ON PRESENTATIONS AND SECOND COHOMOLOGY OF SOME FINITE SIMPLE GROUPS

INNA KORCHAGINA, ALEXANDER LUBOTZKY

In Fond Memory of Edith Szabo

1. Introduction.

As it is well known finite simple groups are all generated by two elements [AG]. But when it comes to presentations, it seems that many relations are needed. This is the case in all known presentations. For example, if $G_n(\mathbb{F}_q)$ is a simple group of Lie type of rank n over a field $\mathbb{F}_q$, the classical Steinberg presentation uses $O(n^4q^2)$ relations. Of course, many of them are redundant, but still, the number of them goes to infinity with n and q.

For a finite group G, denote by $r(G)$ the minimal number of relations over all possible presentations of G.

Theorem 1.1. *Given $n \in \mathbb{N}$, there exists $C = C(n) \in \mathbb{N}$ such that for every untwisted simple group of Lie type $G_l(\mathbb{F}_q)$ of rank $l \leq n$ over a finite field $\mathbb{F}_q$,*

$$r(G_l(\mathbb{F}_q)) \leq C(n)$$

i.e., $G_l(\mathbb{F}_q)$ has a presentation with at most $C(n)$ relations.

It seems likely, that a similar result holds for the twisted groups of Lie type, but we wonder, if such C may exist which is independent of n. One may ask:

Problem. *Does there exist a constant C_0 such that every finite simple group has a presentation with at most C_0 relations?*

We do not know the answer even for the family of alternating groups $Alt(n)$, for which the smallest presentation which is known to us requires $O(n)$ relations ([Car], [BGKLP]).

Our interest in this question grew out from a paper of Holt ([H]), in which he proves the following result:

Theorem (Holt [H]). *There exists a constant C_1 such that if G is a finite simple group and M is a simple $\mathbb{F}_p[G]$-module, then*

$$\dim_{\mathbb{F}_p} H^2(G, M) \leq C_1 \log |G| \dim_{\mathbb{F}_p} M$$

This theorem has various important applications in "counting problems" of finite group theory (see [H1], [Lu1]). Holt conjectured that in his theorem the $\log|G|$ factor can be dropped. Now, in [Lu2] it was shown that if G is a finite group and if $\hat{r}(G)$ denotes the minimal number of relations for G in a profinite presentation, then

$$\hat{r}(G) = \sup_{p,M}\{[[\frac{\dim H^2(G,M) - \dim H^1(G,M)}{\dim M}]] + d(G) - \xi_M\}$$

where p runs over all primes, and M runs over all the finite simple $\mathbb{F}_p[G]$-modules, $\xi_M = 0$ if M is trivial and $\xi_M = 1$ if M is non-trivial, and for a real number t, $[[t]]$ denotes the smallest integer which is at least t. (For the notion of profinite presentation see [Lu2]). Since $\hat{r}(G) \leq r(G)$, and using [AG], one sees that Holt's conjecture is in fact equivalent to:

Holt's Conjecture. *There exists a constant C_2 such that every finite simple group has a profinite presentation with at most C_2 relations.*

We doubt whether this conjecture is true. In fact, our work started with an effort to disprove it. We ended up with a modest contribution toward a positive solution (for some weaker results see [Lu3]). More precisely, it says that counter examples, if exist, are probably of unbounded rank.

Anyway, our positive result also implies (cf. [H]):

Corollary 1.2. *For every $n \in \mathbb{N}$, there exists $C_3 = C_3(n)$ such that if $G_l(\mathbb{F}_q)$ is an untwisted finite simple group of Lie type of rank $l \leq n$ over a finite field $\mathbb{F}_q$, then for every p and every simple $\mathbb{F}_p[G]$-module,*

$$\dim_{\mathbb{F}_p} H^2(G,M) \leq C_3 \dim_{\mathbb{F}_p} M$$

The proof of the main theorem is by reduction via a Theorem of Curtis and Tits (Theorem 2.1 below) to the cases of rank 1 and 2. The rank 1 case is due to Campbell, Robertson and Williams [CRW] from whom we also borrowed an elegant argument, which we name the CRW-trick, which we use frequently (see Section 3). Most of our work is to deal with the rank 2 cases. To do this, we use a theorem of Tits (Theorem 3.4 below) which takes us essentially to the minimal parabolic subgroups. Those we treat by writing Chevalley relations (á la [GLS3], Theorem 1.12.1).

