МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2015
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2015
Proceedings of the Forty Fourth Spring Conference
of the Union of Bulgarian Mathematicians
SOK "Kamchia", April 2–6, 2015

PRESENTATIONS OF FINITE SIMPLE GROUPS AND APPLICATIONS*

Martin Kassabov

We construct presentations of finite simple groups with surprisingly few relations. For example there exists a presentation of the alternating groups A_n and the symmetric groups S_n with only 2 generators and 8 relations. Such presentations have applications in computational group theory. They are one of the key ingredients in algorithms for recognizing finite groups generated by matrices over finite fields.

1. Introduction. One method of defining a group G is by a presentation. One specifies a set S of generators, so that every element of the group can be written as a product of powers of some of these generators, and a set R of relations among those generators. We then say G has presentation $\langle S \mid R\rangle$. Informally, G has the above presentation if it is the "freest group" generated by S subject only to the relations R. Formally, the group G is said to have the above presentation if it is isomorphic to the quotient of a free group on S by the normal subgroup generated by the relations R. The *length* of a presentation is the sum of the number of generators and the lengths of the relations as words in both the generators and their inverses.

In this paper we study presentations of finite simple groups G. Our main result provides unexpected answers to the following questions: How many relations are needed to define G, and how short can these relations be?

There seems to have been an effort, at least in the 1930's but also as far back as 1897, to obtain presentations for symmetric and alternating groups involving as few generators and relations as possible. For example, Moore [29] gave not only the Coxeter presentation for S_n but also one with 2 generators and approximately n relations. Many such presentations are reproduced in [13]. In [6, p. 281] we find the question: "Is there a two-generator presentation for A_n with k relators, where k is independent of n?" Our Theorem 3, as well as [2], answers this question. We note that [6] lists various presentations of small simple groups, using as one of the criteria for "niceness" the short lengths of all relations.

There has been a great deal of research on presentations for relatively small simple groups, and for small-dimensional quasisimple groups. Extensive tables are given in [13].

*2010 Mathematics Subject Classification: 20D06, 20J06.
Key words: presentations of finite groups, finite simple groups.
The author is partially supported by Simons Foundation grant 30518; National Science Foundation grant DMS 1303117; and Bulgarian National Science Fund grant I 02/18 "Computational and Combinatorial Methods in Algebra and Applications".

Special emphasis is given to $\mathrm{PSL}(2,p)$ and $\mathrm{PGL}(2,p)$ in [13]. An indication of the large amount of more recent work of this sort can be found in the references in [4, 6, 7, 9, 10].

On the other hand, there are few general references containing presentations for groups of Lie type; cf. [14, 34, 35, 39], described in [15], and their consequences [1, 24]. However, there are a few specific groups for which presentations have been published; [10] and [5] are typical. The only reference containing a hint in the direction of Theorem 3 is [40], which contains a more precise conjecture than the above question in [6], namely, that the universal central extension of every finite simple group has a presentation with 2 generators and 2 relations.

The classification of the finite simple groups states that every nonabelian finite simple group is alternating, of Lie type, or one of 26 sporadic groups. The latter are of no relevance to our asymptotic results. Instead, we will primarily deal with groups of Lie type, which have a (relative) *rank* n over a field $\mathbb{F}_q$. In order to keep our results uniform, we view the alternating group A_n and symmetric group S_n as groups of rank $n-1$ over "the field $\mathbb{F}_1$ with 1 element" [38]. With this in mind, we will prove the following:

Theorem 1 ([16])**.** *All nonabelian finite simple groups of Lie type of rank n over $\mathbb{F}_q$, with the possible exception of the Ree groups ${}^2G_2(q)$, have presentations with at most C generators and relations and total length at most $C(\log n + \log q)$, for a constant C independent of n and q.*

We estimate that $C < 1000$. This reflects the explicit and constructive nature of our presentations. The theorem is interesting in several ways. It already seems quite surprising that the alternating and symmetric groups have *bounded presentations*, i.e., with a bounded number of generators and relations independent of the size of the group, as in the theorem. This was even less expected for the groups of Lie type such as $\mathrm{PSL}(n,q)$.

The bound in Theorem 1 can be improved significantly if one drops the requirement that all relations are short:

Theorem 2 ([18])**.** *All nonabelian finite simple groups of Lie type, with the possible exception of the Ree groups ${}^2G_2(q)$, have presentations with 2 generators and at most 80 relations.*

In some special cases this result can be improved significantly:

Theorem 3 ([18])**.** *All symmetric and alternating groups have presentations with 2 generators and 8 relations.*

The bound of 80 relations is not optimal – in all cases we shall provide much better bounds, though usually with more generators. Possibly 4 is the correct upper bound for standard presentations. Wilson [40] has even conjectured that 2 relations suffice for the universal covers of all finite simple groups.

