Enumerating finite groups and their defining relations

Avinoam Mann
(Communicated by A. Shalev)

Abstract. We give upper bounds for the number of finite soluble groups of a given order and a given number of generators, and for their number of defining relations. We conjecture that similar bounds are valid for all finite groups, reduce the problem to the same one for simple groups, and remark that for most simple groups it has been solved already. Finally, we show that for $p$-groups, a lower bound of the same order of magnitude as the upper bound exists.

1 Introduction

Let $f(n)$ be the number of (isomorphism classes) of groups of order $n$. If $n = p_1^{e_1} \cdots p_k^{e_k}$ is the prime power factorization of $n$, let $\mu = \mu(n) = \max e_i$. Then it is known that $f(n) \leq n^{(2/27+o(1))\mu^2}$; see Pyber [11]. This bound is achieved if $n$ is itself a prime power; see Higman [5]. There are also estimates for the number of groups with some given restrictions. Here we are interested in the number $f(n,d)$ of groups of order $n$ which can be generated by $d$ elements, for which we have

Conjecture 1. There exists a constant $c$, such that $f(n,d) \leq n^{cd \log n}$.

A similar conjecture is made in Pyber [12].

For definiteness, our logarithms are always to base 2.

We will see that the conjecture follows from the following

Conjecture 2. There exists a constant $c$ such that any group with order $n$ and $d$ generators can be defined by means of $cd \log n$ relations.

Both conjectures hold for $p$-groups (see Neumann [10], Lemma 2.1 for Conjecture 2, and McIver and Neumann [8], Note 6.3 for Conjecture 1). Our main results establish them for soluble groups. In the notation above, let $\lambda(n) = \sum e_i$. Then we have

Theorem 1. A soluble group of order $n$ and $d$ generators can be defined by at most $(d+1)\lambda(n)$ relations in these generators.
Theorem 2. Let \( g(n, d) \) be the number of \( d \)-generator soluble groups of order \( n \). Then
\[
g(n, d) \leq n^{(d+1)\lambda(n)}.
\]

The proofs are completely elementary. An argument similar to the proof of Theorem 2 deduces Conjecture 1 from Conjecture 2, but here we have to use a fact that follows from the classification of the finite simple groups, namely that there exist at most two characteristically simple groups of any given order. It will be seen that in order to prove Conjecture 2, it suffices to show it for simple groups. Moreover, for most simple groups it is already known, so we can state

Proposition 3. Both conjectures hold, if we consider only groups which do not have composition factors isomorphic to \( U(3, q) \), \( Sz(q) \), or \( ^2G_2(q) \).

The bounds in both conjectures are of the right order of magnitude, at least for \( p \)-groups. For Conjecture 1, this is implied by the following result:

Theorem 4. For \( d > 1 \), there exists a constant \( c(d) > 0 \) such that
\[
f(p^n, d) \geq p^{c(d)n^2}
\]
for all prime powers \( p^n \).

The method of proof of Theorem 4 shows that the bound in Conjecture 2 is also of the right order of magnitude.

Finally, we note that one of the reasons for studying \( f(n, d) \) is the investigation of the so called subgroup growth, i.e. counting the number of subgroups of finite index of various kinds of group. In particular, let \( F = F_d \) be a free group of rank \( d \), and let \( t_n(F) \) be the number of normal subgroups of index \( n \) of \( F \). Then \( f(n, d) \leq t_n(F) \leq n^df(n, d) \) (see [9], p. 189).

Some of the research reported in this note was done during the Oberwolfach meeting on Simple Groups and their Applications, 26.4–3.5.97. The author is grateful to Bill Kantor, Alex Lubotzky, Laci Pyber, Aner Shalev, and the referee, for communicating their results prior to publication, and for their helpful comments on earlier versions of this note.