Finally, we mention, that our method of proof is explicit, and if one wants, the explicit bounded presentations can be written. But they are, probably, far from optimal. It will be of interest anyway to give some bounds on $C(n)$ of Theorem 1.1. Our proof shows, that $C(n) = O(n^2)$.

Acknowledgements. We would like to acknowledge the support by the ISF and BSF (USA-Israel). We would especially like to thank for support the Department of Mathematics of Hebrew University in Jerusalem, where most of this work was done while the first author was visiting there.

We are also grateful to Avinoam Mann who provided us with some useful background information.

2. Proof of the Theorem.

Let G be an untwisted group of Lie type over a finite field. We can use the following result of Curtis and Tits ([GLS1], 27.3) to reduce the problem to groups of rank 1 and 2.

Theorem 2.1. (**Curtis – Tits** [**GLS1**]). *Let G be a finite group of Lie type. In a Bruhat decomposition of G, let Σ be the root system and X_α ($\alpha \in \Sigma$) the corresponding root subgroups. Let Π be a fundamental system in Σ and for each $\alpha \in \Pi$, let $I_\alpha = \langle X_\alpha, X_{-\alpha} \rangle$. Assume that $|\Pi| \geq 3$. Then the relations among the elements of the groups I_α holding in the groups $\langle I_\alpha, I_\beta \rangle$, $\alpha, \beta \in \Pi$, form a set of defining relations for a central extension of G.*

As $\langle I_\alpha, I_\beta \rangle$ is a semisimple group of rank 2, the proof is indeed reduced to proving the result for the groups of rank 1 and 2. This will be done in Section 3.

3. Groups of Ranks 1 and 2.

In this section we will deal with the presentations of untwisted groups of Lie type of ranks 1 and 2.

Definition 3.1. *Let $G_l(q)$, $q = r^a$, r a prime, be an untwisted group of Lie type of rank l over a finite field of order q, and $H(q)$ a subgroup of $G_l(q)$. We will call a presentation of $H(q)$ <u>bounded</u> if its size is bounded independently of q.*

The results of [CRW] show that $PSL_2(q)$ has a bounded presentation. In fact, their proof has a lovely trick that we are going to imitate. Let us therefore review it, sending the reader to [CRW] for full details.

In [CRW] the authors start with an unbounded presentation of $G = PSL_2(q)$ ([CRW], eq.(2.1), p.335). The unbounded part consists of commutator relations whose goal is to ensure that all the elements of U, the unipotent subgroup of the upper triangular Borel subgroup B of G, commute with each other. The trick of [CRW] is to define a group K presented by a bounded number of generators and relations which is mapped onto B. They then show ([CRW], Theorem 2.1, p.36), that K is metabelian of exponent r, and that its commutator subgroup K' (which is abelian) is mapped onto U. This enables them to replace all the commutator relations mentioned above by the boundedly many relations of K, and still ensure that U is abelian. This way, they replace the unbounded presentation of $PSL_2(q)$ by a bounded one.

This method works word by word also for $SL_2(q)$. We will later refer to their argument as the CRW-trick.