We have not dealt with the Ree groups ${}^2G_2(q)$ in Theorems 1 and 2. The obstacle to both short and bounded presentations of these groups is the fact that all presentations presently known use more than q relations.

2. Proof of Theorem 3. The main idea behind the proof of Theorem 3 is to start with a presentation of the symmetric group which has many generators and relations which are invariant under a lot of symmetries. This invariance can be used to significantly reduce the presentation by using only one generator and relator for each orbit, see Lemma 4.

The most familiar presentation for the symmetric group S_n is the "Coxeter presenta-

tion" [29]:

$$S_n = \langle x_1, \ldots, x_{n-1} \mid \ x_i^2 = (x_i x_{i+1})^3 = (x_i x_j)^2 = 1 \quad \text{for all possible } i \text{ and for } i+2 \le j \le n-1 \rangle,$$

based on the transpositions $(i, i+1)$.

Unfortunately this presentation is not symmetric enough – it is only invariant under a group of order 2. There is a variant of this presentation where one adds an extra generator $(n, 1)$ which will make the presentation invariant under the dihedral group. This was used by Burnside, who obtained the following presentation of S_n with 2 generators and about n relations

$$S_n = \langle c, t \mid c^n = t^2 = (tt^c)^3 = (ct)^{n-1} = [t, t^{c^k}] = 1 \text{ for all } 2 \le k \le n-3 \rangle,$$

This reduction is obtained using the following lemma:

Lemma 4. *Let $G = \langle X \mid R \rangle$ be a presentation of the group G and let $H = \langle Y \mid R' \rangle$ be a group acting on G which fixes the generating set X. Then*

$$\langle Y \cup X/H \mid R', R/H, R'' \rangle$$

is a presentation of the group $H \ltimes G$, where

- *X/H is a set of orbit representatives of X under H;*
- *R/H is a set of orbit representatives of R under H, where we have replaced each generator by a conjugate of the orbit representative by H;*
- *R'' are the relations $[x, \mathrm{Stab}_H(x)] = 1$ for each $x \in X/H$.*

In order to take a full advantage of this one needs a presentation which is invariant under a very large group of symmetries like the following presentation based on the transpositions $(1, i)$:

$$S_n = \langle x_2, \ldots, x_n \mid x_i^2 = (x_i x_j)^3 = (x_i x_j x_i x_k)^2 = 1 \ \text{ for distinct } i, j, k \rangle.$$

This presentation is due to Burnside [3] and Miller [28] in 1911; Burnside describes it as probably "the most symmetrical form into which the abstract definition [of S_n] can be thrown".

The other essential ingredient in the proof of Theorem 3 is a presentation of a family of 3-transitive groups with a fixed number of generators and relations: Sunday [36] obtained the following presentation for $\mathrm{PSL}(2, p)$ with only 2 generators and 3 relations

$$\langle u, t \mid u^p = 1, t^2 = (ut)^3, (u^4 t u^{(p+1)/2} t)^2 = 1 \rangle.$$

There is no presentation for this group with smaller $|X| + |R|$. By [32], this follows from the fact that the Schur multiplier of $\mathrm{PSL}(2, p)$ has order 2.

Using the gluing lemma this leads to the following presentation of the semidirect product $\mathrm{PSL}(2, p) \ltimes S_{p+2}$, where the action on $\mathrm{PSL}(2, p)$ is via the action on the projective line:

$$\begin{aligned} \mathrm{PSL}(2, p) \ltimes S_{p+2} \quad = \quad & \langle u, t, z \mid u^p = 1, t^2 = (ut)^3, (u^4 t u^{(p+1)/2} t)^2 = 1, \\ & z^2 = 1, [u, z] = 1, (z z^t)^3 = 1, (z z^t z z^{tu})^2 = 1 \rangle. \end{aligned}$$

The final step in obtaining a presentation of S_{p+2} with bounded number of generators and relations is the observation that the semidirect product $\mathrm{PSL}(2, p) \ltimes S_{p+2}$ is isomorphic to the direct product $\mathrm{PSL}(2, p) \times S_{p+2}$. This leads to the following presentation with 3

generators and 8 relations

$$\begin{aligned} S_{p+2} &= \langle u,t,z \mid u^p = 1, t^2 = (ut)^3, (u^4 t u^{(p+1)/2} t)^2 = 1, \\ &\quad z^2 = 1, [u,z] = 1, (zz^t)^3 = 1, (zz^t zz^{tu})^2 = 1, (uz^t)^{p+1} = 1 \rangle. \end{aligned}$$

From here obtaining presentations of all symmetric groups is relatively easy, because one can obtain a presentation of S_m starting from a presentation of S_n for $m/2 < n < m$. The resulting presentations will have 4 generators and about 20 relations. Reducing the number of relations to 8 requires significant optimizations, including case by case handing of groups with $n < 50$.

