The Number of Generators of a Finite Group

FEDERICO MENEGAZZO

ABSTRACT. In this expository article, which is a slightly expanded version of the lecture given at the All Ireland Algebra Days (Belfast, 16–19 May, 2001), we first recall a technique recently developed by F. Dalla Volta and A. Lucchini to study generation properties of finite groups. We then discuss some problems in permutation groups, linear groups and profinite groups where this technique has proved useful. Finally, we comment on some results and problems related to probability and computation.

1. INTRODUCTION

If G is a finite group (all groups in this paper will be finite, unless explicitly stated otherwise), we denote by $\mathrm{d}(G)$ the minimum cardinality of a set of generators of G.

(This is not to be confused with the related notion of 'cardinality of an irredundant set of generators': *e.g.* in $\mathrm{Sym}(n)$, $(1\,2), (2\,3), \ldots,$ $(n-1\,n)$ is an irredundant set of generators having $n-1$ elements, but $\mathrm{d}(\mathrm{Sym}(n)) = 2$: $(1\,2), (1\,2\,\ldots n)$ suffice. But in the particular case of p-groups the two notions coincide, namely, according to Burnside's Basis Theorem, if G is a finite p-group, then any irredundant set of generators has $\mathrm{d}(G)$ elements.)

It is well known that the map $G \mapsto \mathrm{d}(G)$ is not well behaved with respect to subgroups. As a familiar example, consider the group $\mathrm{Sym}(n)$: $\mathrm{d}(\mathrm{Sym}(n)) = 2$, but $\mathrm{Sym}(n)$ has a subgroup $E = \langle (1\,2), (3\,4), \ldots, (2i-1\,2i), \ldots \rangle$ with $\mathrm{d}(E) = [n/2]$.

And this time p-groups are no exception: if we denote C_m a cyclic group of order m, the standard wreath product $W = C_p \,\mathrm{wr}\, C_{p^n}$ has $\mathrm{d}(W) = 2$, while its 'base subgroup' B has $\mathrm{d}(B) = p^n$.

On the other hand, if $\mathrm{d}(G) = m$ and X is any epimorphic image of G, then obviously $\mathrm{d}(X) \leq \mathrm{d}(G)$, and there is an epimorphic image H of G with the property

$\mathrm{d}(H) = m$ and $\mathrm{d}(X) < m$ for all proper epimorphic images of H.
We refer to such groups as being *generator-critical.*

To transform this simple-minded remark into a useful tool, we will need to study generator-critical groups in some detail.

We note at this point that the classification of finite simple groups enters heavily in most general results on the generation of finite groups. In particular, the classification allows to assemble classical results on alternating groups and groups of Lie type with individual checks on the sporadic simple groups into the fundamental unified statement.

Theorem. *If S is any non abelian simple finite group, then $\mathrm{d}(S) = 2$.*

And it is also required in the proof of the following more technical results which will be basic in our discussion:

Theorem. [17]. *Let N be a proper, minimum normal subgroup of the finite group G. Then $\mathrm{d}(G) \leq \mathrm{d}(G/N) + 1$.*

Theorem. [20]. *Let the finite, non cyclic group G have a unique minimum normal subgroup M. Then $\mathrm{d}(G) = \max(2, \mathrm{d}(G/M))$.*

2. GENERATOR-CRITICAL GROUPS

Let $\mathcal{L}$ be the set of finite groups L with the properties:

- L has a unique minimal normal subgroup, M;
- if M is abelian then it has a complement in L.

The groups in $\mathcal{L}$ are rather well understood. With M abelian, easy examples are: if F is the field with p elements, take $M = F$ (the additive group of the field), $L = M \rtimes H$ with $H \leq F^{\times}$ (the multiplicative group of F; we do not exclude $H = 1$). In general L is an affine group $L = M \rtimes H$, where M is an F-vector space and H is an irreducible subgroup of $\mathrm{GL}_F(M)$.

With M non abelian, easiest examples are: if S is a non abelian simple group, $S \leq L \leq \operatorname{Aut} S$ (*i.e.* L is almost simple; we do not exclude $L = S$. We record that $\mathrm{d}(L) \leq 3$ for any almost simple group [4]). Here are more examples: $L = S \operatorname{wr} \operatorname{Sym}(n)$, where $M = S^n$ is the base subgroup. The general case is as follows: L is a subgroup of $W = \operatorname{Aut} S \operatorname{wr} \operatorname{Sym}(n)$, $M = S^n \leq L \leq W$, such that L projects onto a transitive subgroup of $\operatorname{Sym}(n)$.

