. This completes the proof of the first inequality.

The proof of the second inequality is easier. Note that

$$Aut(PSL_n(q)) = P\Gamma L_n(q).\mathbb{Z}_2$$

(where $\mathbb{Z}_2$ is generated by the inverse-transpose automorphism), and so we have from Lemma 3.5

$$\mu_{\mathcal{F}}(Aut(PSL_n(q))) \leqslant \mu_{\mathcal{F}}(P\Gamma L_n(q) \wr \mathbb{Z}_2) \leqslant \mu_{\mathcal{F}}(P\Gamma L_n(q))^2 \leqslant q^{2Cn^2}.$$

□

Corollary 5.2. *There are constants D and E such that for simple classical linear groups $G = PSL_n(q), PSp_{2n}(q), PSU_n(q^2), P\Omega_n^{\pm}(q)$ we have*

$$\mu_{\mathcal{F}}(Aut(G)) \leqslant q^{Dn^2}$$

and

$$\mu_{\mathcal{F}}(G) \leqslant |G|^E.$$

Proof. It is well-known that the group $Aut(G) = G_1 \rtimes \Gamma$, where G_1 is generated by inner, diagonal and field automorphisms and Γ is the group of graph automorphisms [5]. Notice also that G_1 is a subgroup of $Aut(PSL_n(q))$ ($Aut(PSL_n(q^2))$ in the case of $G = PSU_n(q^2)$) and Γ is a subgroup of Sym_3. Thus $Aut(G)$ is a subgroup of $Aut(PSL_n(q)) \wr Sym_3$ (replace q by q^2 for the unitary group, here and in the further arguments) and, by Corollary 5.1 and Lemma 3.5,

$$\mu_{\mathcal{F}}(Aut(G)) \leqslant \mu_{\mathcal{F}}(Aut(PSL_n(q)) \wr Sym_3) \leqslant \mu_{\mathcal{F}}(Aut(PSL_n(q)))^6 \leqslant q^{Dn^2},$$

for a constant $D = 12C$ (or $24C$ in the case of $PSU_n(q)$). The second inequality follows easily from the well-known formulas for the orders of G. □

A modification of the same argument yields an analogous estimate for all simple finite groups of Lie type:

Corollary 5.3. *Let L be a simple group of Lie type. Then*

$$\mu_{\mathcal{F}}(Aut(L)) \leqslant |L|^C$$

for some constant C which does not depend on L (but depends on $\mathcal{F}$).

Proof. In view of the previous corollary we have to consider only the case of exceptional (E_6, E_7, E_8, F_4 and G_2) and non-classical twisted (${}^2E_6$, ${}^3D_4$, ${}^2G_2$ and ${}^2F_4$) series of groups of Lie type. In particular, we can assume that the Lie rank of L is bounded (by $\leqslant 8$).

First note that if L is a group of a twisted Lie type, then L is a subgroup of the group of fixed points of an automorphism of order 2 or 3 in a group L_1 of a non-twisted Lie type over a field of order q^2 or q^3, correspondingly, for some $q = p^n$ (for example, $L = {}^2G_2(q^2)$ in $L_1 = G_2(q^2)$).

Notice that the orders of L and L_1 are polynomials in q; since we have only finitely many such polynomials, we can conclude without further elaboration that, for some constant c, $|L_1| < |L|^c$. Also we have from the construction of the automorphism groups for L and L_1 that $Aut(L) \leqslant Aut(L_1)$. Thus if $\mu_{\mathcal{F}}(Aut(L_1))$ is bounded by $|L_1|^C$ for some C, then $\mu_{\mathcal{F}}(Aut(L)) \leqslant \mu_{\mathcal{F}}(Aut(L_1))$ is bounded by $|L|^{cC}$.

For this reason it is enough for our purposes to consider only non-twisted groups. All of them can be obtained by the following construction.