The alternating groups are handled in a similar way, starting with a presentation of A_n due to Carmichael [11].

3. Outline of the Proof of Theorems 2 and 1. We first deal with rank 1 groups (especially $\mathrm{SL}(2,q)$, $\mathrm{SU}(3,q)$ and $\mathrm{Sz}(q)$). The case of groups over prime field is relatively easy, however encoding the field is not trivial. The main difficulty is that the unipotent subgroup is elementary abelian of large rank and does not have a presentation with small number of generators and relations. This is bypassed by considering presentations of the Borel subgroups. Presentations of these subgoups are combined in a standard presentation of Steinberg [35], based on rank 1 BN-pairs to obtain presentations of the whole groups.

The rank 1 presentations, combined with the Curtis-Steinberg-Tits presentations [14, 39], are used to obtain short bounded presentations for bounded rank groups. Bounded (but not short) presentations for untwisted groups of bounded rank were obtained in [24].

Finally, one needs to handle the classical groups of unbounded rank. Presentations of the groups $\mathrm{SL}(n,q)$ are obtained by combing a presentation of $\mathrm{SL}(4,q)$ and A_n (The consideration for the other classical groups are similar).

As in the case of Theorem 3 further optimization of the presentations is needed in order to reduce the number of relations in the presentations to under 100. Most of the optimization is achieved by technical tricks which allow us to replace several relations by a single one.

Either bounded *or* short presentations for nonabelian simple groups go substantially beyond what one might expect. Obtaining both as in Theorem 1 simultaneously was a surprise. By contrast, while abelian simple groups (i.e., cyclic groups of prime order) have bounded presentations, as well as ones that are short, they cannot have presentations satisfying both of these conditions. In fact, this example led us to believe, initially, that nonabelian simple groups also would not have short bounded presentations. A hint that nonabelian finite simple groups behave differently from abelian ones came from the Congruence Subgroup Property, which can be used to obtain a short bounded presentation for $\mathrm{SL}(2,p)$ when p is prime.

Pushing this idea to the other simple groups required many technical tricks. One of the main challanges was the case of rank 1 groups because their Borel subgroups do not have bounded and short presentations. Instead we work with infinite central extensions of these groups which are later collapsed by adding suitable relations. Another challenge is ensuring that certain elements can be represented as short words on the generators, which will later be needed to collapse the centers of the Lie groups of high rank. Not surprisingly the cost of having such control is a significant increase of the number of generators and relators in the presentations.

4. Applications. The quantitative study of profinite presentations of finite simple groups was started in [26], motivated by an attempt to prove the Mann-Pyber conjecture [27, 30], which asserts that *the number of normal subgroups of index n of the free group F_d is $O(n^{cd \log n})$* for some constant c. Mann [27] showed that his conjecture about $O(\log |G|)$-relation presentations for finite simple groups implies the Mann-Pyber conjecture; and hence he proved that conjecture except for the twisted rank 1 groups.

In [26] the Mann-Pyber conjecture was proved by using a weaker version of Mann's conjecture: *There is a constant C such that every finite simple group G has a* profinite *presentation with* 2 *generators and at most $C \log |G|$ relations.*

On the other hand, whereas our theorem shows that nonabelian finite simple groups have presentations far shorter than $O(\log |G|)$, [1] (combined with [37, 22]) showed that every finite group G with no ${}^2G_2(q)$ composition factor has a presentation of length $O((\log |G|)^3)$, where the constant 3 is best possible.

Short and bounded presentations are goals of one aspect of Computational Group Theory ([33] and [21]). Such presentations have various applications, such as in [25, 23] for gluing together presentations in a normal series in order to obtain a presentation for a given matrix group. We hope that both types of presentations will turn out to be useful in Computational Group Theory.

The crucial ingredient in the proof of the above mentioned proof of Mann-Pyber conjecture by Lubotzky [26] was a theorem of Holt [20]: *There is a constant C such that, for every finite simple group G, every prime p and every irreducible $\mathbb{F}_pG$-module M,*

$$\dim H^2(G, M) \leq C(\log_p |G|_p) \dim M,$$

where $|G|_p$ denotes the p-part of the integer $|G|$. In fact, Holt proved that C can be taken to be 2, using tools including standard cohomology methods. Moreover, Holt [20] conjectured the following stronger result which is an easy consequence of Theorem 2:

Theorem 5 (Holt's Conjecture for simple groups, [16])**.** *There is a constant C such that, for every finite simple group G, every prime p and every irreducible $\mathbb{F}_pG$-module M,* $\dim H^2(G, M) \leq C \dim M$.