2 Proofs

Proof of Theorem 1. Let \( G \) be as stated, with generators \( x_1, \ldots, x_d \). If \( G \) has prime order \( p \), then it is generated already by \( x_1 \), say, and we can present it by the relations \( x_1^n = 1 \), and \( x_i = x_1^{k_i} \), for \( i > 1 \), and some \( k_i \). If \( G \) is not of prime order, let \( N \) be a minimal normal subgroup of \( G \). Then \( m := |N| = p^k \), for some prime \( p \). By induction, \( G/N \) can be defined by \( r \leq (d + 1)\lambda(n/m) \) relations in the generators \( x_iN \). Let these relations be \( u_1(xN) = 1, \ldots, u_r(xN) = 1 \). (Here and below, \( xN \) stands for the \( d \)-tuple \( (x_1N, \ldots, x_dN) \), similarly for \( x \) etc.). Let \( y_1, \ldots, y_k \) be a set of generators for \( N \),
chosen so that they are conjugate in $G$. Express $y_1$ as a word $w_1(x)$ in the generators of $G$, find words $v_i(x)$ such that $y_i = v_i^{x_i}$, for $i \geq 2$, and let $w_i(x)$ be the word $w_i^x$. Since $G$ is finite, the words $v_i$ can be chosen as negative ones, i.e. products of negative powers of the generators. Next, find words $t_i$ such that $w_i(x) = t_i(y)$, and words $s_y$ such that $y_i^{w_i} = s_y$. We claim that $G$ can be defined by the following relations, where $w_i$ etc. stand for the expression of these words in terms of the letters $x_1, \ldots, x_d$, i.e. $w_i$ is a shorthand notation for the word $w_i^{x_i}$, and $t_i(w), s_y(w)$ are the words (in $x_i$) obtained by substituting the word $w_i$ for the variable $y_i$ in the words $t_i$ and $s_y$. The number of possibilities for each $y_i$ is finite, the words $w_i^{x_i}$ can be de®ned by the following relations.

Indeed, let $X$ be the group defined by this presentation. Since the relations are ful®lled in $G$, there is a homomorphism $\phi$ from $X$ onto $G$ (mapping the generators $x_i$ of $X$ to the generators of the same name of $G$). The elements $w_1(x), \ldots, w_k(x)$ are conjugate in $X$, by the form of the words $w_i$. Let $Y$ be the subgroup of $X$ generated by them. Then the relations show that $Y^x \leq Y$, therefore $Y^\pi \leq Y$, whenever $\pi$ is a positive word on the $x_i$, and since the words $v_j$ are negative, $Y \leq Y^x$. Now $w_1$ is a central element of order $p$ of $Y$, therefore $w_1$ is central in $Y^x$, and so also in $Y$. Thus $Y$ is an elementary abelian group of order dividing $p^k$. It follows that $\phi$ induces an isomorphism from $Y$ onto $N$. In particular $Y$ is finite, so that $Y^x = Y$, and $Y \leq X$. A presentation for $X/Y$ is obtained by putting the generators of $Y$ equal to 1 in the presentation of $X$, and the resulting presentation is the given presentation for $G/N$. Thus $\phi$ induces also an isomorphism from $X/Y$ onto $G/N$, and $X \cong G$.

The number of the relations is thus $k + dk + r = r + (d + 1)k \leq (d + 1)(\lambda(n/m) + k) = (d + 1)\lambda(n)$.

**Proof of Theorem 2.** Let $G$ be a $d$-generator soluble group of order $n$, and let $N$ be a minimal normal subgroup of $G$, of order $m = p^k$, for some prime $p$. The number of possibilities for $m$ is $\lambda(n)$. Find $r \leq (d + 1)\lambda(n/m)$ relations defining $G/N$. We use notation similar to that of the preceding proof. Then $G$ has a presentation consisting, first of a presentation for $N$. This fragment of the presentation of $G$ depends only on $m$. Next, we add relations expressing the action of the generators of $G$ on the generators of $N$. There are $kd$ such relations, of the form $y^x = s(y)$, and the number of possibilities for each $s(y)$ is $m$, so that we have $m^{kd}$ possibilities for these relations. Finally, we express the relations of $G/N$ in terms of the $y$’s, finding $m^r$ possibilities for such relations. We see that if $N$ and $G/N$ are given, the number of possibilities for $G$ is at most $m^{\lambda(n/m)}m^{(d+1)\lambda(n/m)} = m^{\lambda(n)+2\lambda(n/m)}$.

By induction, the number of possibilities for $G/N$ is at most $(n/m)^{(d+1)\lambda(n/m)}$, so if $m$ is fixed, the number of possibilities for $G$ is at most $n^{\lambda(n)}m^{(d+1)\lambda(n/m)} \leq n^{(d+1)\lambda(n)}$, Recalling that there are $\lambda(n)$ possibilities for $m$, we get the required bound $n^{(d+1)\lambda(n)}$ for $g(n, d)$.