Given $L \in \mathcal{L}$ with $M = \operatorname{soc} L$ and a positive integer t define the group L_t as follows:

$$L_t := \{ (l_1, \dots, l_t) \in L^t \mid l_1 \equiv \dots \equiv l_t \bmod M \}.$$

Moreover let $L_0 := L/M$.

The following properties of these groups L_t for $t > 0$ are easily proved:

- $\operatorname{soc} L_t = M^t$;
- if K is a minimal normal subgroup of L_t, then $K \cong M$ and $L_t/K \cong L_{t-1}$;
- $\mathrm{d}(L_{t-1}) \leq \mathrm{d}(L_t) \leq \mathrm{d}(L_{t-1}) + 1$ for $t > 1$;
- $\lim_{t\to\infty} \mathrm{d}(L_t) = \infty$.

Hence if $m > \mathrm{d}(L)$ there is a unique $t = f(L, m)$ such that

$$\mathrm{d}(L_t) = m, \qquad \mathrm{d}(L_{t-1}) < m.$$

This means that $\mathrm{d}(L_{f(L,m)}) = m$ and for every proper epimorphic image X we have $\mathrm{d}(X) < m$: in other words, $L_{f(L,m)}$ is generator-critical.

The significance of this construction comes from the following

Theorem. [5]. *If H is a generator-critical finite group and $\mathrm{d}(H) = m$, then H is isomorphic to $L_{f(L,m)}$ for some $L \in \mathcal{L}$.*

Hence, if G is any nontrivial finite group, there exist $L \in \mathcal{L}$ and a positive integer t such that L_t is an epimorphic image of G and $\mathrm{d}(G) = \mathrm{d}(L_t)$.

When trying to prove that a finite group which has a given property $\mathcal{P}$ can by generated by a certain number m of elements, a minimum counterexample is often a generator-critical group with $m + 1$ generators. Hence results on the generation of groups L_t allow us to prove general results on the generation of finite groups. In particular, we are interested in getting information about $f(L, m)$.

Here is an informal and very crude summary: if M is abelian, then $f(L, m)$ is linear in m, while if M is not abelian, then $f(L, m)$ is approximately exponential in m.

For a precise statement, we distinguish several cases.

Case 1: $L = M$ is cyclic of order p. In this case of course $L_t = L^t$ and $f(L, m) = m$.

Case 2: $L > M$, M abelian.

Let F be the field $C_{\operatorname{End} M}(L_0)$, and define r_L, s_L by $r_L = \dim_F M$, $s_L = \dim_F \mathrm{H}^1(L_0, M)$. If $m > \mathrm{d}(L_0)$, then $f(L, m) = r_L(m - 2) +$

$1-s_L$. Since $s_L < r_L$ [1], we get the inequalities $m-1 \leq f(L,m) \leq r_L(m-2)+1$.

Case 3: M non abelian.

For any finite group X, let $\phi_X(s)$ denote the number of s-bases, that is, ordered s-tuples $(x_1,\dots,x_s)$ of elements of X that generate X. We may identify L with a subgroup of $\operatorname{Aut} M$, and there is a simple group S such that $M \cong S^n$. Let $\gamma_L = |C_{\operatorname{Aut} M}(L/M)|$ and for any $s \in \mathbb{N}$ define $\psi_L(s) = \frac{\phi_L(s)}{\gamma_L \phi_{L/M}(s)}$. It can be proved that if $m > \mathrm{d}(L_0)$ then $f(L,m) = \psi_L(m-1)+1$. Moreover, there is a constant γ, $0<\gamma<1$, such that for any $s \geq \max(2, d(L_0))$ we have

$$\frac{\gamma |M|^{s-1}}{n|\operatorname{Out} S|} \leq \psi_L(s) \leq |M|^{s-1}.$$

And then, known information on the automorphism groups of simple groups allows to conclude that there is a constant c such that

$$\frac{c|M|^{m-2}}{\log |M|} \leq f(L,m) \leq |M|^{m-2}.$$

As a matter of fact, it turns out that in many instances the following simplified statement is enough to get the desired conclusion:

If m elements are really needed to generate a group G, then G has a normal section H/K that is either elementary abelian of rank $\geq m-1$ or the direct product of at least a constant times 2^m isomorphic simple groups.