The bound C in the above theorem could be improved to 20, see [17], however there is an expectation that the best possible bound is $C = 1$.

As noted above, Theorems 1 and 2 do not require the classification of the finite simple groups: it only deals with groups having rank n over $\mathbb{F}_q$. Of course, by the classification this ignores only the 26 sporadic simple groups. On the other hand, Theorem 5 does use the classification. However, unlike many papers no classification-dependent internal structural properties of these groups are required for the proof.

Acknowledgments. This paper contains a summary of the results in [16, 17, 18, 19]. The author is grateful to his collaborators R. Guralinick, W. Kantor and A. Lubotzky for their essential contribution to this project. Similar results were obtained independently by J. Bray, M. Conder, C. Leedham-Green and E. O'Brien in [2]. After this project was competed we discovered a forgotten work of Sass [31] who constructed a presentation of A_{p+2} similar to ours.

REFERENCES

[1] L. Babai, A. J. Goodman, W. M. Kantor, E. M. Luks, P. P. Pálfy. Short presentations for finite groups. *J. Algebra*, **194** (1997), 79–112.

[2] J. Bray, M. D. E. Conder, C. R. Leedham-Green, E. A. O'Brien. Short presentations for alternating and symmetric groups (preprint).

[3] W. Burnside. Theory of Groups of Finite Order, 2nd ed. Cambridge, Cambridge Univ. Press, 1911.

[4] C. M. Campbell, P. P. Campbell, B. T. K. Hopson, E. F. Robertson. On the efficiency of direct powers of $\mathrm{PGL}(2,p)$. In: Recent advances in group theory and low-dimensional topology, Pusan, 2000 (Eds J. Rae Cho, J. Mennicke). Heldermann, Lemgo 2003, 27–34.

[5] C. M. Campbell, G. Havas, S. Linton, E. F. Robertson. Symmetric presentations and orthogonal groups. In: The atlas of finite groups: ten years on, Birmingham, 1995 (Eds R. Curtis and R. Wilson), Lond. Math. Soc. Lecture Note, vol. **249**. Cambridge, Cambridge Univ. Press, 1998, 1–10.

[6] C. M. Campbell, G. Havas, C. Ramsay, E. F. Robertson. Nice efficient presentations for all small simple groups and their covers. *Lond. Math. Soc. J. Comput. Math.*, **7** (2004), 266–283.

[7] C. M. Campbell, E. F. Robertson. Classes of groups related to $F^{a,b,c}$. *Proc. Roy. Soc. Edinburgh*, **A78** (1977/78), 209–218.

[8] C. M. Campbell, E. F. Robertson. A deficiency zero presentation for SL(2, p). *Bull. Lond. Math. Soc.*, **12** (1980), 17–20.

[9] C. M. Campbell, E. F. Robertson, P. D. Williams. On presentations of $\mathrm{PSL}(2,p^n)$. *J. Austral. Math. Soc.*, **48** (1990), 333–346.

[10] C. M. Campbell, E. F. Robertson, P. D. Williams. Efficient presentations for finite simple groups and related groups. In: Groups–Korea 1988, Pusan, 1988 (Eds. Y. Gheel Baik et al.), Berlin, Springer, 1989, 65–72.

[11] R. D. Carmichael. Abstract definitions of the symmetric and alternating groups and certain other permutation groups. *Quart. J. of Math.*, **49** (1923), 226–270.

[12] H. S. M. Coxeter. Abstract groups of the form $V_1^k = V_j^3 = (V_iV_j)^2 = 1$. *J. Lond. Math. Soc.*, **9** (1934), 213–219.

[13] H. S. M. Coxeter, W. O. J. Moser. Generators and relations for discrete groups, 3rd ed. Ergebnisse der Mathematik und ihrer Grenzgebiete B. 14. New York-Heidelberg, Springer, 1972.

[14] C. W. Curtis. Central extensions of groups of Lie type. *J. reine angew. Math.*, **220** (1965), 174–185.

[15] D. Gorenstein, R. Lyons, R. Solomon. The classification of the finite simple groups. Number 3. Part I. Chapter A. Almost simple K-groups. Providence, Amer. Math. Soc., 1998.