This proof shows that Conjecture 1 follows from Conjecture 2. The only difference needed is to note that $m$ does not determine $N$ uniquely, but only up to two possi-
bilities at most; see [7]. Moreover, to prove Conjecture 2, it suffices to prove it for simple groups. To see this, consider the proof of Theorem 1, without assuming that $G$ is soluble. Choosing $N$ as there, if $N$ is abelian and the conjecture holds for orders less than $n$, the proof carries through. Suppose that $N$ is not abelian, and write it as $S_1 \times \cdots \times S_k$, where $S_i$ are conjugate simple groups. For each $S_i$, choose two generators $y_i, z_i$, conjugate simultaneously to $y_1, z_1$. We find for $G$ a presentation as in the abelian case, specifying the action of the $x_i$’s on the $y_j$’s and $z_j$’s, and making $y_1$ and $z_1$ commute with the other $y$’s and $z$’s. The subgroup $Y$ will be this time the one generated by $y_i, z_i$. The assumed relations ensure that a given pair $y_i, z_i$ centralizes all other such pairs, and therefore $Y$ is the central product of the subgroups $\langle y_i, z_i \rangle$. To identify these subgroups, we replace the relation $y_1^c = 1$ by a set of defining relations for $S_1$. Then $\langle y_1, z_1 \rangle$ is isomorphic to $S_1$ or to $1$ (because $S_1$ is simple), and because these relations are satisfied in $G$, it is $S_1$. Then the central product $Y$ is actually a direct product of the subgroups $S_i$. Now the proof that the new set of relations defines $G$ is the same as above.

Next we count the number of relations. We have $r$, say, relations for $G/N$, and the induction hypothesis is that $r \leq cd \log(n/m)$, for some $c$. The value of $c$ will be specified later. We have conjugation relations for each pair $x_i, y_j$ or $x_i, z_j$, so $2dk$ relations, and relations ensuring that $y_1$ and $z_1$ commute with the other $y$’s and $z$’s, so there are $4(k - 1)$ of these. Finally we have the number of defining relations of $S_1$. If this number is $O(\log|S_1|)$, say bounded by $c'\log|S_1|$, then the total number of relations is at most

$$cd \log(n/m) + (2d + 4)k + c' \log|S_1| \leq cd \log(n/m) + (2d + 4 + c') \log m \leq cd \log n,$$

provided that we choose $c$ so that $cd \geq 2d + 4 + c'$. Thus we see that the proof works, provided that the number of the defining relations for all composition factors $S$ of $G$ is $O(\log|S|)$.

Presentations for the alternating groups $A_n$, requiring about $n/2$ relations, are given in [3], pp. 66–67. In [1] (see also [6]), the length of presentations of finite groups is examined. This is defined as the number of generators added to the sum of the lengths of the relators. Obviously, the number of relations is less than the length. In that paper it is shown that most simple groups of Lie type have presentations of length $O(\log|S|)$, and thus the conjecture holds for these groups. The exceptions are the unitary groups $U/(2n + 1, q), n \geq 2$ and the Ree groups $^2F_4(q)$, (for these two families presentations of length $O((\log|S|)^2)$ are found), and the groups $U(3, q), Sz(q)$, and the Ree groups $^2G_2(q)$. However, for the unitary groups of odd dimension at least 5, and for the groups $^2F_4(q)$, the number of relations is still $O(\log|S|)$. These results establish Proposition 3.

**Proof of Theorem 4.** Let $F$ be a free group of rank $d$, and let $F_t$ be the lower $p$-central series of $F$. This is defined by $F_1 = F, F_{t+1} = F_t^p[F_t, F]$. Let $H = F/F_{c+1}$, for some $c$, and let $G = H/N$, for some subgroup $N$ of $H/\langle F_c/F_{c+1} \rangle$, satisfying $|H_c/N| = |N|$. 

or \( p | N \). Since \( H \) is the free group of rank \( d \) in the variety of groups with lower \( p \)-central series of length \( c \), two such factor groups \( H / N \) and \( H / M \) are isomorphic if and only if \( M \) and \( N \) are conjugate under \( \text{Aut}(H) \). Now \( \text{Aut}(H) \) acts on \( H / H' \) as \( \text{GL}(d, p) \), and the kernel of this action is a \( p \)-group which acts trivially on each factor \( H / H_{i+1} \). Therefore the size of the orbits of subgroups of \( H \), under \( \text{Aut}(H) \) is at most \( |\text{GL}(d, p)| \), and the number of such orbits, hence the number of factor groups \( G \), is at least the number of subgroups \( N \), divided by \( |\text{GL}(d, p)| \). Writing \( |G| = p^m \), we obtain that \( f(p^m, d) \) is at least the number of groups like \( G \). For fixed \( d \) and \( p \), we can regard \( |\text{GL}(d, p)| \) as a constant. By Bryant and Kovács [2], Section 3, \( F_k / F_{k+1} \) is an elementary abelian group whose rank is \( s(k) = \sum^k r(i) \), where \( r(i) \), given by Witt’s formula, is asymptotically \( d^i / i \) (see for example [4], 11.2.2]). More precisely, \( d^i / i \leq (d^i - d^{(i-1)} / i) \leq r(i) \leq d^i / i \). (Since we are interested in asymptotic results, we may ignore the small values of \( i \).) It is easy to see that for \( d \geq 2 \) the inequality \( d^i / k \geq \frac{1}{2} \sum^i j d^j / j \) holds. It follows that \( s(k) = s(k-1) + r(k) = s(k-1) + d^i / 2k \geq (7/6)s(k-1) \). Writing \( |H_c| = p^r \), and \( |H| = p^i \), we conclude that \( m \leq t \leq 7s \). Then the number of subgroups \( N \) is at least \( p^{7s/4p^d} \), and dividing by \( |\text{GL}(d, p)| \leq p^{d^2} \), we obtain the desired inequality, for groups of order \( p^m \).