3. Generating Permutation Groups

Every subgroup of $\mathrm{Sym}(n)$ can be generated by at most n elements [10]; this bound has been lowered, using the classification, to $[\frac{n}{2}]$ if $n > 3$ (P. Neumann, in [3]). But for special classes of permutation groups, such as transitive and primitive ones, it has long been suspected that substantially smaller bounds would hold.

Theorem. [21] *There is a constant C such that, if $G \leq \mathrm{Sym}(n)$ is transitive, then*

$$\mathrm{d}(G) \leq \frac{Cn}{\sqrt{\log n}}.$$

To prove this result, which was first obtained for nilpotent groups in [12] and extended to soluble groups in [2], we used the approach *via* generator-critical groups introduced above, but also a bound on the number of abelian composition factors [27] and the following lemma, also proved in the soluble case in [2]:

Lemma. *There is a constant b such that, if H is a subgroup of index $n \geq 2$ of a finite group G, F is any field, V is an FH-module of dimension a over F, then every submodule of the induced module $W = V\uparrow_H^G$ can be generated by $[abn/\sqrt{\log n}]$ elements.*

The same ideas, plus information on linear groups which will be described in the next section, yield

Theorem. [22] *There is a constant C such that, if G is a primitive permutation group of degree $n \geq 3$, then*

$$\mathrm{d}(G) \leq \frac{C \log n}{\sqrt{\log \log n}}.$$

Note that the bounds given by the above theorems are asymptotically best possible [12], [29].

4. Generating Linear Groups

In this section K is a field, V a K-vector space, $\dim_K V = n$ is finite, and G is a finite subgroup of $\mathrm{GL}_K(V)$. The goal is to give bounds for $\mathrm{d}(G)$ (under suitable restrictions for G and K) in terms of n (and possibly of K).

The starting point is the following

Theorem. [13] *If G is completely reducible, then* $\mathrm{d}(G) \leq \frac{3}{2}n$.

Note that this statement is valid for arbitrary fields, and contains no unspecified constant!

If we restrict to irreducible groups, one might suspect that a better bound could be found; but the examples in [9] show that any bound for the number of generators of an irreducible linear group of degree n over an arbitrary field K must be linear in n.

So we assume that the field K has finite degree d over its prime subfield.

Theorem. [22] *Let V be a vector space of finite dimension $n \geq 2$ over the finite field K of order p^d. There exists a constant C such that, if G is an irreducible subgroup of $\mathrm{GL}_K(V)$, then*

$$\mathrm{d}(G) \leq C d \log p \frac{n}{\sqrt{\log n}}.$$

Theorem. [24] *Let K be a finite extension field of the rational field $\mathbb{Q}$, and let $d = [K : \mathbb{Q}]$. If G is an irreducible linear group of degree $n \geq 2$ over K, then*

$$\mathrm{d}(G) \leq (C_1 + C_2 d)\frac{n}{\sqrt{\log n}}$$

for some constants C_1, C_2.

The study of the particular case of primitive linear groups is crucial in the proof of both theorems. But the result in this case is more satisfactory: it holds for arbitrary fields and the bound for the number of generators is much stronger.

Theorem. [24] *Let K be a field, V a K-vector space of dimension $n \geq 2$, G a finite primitive subgroup of $\mathrm{GL}_K(V)$. Then $\mathrm{d}(G) \leq C \log n$ for some constant C.*

Also for linear groups, there are examples showing that these bounds have the correct order (up to the choice of the constants).

5. Composition Length, and a Problem in Number Theory

In order to be able to apply the machinery of generator-critical groups to linear groups, as a preliminary step it was necessary to find estimates for the composition length of the groups involved – especially so for primitive linear groups over number fields and finite fields.

If X is any finite group, we denote by $\mathrm{a}(X)$ the length of a composition series of X.

Theorem. [15] *Let K be a finite extension field of $\mathbb{Q}$, and let $d = [K : \mathbb{Q}]$; let V be a K-vector space of dimension n, G a finite quasi-primitive subgroup of $GL_K(V)$. Then $\mathrm{a}(G) \leq c_1 \log n + 2 \log d + 1$, where c_1 is an absolute positive constant.*

This result is again best possible, in the sense that the lower bound for $\mathrm{a}(G)$ is of the same form but with a different constant.

The problem for finite fields is more difficult – and perhaps more interesting.

For any positive integer n, denote by $\Omega(n)$ the number of prime factors of n, counting multiplicities, and as customary by $\mathrm{d}(n)$ the number of positive divisors of n. Then clearly for a finite abelian group X, the composition length equals $\Omega(|X|)$.