Let G be a simple algebraic group of adjoint type defined over a prime field $\mathbb{F}_p$. Let $G(\mathbb{F}_q)$ be its group of points over $\mathbb{F}_q$, $q = p^n$, and $L = O^{p'}(G(\mathbb{F}_q))$. Then L is a finite simple group of Lie type (with a small number of soluble exceptions). Notice that L acts on its Lie algebra $Lie(L)$ which is a vector space of dimension $m = dim(G)$ over $\mathbb{F}_q$.

It is also important that the order of L is a polynomial in q of degree $m = dim(G)$. In all cases $m \leqslant 248$.

Now consider the structure of $Aut(L)$. Notice that the so-called 'field' automorphisms of L are induced by the automorphisms of $\mathbb{F}_q$. We know further that $Aut(L) = L_1 \rtimes \Lambda$, where L_1 is the group generated by inner, diagonal and graph automorphisms and Λ is the group of field automorphisms. In all cases $L_1 \leqslant Aut_{\mathbb{F}_q}(Lie(L)) \leqslant GL_m(q)$ and $Aut(L) \leqslant \Gamma L_m(q)$.

Now $\mu_{\mathcal{F}}(Aut(L)) \leqslant \mu_{\mathcal{F}}(\Gamma L_m(q))$ is bounded, in view of Corollary 5.1, by a polynomial in q. Since $|L|$ is bounded by another polynomial in q, the result follows immediately. □

We can now obtain the main result of this section.

Theorem 5.4. *There is a constant C (which depends only on $\mathcal{F}$) such that for any finite group G*

$$\mu_{\mathcal{F}}(G) \leqslant |G|^C.$$

Proof. By the Classification Theorem for Finite Simple Groups every non-abelian composition factor S of G is either a group of Lie type, or an alternating group, or one of the 26 sporadic groups. In the case of a group of Lie type $\mu_{\mathcal{F}}(Aut(S)) \leqslant |S|^C$ for some constant C which depends only on $\mathcal{F}$. If S is alternating, we have an even better bound in view of Lemma 2.2. Since the number of sporadic groups is finite, we have, after appropriately increasing the constant C, that $\mu_{\mathcal{F}}(Aut(S)) \leqslant |S|^C$ for all non-abelian composition factors S of G. Now the result follows immediately from the Reduction Lemma. □

Proof of Theorem 1.4. This is just a special case of Theorem 5.4, where $\mathcal{F}$ is the class of finite soluble groups. □

Proof of Corollary 1.5. By [2] every finite group is generated by a soluble subgroup and another element. Therefore the number of subgroups $s(G)$ of G is bounded by $s_{sol}(G) \cdot |G|$, where $s_{sol}(G)$ denotes the number of soluble subgroups of G. Now, every soluble subgroup of G is a subgroup of some maximal soluble subgroup M of G, and G has at most $|G|^c$ maximal soluble subgroups. Therefore $s_{sol}(G) \leqslant N \cdot |G|^c$ where $N = \max\{s(H) : H \leqslant G \text{ is soluble}\}$. Let H be a soluble subgroup of G. Then H has a Hall system of pairwise commuting Sylow subgroups $\{H_p : p||G|\}$, and every subgroup of H is conjugate to a product of subgroups of H_p for the various primes p. We see that

$$s(H) \leqslant |H| \cdot \prod_p s(H_p) \leqslant |G| \prod_p s(G_p).$$

Therefore $N \leqslant |G| \prod_p |G_p|$ and the result follows. □

Proof of Corollary 1.6. By [19, Lemma 4.2], a group of order p^n (p prime) has at most $4p^{k(n-k)}$ subgroups of order p^k. Summing up over $k = 0, \dots, n$ we obtain

$$|G| = p^n \Rightarrow s(G) \leqslant b \cdot p^{n^2/4} = b \cdot |G|^{1/4 \log_p |G|},$$

where b is some absolute (small) constant. Combining this inequality with Corollary 1.5 we see that, if G is any finite group, then

$$\begin{aligned} s(G) &\leqslant |G|^{c+1} \prod_p b |G_p|^{1/4 \log_p |G_p|} \\ &\leqslant |G|^{c+1} \cdot b^{l(|G|)} \cdot \prod_p |G_p|^{1/4 \log_2 |G|}, \end{aligned}$$