Now consider any order \( p^m \). Then we have \( m \leq n \leq m' \), where \( m \) is as above, for some \( c \), and \( m' \) is the corresponding value for \( c+1 \). The inequalities above imply \( r(k+1) \leq d^k / (k+1) \leq d^k / k \leq 2d^k / k \), so \( s(k+1) = s(k) + r(k+1) \leq (2d + 1)s(k) \). The construction of \( G \) shows that \( s(k) \leq 2m \), and so \( n \leq m' \leq m + (s(k+1) / 2 + s(k+1) / 2) \leq (2d + 3)m \).

For each group \( G \) of order \( p^m \) as constructed above, we will construct a group \( K \) of order \( p^n \), in such a way that \( K \) determines \( G \) uniquely. Thus for \( f(p^n, d) \) the same bound as the one obtained for \( f(p^m, d) \) holds, i.e., \( f(p^n, d) \geq p^{(d^i)m^2} \geq p^{(d^i)m^2 / (2d^i+4)} \), proving the theorem.

We note first that \( \exp(G) \leq \exp(H) \leq p^d \). On the other hand, \( H \) maps onto any \( d \)-generator group whose lower \( p \)-central series has length at most \( c \), and in particular onto the free abelian group \( A \) of rank \( d \) and exponent \( p^d \). It follows that \( G / G' \cong H / H' \cong A \). Form a direct product \( G \times B \), where \( B \) is a \( d \)-generator abelian group of order \( p^{d^i \cdot m \cdot c} \), which maps onto \( A \). Then \( (G \times B)^p = B^p \) has order \( p^{d^i \cdot m} \). Let \( G \) and \( B \) be generated by \( x_1, \ldots, x_d \) and \( b_1, \ldots, b_d \), respectively, and let \( K \) be the subgroup of \( G \times B \) generated by \( (x_1, b_1), \ldots, (x_d, b_d) \). Note that \( K^p = B^p \). There is a map \( \phi \) of \( K \) onto \( G' \), with kernel \( \text{ker}(\phi) \geq K^p \). Let \( u \in \ker(\phi) \), and write \( u = w(x_j, b_j) = (w(x_j), w(b_j)) = (1, w(b_j)) \), for some word \( w \). Write \( w(x_i) = (\Pi_i^j x_i^p) v \), for some commutator word \( v \). Then \( \Pi_i^j x_i^p \in G' \), implying that the exponents \( n_i \) are divisible by \( p^d \), and therefore \( u = (1, w(b_j)) \in K^p \). Thus \( \ker(\phi) = K^p \), which shows that \( |K| = p^n \) and that \( G \cong K / K^p \), and thus \( K \) determines \( G \). This ends the proof.

**Remark.** The number of \( p \)-groups of class two is already more or less of the same order of magnitude as the number of all \( p \)-groups. More precisely, \( \log f(p^d) \) is asymptotic to the similar quantity for the number of \( p \)-groups of class two, by [5] and [14]. (However, I know of no proof of the statement that is sometimes made, that most \( p \)-groups are of class two.) But a similar phenomenon does not hold for the number of \( d \)-generated \( p \)-groups of class at most \( c \), for any \( c \). This is so because the
number of $p$-groups of order $n$ and class at most $c$ is not more than the number of normal subgroups of index $n$ of the free nilpotent group of class $c$ and rank $d$. However, it is known that even the number of all subgroups of index $n$ of the latter group is polynomial in $n$; see [13].

References


Received 13 May, 1997; revised 10 July, 1997

Avinoam Mann, Einstein Institute of Mathematics, Hebrew University, Givat Ram, Jerusalem 91904, Israel