[16] R. M. Guralnick, W. M. Kantor, M. Kassabov, A. Lubotzky. Presentations of finite simple groups: a quantitative approach. *J. Amer. Math. Soc.* , **21** (2008), 711–774.

[17] R. M. Guralnick, W. M. Kantor, M. Kassabov, A. Lubotzky. Presentations of finite simple groups: a cohomological and profinite approach. *Groups, Geometry and Dynamics*, **1** (2007), 469–523

[18] R. M. Guralnick, W. M. Kantor, M. Kassabov, A. Lubotzky. Presentations of finite simple groups: a computational approach. *J. Eur. Math. Soc.*, **13**, No 2 (2011), 391–458.

[19] R. M. Guralnick, W. M. Kantor, M. Kassabov, A. Lubotzky. Remarks on proficient groups. *J. Algebra*, **326** (2011), 169–184.

[20] D. F. Holt. On the second cohomology group of a finite group. *Proc. Lond. Math. Soc.* (*3*), **55** (1987) 22–36.

[21] D. F. Holt, B. Eick, E. A. O'Brien. Handbook of computational group theory. Boca Raton, Chapman & Hall, 2005.
[22] A. Hulpke, Á. Seress. Short presentations for three-dimensional unitary groups. *J. Algebra*, **245** (2001) 719–729.
[23] W. M. Kantor, Á. Seress. Computing with matrix groups. In: Groups, combinatorics and geometry, Durham, 2001 (Eds A. A. Ivanov et al.) River Edge, NJ, World Sci. Publ., 2003, 123–137.
[24] I. Korchagina, A. Lubotzky. On presentations and second cohomology of some finite simple groups. *Publ. Math. Debrecen*, **69** (2006) 341–352.
[25] C. R. Leedham-Green. The computational matrix group project. In: Groups and Computation III (Eds W. M. Kantor, Á. Seress). Berlin-New York, deGruyter, 2001, 229–247.
[26] A. Lubotzky. Enumerating boundedly generated finite groups. *J. Algebra*, **238** (2001), 194–199.
[27] A. Mann. Enumerating finite groups and their defining relations. *J. Group Theory*, **1** (1998) 59–64.
[28] G. A. Miller. Abstract definitions of all the substitution groups whose degrees do not exceed seven. *Amer. J. Math.*, **33** (1911) 363–372.
[29] E. H. Moore. Concerning the abstract groups of order $k!$ and $\frac{1}{2}k!$ holohedrically isomorphic with the symmetric and the alternating substitution groups on k letters. *Proc. Lond. Math. Soc.*, **28** (1897) 357–366.
[30] L. Pyber. Enumerating finite groups of given order. *Ann. of Math.*, **137** (1993) 203–220.
[31] H. Sass. Eine abstrakte Definition gewisser alternierender Gruppen. *Math. Z.*, **128** (1972), 109–113 (in German).
[32] I. Schur. Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen. *J. reine angew. Math.*, **132** (1907), 85–137.
[33] C. C. Sims. Computation with finitely presented groups. Cambridge, Cambridge Univ. Press, 1994.
[34] R. Steinberg. Lectures on Chevalley groups (mimeographed notes). Yale Univ., 1967.
[35] R. Steinberg. Generators, relations and coverings of algebraic groups, II. *J. Algebra*, **71** (1981), 527–543.
[36] J. G. Sunday. Presentations of the groups SL(2, m) and PSL(2, m). *Canad. J. Math.*, **24** (1972), 1129–1131.
[37] M. Suzuki. On a class of doubly transitive groups. *Ann. of Math.*, **75** (1962), 105–145.
[38] J. Tits. Les groupes de Lie exceptionnels et leur interprétation géométrique. *Bull. Soc. Math. Belg.*, **8** (1956) 48–81.
[39] J. Tits. Buildings of spherical type and finite BN-pairs. Berlin-New York, Springer, 1974.
[40] J. S. Wilson. Finite axiomatization of finite soluble groups. *JLMS*, **74** (2006) 566–582.

Martin Kassabov
Department of Mathematics, Cornell University
Malott Hall, Ithaca, NY 14850, USA
e-mail: kassabov@math.cornell.edu

ПРЕДСТАВЯНИЯ НА КРАЙНИТЕ ПРОСТИ ГРУПИ И ПРИЛОЖЕНИЯ

Мартин Димитров Касабов

Ние конструираме представяния на крайните прости групи с изненадващо малко определящи съотношения. Например, алтернативните групи A_n и симетричните групи S_n имат представяния само с 2 пораждащи и 8 съотношения. Такива представяния намират приложение в компютърната теория на групите. Те са ключови компоненти в алгоритмите за разпознаване на крайни групи, породени от матрици над крайно поле.