where $l(m)$ is the number of distinct prime divisors of m. It is quite obvious that $b^{l(|G|)} \leqslant |G|^{o(1)}$, and so we have

$$s(G) \leqslant |G|^{c+1+o(1)+1/4 \log_2 |G|} \leqslant |G|^{(1/4+o(1)) \log_2 |G|},$$

as required. □

References

1. M. Aschbacher, *On the maximal subgroups of the finite classical groups*, Invent. Math. **76** (1984), 469–514. MR **86a:**20054
2. M. Aschbacher and R. Guralnick, *Solvable generation of groups and Sylow subgroups of the lower central series*, J. Algebra **77** (1982), 189–201. MR **84c:**20025
3. L. Babai, P. J. Cameron, P. P. Pálfy, *On the orders of primitive permutation groups with restricted nonabelian composition factors*, J. Algebra **79** (1982), 161–168. MR **84e:**20003
4. M. Bhattacharjee, *The probability of generating certain profinite groups by two elements*, Israel J. Math. **86** (1994), 311–329. MR **95c:**20039
5. R. W. Carter, *Simple Groups of Lie Type*, John Wiley and Sons, London, 1972. MR **53:**10946
6. F. Dalla Volta and A. Lucchini, *Generation of almost simple groups*, Preprint.
7. W. Kantor and A. Lubotzky, *The probability of generating a finite classical group*, Geom. Ded. **36** (1990), 67–87. MR **91j:**20041
8. P. Kleidman and M. W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Ser. **129**, Cambridge University Press, Cambridge, 1990. MR **91g:**20001
9. V. Landazuri and G. M. Seitz, *On the minimal degrees of projective representations of the finite Chevalley groups*, J. Algebra **32** (1974), 418–443. MR **50:**13299
10. M. W. Liebeck, C. Praeger and J. Saxl, *On the O'Nan-Scott theorem for finite primitive permutation groups*, J. Austral. Math. Soc. (A) **44** (1988), 389–396. MR **89a:**20002
11. M. W. Liebeck and A. Shalev, *The probability of generating a finite simple group*, Geom. Ded. **56** (1995), 103–113. CMP 95:14
12. A. Lubotzky, *Subgroup growth and congruence subgroups*, Invent. Math. **119** (1995), 267–295. MR **95m:**20054
13. A. Lubotzky, A. Mann and D. Segal, *Finitely generated groups of polynomial subgroup growth*, Israel J. Math. **82** (1993) (the Thompson Volume), 363–371. MR **95b:**20051
14. A. Mann, *Positively finitely generated groups*, Forum Math., to appear.
15. A. Mann and D. Segal, *Subgroup growth: a survey of current developments*, to appear in the Proc. of the 1994 Ravello meeting.
16. A. Mann and A. Shalev, *Simple groups, maximal subgroups, and probabilistic aspects of profinite groups*, Israel J. Math., to appear.
17. L. Pyber, *Enumerating finite groups of given order*, Ann. of Math. **137** (1993), 203–220. MR **93m:**11097
18. L. Pyber and A. Shalev, *Groups with super-exponential subgroup growth*, Combinatorica, to appear.

19. A. Shalev, *Growth functions, p-adic analytic groups, and groups of finite coclass*, J. London Math. Soc. (2) **46** (1992), 111–122. MR **94a:**20047
20. D. A. Suprunenko, *Matrix Groups*, Amer. Math. Soc., Providence, 1976, 252 pp. MR **52:**10852

Department of Mathematics, University of Manchester, Institute of Science and Technology, P.O. Box 88, Manchester M60 1QD, United Kingdom
E-mail address: borovik@lanczos.ma.umist.ac.uk

Mathematical Institute, Hungarian Academy of Science, P.O.B. 127, Budapest H-1364, Hungary
E-mail address: H1130Pyb@HUELLA.EARN

Institute of Mathematics, Hebrew University, Jerusalem 91904, Israel
E-mail address: shalev@math.huji.ac.il