A most natural example of a primitive linear group is the multiplicative group $F^\times$ of the field F with q^n elements acting by multiplication on F itself, viewed as a vector space of dimension n over the field with $q = p^d$ elements. It is easy to see that the action is indeed primitive, since it is transitive on the set of non-zero vectors. Hence, a particular case of our question is the following number-theoretic

Problem: Find the asymptotic behaviour of $\Omega(q^n - 1)$.

As far as I know, the problem is still open. We have been able to find an upper bound:

Theorem. [15] *Let $q > 1$ be an integer. Then*

$$\Omega(q^n - 1) \leq C \frac{n}{\log n} \log q$$

for all $n \geq 2$, where C is an absolute positive constant.

We do not know how good this estimate is; it is to be compared with the lower bounds that come from

Proposition. [31] *For every integer $n \geq 1$*

a) $\Omega(2^n - 1) \geq d(n) - 1$;
b) $\Omega(q^n - 1) \geq d(n)$ *if* $q > 2$.

which, combined with a well-known result of Wigert, gives

Proposition. *For any given $\epsilon > 0$, for infinitely many natural numbers n we have, uniformly over q, that*

$$\Omega(q^n - 1) > 2^{\frac{(1-\epsilon)\log n}{\log\log n}}.$$

This partial solution to the number-theoretic problem leads to the following

Theorem. [15] *Let K be a finite field of characteristic p and order p^d, V a K-vector space of dimension n, G a quasi-primitive subgroup of $GL_K(V)$. Then* $\mathrm{a}(G) \leq \log p \max\left\{1, \frac{Cnd}{\log(nd)}\right\}$, *where C is an absolute positive constant.*

6. 'PROFINITE GRUSHKO-NEUMANN THEOREM'

The method of generator-critical groups has been successfully applied to profinite groups.

We start by recalling a well-known result on free products:

Theorem (Grushko - Neumann). *If H_1, H_2 are finitely generated groups, then* $\mathrm{d}(H_1 * H_2) = \mathrm{d}(H_1) + \mathrm{d}(H_2)$.

The free product is a coproduct in the category of groups; a coproduct exists also in the category of profinite groups, and the question has been open for some time whether $\mathrm{d}(H_1 \coprod H_2) = \mathrm{d}(H_1) + \mathrm{d}(H_2)$ for any pair of topologically finitely generated profinite groups (it is Problem 12.71 in the 'Kourovka Notebook').

Ribes and Wong [30] have shown that the question is equivalent to: for every pair H_1, H_2 of finite groups, does there exist a finite group G such that $G = \langle H_1, H_2 \rangle$ and $\mathrm{d}(G) = \mathrm{d}(H_1) + \mathrm{d}(H_2)$?

If both H_1, H_2 are p-groups, for the same prime, then $\mathrm{d}(H_1 \times H_2) = \mathrm{d}(H_1) + \mathrm{d}(H_2)$. It is then natural to look at the other extreme – namely, the case of groups of coprime orders.

If H_1, H_2 and G are assumed to be soluble, then the answer is negative [14].

The answer is negative also for arbitrary finite groups [18], [19]:

Theorem. *There exist two constants α and β, with $\alpha < 1$, such that if a finite group G is generated by two subgroups H_1 and H_2 of coprime orders and each of these subgroups can be generated by d elements then $d(G) \leq d(1+\alpha) + \beta$.*

Theorem. *There exists an integer δ such that for any $d \geq \delta$ the following is true: for any pair p and q of distinct primes, if P is a p-group, Q is q-group, and P and Q can be generated by d elements then $d(G) \leq d+1$ for any finite group G generated by P and Q.*

7. Probability

For any finite group G, we already defined $\phi_G(s)$ as the number of s-bases, that is, ordered s-tuples $(g_1, \ldots, g_s)$ of elements of G that generate G. The number $P_G(s) = \frac{\phi_G(s)}{|G|^s}$ gives the probability that s randomly chosen elements of G generate G.

