Available online at www.sciencedirect.com
SciVerse ScienceDirect
Advances in Mathematics 248 (2013) 59–95
ADVANCES IN Mathematics
www.elsevier.com/locate/aim

# Generation and random generation: From simple groups to maximal subgroups

Timothy C. Burness [a,*], Martin W. Liebeck [b], Aner Shalev [c]

[a] School of Mathematics, University of Bristol, Bristol BS8 1TW, UK
[b] Department of Mathematics, Imperial College, London SW7 2BZ, UK
[c] Institute of Mathematics, Hebrew University, Jerusalem 91904, Israel

Received 1 April 2011; accepted 23 July 2013

Available online 24 August 2013

Communicated by Roman Bezrukavnikov

**Abstract**

Let $G$ be a finite group and let $d(G)$ be the minimal number of generators for $G$. It is well known that $d(G) = 2$ for all (non-abelian) finite simple groups. We prove that $d(H) \leqslant 4$ for any maximal subgroup $H$ of a finite simple group, and that this bound is best possible.

We also investigate the random generation of maximal subgroups of simple and almost simple groups. By applying a recent theorem of Jaikin-Zapirain and Pyber we show that the expected number of random elements generating such a subgroup is bounded by an absolute constant.

We then apply our results to the study of permutation groups. In particular we show that if $G$ is a finite primitive permutation group with point stabilizer $H$, then $d(G) - 1 \leqslant d(H) \leqslant d(G) + 4$.


*Keywords:* Finite simple groups; Maximal subgroups; Minimal generation; Primitive permutation groups

## 1. Introduction

Let $G$ be a finite group and let $d(G)$ be the minimal number of generators for $G$. We say that $G$ is *$d$-generator* if $d(G) \leqslant d$. The investigation of generators for finite simple groups has a rich history, with numerous applications. Perhaps the most well known result in this area is

* Corresponding author.
*E-mail addresses:* t.burness@bristol.ac.uk (T.C. Burness), m.liebeck@imperial.ac.uk (M.W. Liebeck), shalev@math.huji.ac.il (A. Shalev).

0001-8708/$ – see front matter 
http://dx.doi.org/10.1016/j.aim.2013.07.009

the fact that every finite simple group is 2-generator. For the alternating groups, this was first stated in a 1901 paper of G.A. Miller [47]. In 1962 it was extended by Steinberg [54] to the simple groups of Lie type, and post-Classification, Aschbacher and Guralnick [2] completed the proof by analyzing the remaining sporadic groups. More generally, if $G$ is an almost simple group with socle $T$ (so that $T \leqslant G \leqslant \mathrm{Aut}(T)$ with $T$ a non-abelian finite simple group) then $d(G) = \max\{2, d(G/T)\} \leqslant 3$ (see [14]).

A wide range of related problems on the generation of finite simple groups has been investigated in recent years. For instance, we may consider the abundance of generating pairs: if we pick two elements of a finite simple group $G$ at random, what is the probability that they generate $G$? In 1969 Dixon [15] proved that if $G = A_n$ then this probability tends to 1 as $n \to \infty$, confirming an 1882 conjecture of Netto [48]. This was extended in [27,37] to all finite simple groups, as conjectured by Dixon in [15].

Various generalizations have subsequently been studied by imposing restrictions on the orders of the generating pairs. Here there are some interesting special cases. For example, the simple groups that can be generated by a pair of elements of order 2 and 3 coincide with the simple quotients of the modular group $\mathrm{PSL}_2(\mathbb{Z}) \cong Z_2 \star Z_3$, and they have been intensively studied in recent years (see [39,41], and also [40,53] for related results). In a different direction, in [21] it is proved that every non-trivial element of a finite simple group belongs to a pair of generating elements, confirming a conjecture of Steinberg [54]. A more general notion of *spread* for 2-generator groups was introduced by Brenner and Wiegold [8], and this has been widely studied in the context of finite almost simple groups (see [10,9,22], for example).

Our understanding of the subgroup structure of the finite simple groups has advanced greatly in the last 30 years or so (see [30,31,36] for an overview). Indeed, almost all of the above results require detailed information on the maximal subgroups of simple groups. The main purpose of this paper is to investigate various generation properties of the maximal subgroups themselves, establishing some new and rather unexpected results. Our aim is to show that some of the above results for simple groups can be extended, with some suitable small (and necessary) modifications, to all their maximal subgroups. For example, just as every finite simple group is 2-generator, our main result states that any maximal subgroup $H$ can also be generated by very few elements.

**Theorem 1.** *Every maximal subgroup of a finite simple group is* 4*-generator.*

There are infinitely many examples with $G$ simple and $d(H) = 4$ (see Remarks 4.5 and 5.12, for example), so Theorem 1 is best possible. In fact this theorem follows from a more general result, stated below, dealing also with maximal subgroups of almost simple groups.

**Theorem 2.** *Let $G$ be a finite almost simple group with socle $G_0$ and let $H$ be a maximal subgroup of $G$. Then $d(H \cap G_0) \leqslant 4$, and also $d(H) \leqslant 6$.*

It is likely that 4 is also the optimal bound in the more general almost simple situation.

In view of the explicit bounds obtained in Theorem 2, it is natural to investigate the probabilistic generation of maximal subgroups of simple and almost simple groups, in analogy with the aforementioned work on the simple groups themselves.

We introduce some relevant background and notation. For a finite or profinite group $G$ and a positive integer $k$ let $P(G,k)$ denote the probability that $k$ randomly chosen elements of $G$ generate $G$ (topologically, if $G$ is infinite). A profinite group $G$ is said to be *positively finitely*