A rather active research area in the past few years has been concerned with the problem of finding conditions on G and s which imply that $P_G(s)$ is 'high' (s must of course be at least $\mathrm{d}(G)$). A particularly good example is the following

Theorem. [7], [11], [16] *If S is a finite non abelian simple group and $S \leq G \leq \mathrm{Aut}\, G$, then the probability that two randomly chosen elements of G generate a subgroup containing S tends to 1 as $|S| \to \infty$.*

A similar result holds for groups in the class $\mathcal{L}$. To formulate it neatly, we introduce a related notion: if G is a finite group and N

is a normal subgroup of G, let $P_{G,N}(s) = \frac{P_G(s)}{P_{G/N}(s)}$. This number is the probability that a s-tuple generates G, given that it generates G modulo N.

Theorem. [25] *Assume that a finite group L has a unique minimum normal subgroup M and that $s \geq \mathrm{d}(L)$. Then $P_{L,M}(s) \to 1$ as $|M| \to \infty$.*

This means that, if L has a unique minimum normal subgroup M, M is 'large', and we choose at random s elements which generate L modulo M, then these elements almost certainly generate L itself.

On the other hand, it is a remark of Kantor and Lubotzki [11] that, given any real number α with $0 < \alpha < 1$, there is no function f such that if $s \geq f(\mathrm{d}(G))$ then $P_G(s) > \alpha$. Hence, in probabilistic estimates of the kind we are considering, it is not possile to refer only to $\mathrm{d}(G)$, and it will be necessary to take other invariants of G into account. In this context, some attention has centered around the

Conjecture (Pak [26]): *given a real number α with $0 < \alpha < 1$ there exists an absolute constant β such that for any finite group G, if $s \geq \beta d(G) \log\log |G|$ then $P_G(s) \geq \alpha$.*

Pak's conjecture is still open. Evidence in favour of it comes from the study of generator-critical groups:

Theorem. [6] *Given a real number α with $0 < \alpha < 1$ there exist two constants β_1, β_2 such that, for every $L \in \mathcal{L}$ and positive integer t, $P_{L_t, \mathrm{soc}\, L_t}(s) \geq \alpha$ provided*

- *$s \geq \beta_1 + \mathrm{d}(L_t)$ if $\mathrm{soc}\, L$ is abelian*
- *$s \geq \beta_2 \log(t+1)$ if $\mathrm{soc}\, L$ is non abelian.*

8. Computer Algebra

In computer algebra packages, the standard way of giving a permutation or linear group G is to exhibit a list S of generators. Most algorithms to study properties of G or of its subgroups will have S in their input.

Analysis of the complexity shows that the size $|S|$ will usually seriously affect the performance of the algorithms, and this is confirmed by practice. It would therefore be important to be able to reduce $|S|$ as far as possible. The results described in the previous sections may be considered as a small step in this direction: at least, we have some indication of how big a generating set should be. Notice however that a small size is by no means the only requirement that a good generating set should fulfil: the ability to perform a membership test is certainly at the same level of importance, and there will usually be further requirements depending on the particular task that an algorithm is aimed at.

For permutation groups, Jerrum's filter [10] is an elegant algorithm which, given a subset S of $\mathrm{Sym}(n)$, outputs a generating set T of $G = \langle S \rangle$ of cardinality at most n (actually, $|T| \leq n-k$, where k is the number of G-orbits). On the other hand, the algorithm to get $|T| \leq [n/2]$ which has been recently developed [23] is neither simple nor elegant.

These elementary considerations suggest that we conclude with the warning that to the following problems, that is quite natural to formulate at this point, it may be rather hard to give satisfactory answers:

Problem 1: Give an algorithm to transform a given set of generators into a generating set of minimum cardinality, for permutation and linear groups.

Problem 2: Give an algorithm to find a set of generators of the expected cardinality, for particular classes of permutation and linear groups (*e.g.* $\log n$ for primitive subgroups of $\mathrm{Sym}(n)$, etc.).

REFERENCES

[1] M. Aschbacher and R. Guralnick, *Some applications of the first cohomology group*, J. Algebra **90** (1984), 446–460.

[2] R.M. Bryant, L. Kovács and G.R. Robinson, *Transitive permutation groups and irreducible linear groups*, Quart. J. Math. Oxford (2) **46** (1995), 385–407.

[3] P.J. Cameron, R. Solomon and A.Turull, *Chains of subgroups in symmetric groups*, J. Algebra **127** (1989), 340–352.

[4] F. Dalla Volta and A. Lucchini, *Generation of almost simple groups*, J. Algebra **178** (1995), 194–233.

[5] F. Dalla Volta and A. Lucchini, *Finite groups that need more generators than any proper quotient*, J. Austral. Math. Soc. (Series A) **64** (1998), 82–91.

[6] F. Dalla Volta, A. Lucchini and F. Morini, *On the probability of generating a minimal d-generated group*, J. Australian Math. Soc. **71** (2001), 177–185.

[7] J. D. Dixon, *The probability of generating the symmetric group*, Math. Z. **110** (1969), 199–205.

[8] J.D. Dixon and L. Kovács, *Generating finite nilpotent irreducible linear groups*, Quart. J. Math. Oxford (2) **44** (1993), 1–15.

[9] I.M. Isaacs, *The number of generators of a linear p-group*, Canad. J. Math. **24** (1972), 851–858.

[10] M. Jerrum, *A compact presentation for permutation groups*, J. Algorithms **7** (1986), 60–78.

[11] W. Kantor and A. Lubotzky, *The probability of generating a finite classical group*, Geom. Dedicata **36** (1990), 67–87.

[12] L. Kovács and M.F. Newman, *Generating transitive permutation groups*, Quart. J. Math. Oxford (2) **39** (1988), 361–372.

[13] L. Kovács and G.R. Robinson, *Generating finite completely reducible linear groups*, Proc. Amer. Math. Soc. **112** (1991), 357–364.

[14] L. Kovács and H. Sim, *Generating finite soluble groups*, Indag. Math. (N.S.) **2** (1991), 229–232.

[15] A. Languasco, F. Menegazzo and M. Morigi, *On the composition length of finite primitive linear groups*, Arch. Math., to appear

[16] M.W. Liebeck and A. Shalev, *The probability of generating a finite simple group*, Geom. Dedicata **56** (1995), 103–113.

[17] A. Lucchini, *Generators and minimal normal subgroups*, Arch. Math. **64** (1995), 273–276.

[18] A. Lucchini, *On the minimal number of generators of free profinite products of profinite groups*, J. Group Theory **4** (2001), 53–58.

[19] A. Lucchini, *On the number of generators of finite images of free products of finite groups*, J. Algebra **245** (2001), 552–561.

[20] A. Lucchini and F. Menegazzo, *Generators for finite groups with a unique minimal normal subgroup*, Rend. Sem. Mat. Univ. Padova **98** (1997), 173–191.

[21] A. Lucchini, F. Menegazzo and M. Morigi, *Asymptotic results for transitive permutation groups*, Bull. London Math. Soc. **32** (2000), 191– 195.

[22] A. Lucchini, F. Menegazzo and M. Morigi, *Asymptotic results for primitive permutation groups and irreducible linear groups*, J. Algebra **223** (2000), 154–170.

[23] A. Lucchini, F. Menegazzo and M. Morigi, *Generating permutation groups*, Comm. Algebra, to appear.

[24] A. Lucchini, F. Menegazzo and M. Morigi, *On the number of generators and composition length of finite linear groups*, J. Algebra **243** (2001), 427–447.

[25] A. Lucchini and F. Morini, *On the probability of generating finite groups with a unique minimal normal subgroup*, Pacific J. Math. **203** (2002), 429–440.

[26] I. Pak, *On probability of generating a finite group*, preprint.

[27] L. Pyber, *Asymptotic esults for permutation groups*, Groups and computation, DIMACS Ser. Discrete Math. Theoret. Comput. Sci. **11** (ed. L. Finkelstein and W.M. Kantor, AMS, 1993), 197–219.

[28] L. Pyber, *Asymptotic results for simple groups and some applications, Groups and computation*, DIMACS Ser. Discrete Math. Theoret. Comput. Sci. **28** (ed. L. Finkelstein and W.M. Kantor, AMS, 1997), 309–327.

[29] L. Pyber and A. Shalev, *Asymptotic results for primitive permutation groups*, J. Algebra **188** (1997), 103–124.

[30] L. Ribes and K. Wong, *On the minimal number of generators of certain groups*, Groups—St. Andrews 1989, Vol. 2, 408–421, London Math. Soc. Lecture Note Ser. **160**, Cambridge Univ. Press, Cambridge, 1991.

[31] J.J. Sylvester, *On the divisors of the sum of a geometrical series whose first term is unity and common ratio any positive or negative integer*, Nature **37** (1888), 417–418; "Collected Papers" v. IV, Cambridge University Press, 1912, 625–629.

Federico Menegazzo,
Dipartimento di Matematica Pura e Applicata,
Universita di Padova,
Via Belzoni 7,
I–35131 Padova, Italy
federico@math.unipd.it

Received on 4 October 2001 and in revised form on 9 May 2003.