From the cases of $SL_2(q)$ and $PSL_2(q)$, we can easily deduce:

Lemma 3.2. (1) *The group $GL_2(q)$ has a bounded presentation.*
(2) *Any central product of two groups of type $A_1(q)$ has a bounded presentation.*
(3) *Any central product of $A_1(q)$ and a cyclic group has a bounded presentation.*

Remark 3.3. *When it is not important to specify which version (adjoint or universal) of a group we are working with, we will use the usual Lie notation (cf.* [Ca] *or* [GLS3]*). For example, $A_1(q)$ stands for either $SL_2(q)$ or $PSL_2(q)$.*

Proof. (1) $GL_2(q)$ has a subgroup of index at most 2, call it $Y(q)$, which is a central product of $SL_2(q)$ and a cyclic group T. Just like the standard argument that a group is finitely presented if and only if a finite index subgroup is, we see that $GL_2(q)$ is boundedly presented iff $Y(q)$ is. Now, $SL_2(q) \times T$ is clearly boundedly presented, and quotienting out a cyclic group keeps the presentation bounded.
(2) and (3) are clear. □

Let G be now an untwisted quasisimple group of rank 2 (with Π being its fundamental root system). To show that G has a bounded presentation, we will use the following theorem of Tits ([Se], p.92).

Theorem 3.4. (**Tits** [**Se**]). *Let (G, B, N, S) be a Tits system; for each $s \in S$, let G_s be the corresponding standard parabolic subgroup. Then G is the sum of N and the G_s ($s \in S$) amalgamated along their intersections.*

The theorem actually says, that if $G_{\{\alpha_1\}}$ and $G_{\{\alpha_2\}}$ are the minimal (in this particular case, also maximal) parabolic subgroups of G ($\{\alpha_1, \alpha_2\} = \Pi$), a presentation for G is obtained by taking a union of presentations of $G_{\{\alpha_1\}}$, $G_{\{\alpha_2\}}$ and N, and identifying the intersections $G_{\{\alpha_i\}} \cap N$ for $i = 1, 2$ and $G_{\{\alpha_1\}} \cap G_{\{\alpha_2\}}$. The first two intersections are subgroups of N, and the last one is the Borel subgroup of G. In all cases, these are generated by a bounded number of elements. For the subgroups of N, this is obvious, as N is an extension of an abelian group generated by two elements by a bounded group (the Weyl group). The Borel subgroups of rank 2 groups are also boundedly generated. So, a bounded number of relations is added by these identifications.

Moreover, N has a bounded presentation. Finally, we will show that the parabolic subgroups $G_{\{\alpha_1\}}$ and $G_{\{\alpha_2\}}$ are boundedly presented, which will finish the proof.

Proving that the minimal parabolics are boundedly presented will be done first for $SL_3(q)$ for clarity of exposition. We then treat the general case. From now on, λ will denote a generator for $\mathbb{F}_q^*$.

$A_2(q)$-Case.

Proposition 3.5. *Let $P = U.L$ where $U = F_1 \times F_2 \cong \mathbb{F}_q \times \mathbb{F}_q = \mathbb{F}_q^2$, $L \cong GL_2(q)$, and L acts on U as on the natural module. Then P is boundedly presented.*

Proof. The group P is clearly boundedly generated. One can write a presentation for it consisting of

(a) a bounded presentation for $L \cong GL_2(q)$,
(b) unbounded number of relations expressing the fact that every element of U is of order r,
(c) unbounded number of relations ensuring that $U \cong \mathbb{F}_q^2$ is abelian, and
(d) relations expressing the action of $L \cong GL_2(q)$ on $U \cong \mathbb{F}_q^2$.

The relations in (b) can be replaced by one relation: indeed, all the non-trivial elements of U are conjugate to each other in P, and so, it suffices to declare one of them to be of order r.

For the relations in (c), we can use first the CRW-trick in the following way: for each F_i, we have a cyclic diagonal subgroup T_i of L acting on it with at most two orbits such that $F_i.T_i$ is isomorphic to a Borel subgroup of $SL_2(q)$. We can then use the metabelian group K described above (following Theorem 2.1 of [CRW]) to make F_i abelian with a bounded number of relations.

At this point we still need to ensure that F_1 commutes with F_2. In order to do this, we claim:

Lemma 3.6. *For $\{i, j\} = \{1, 2\}$, there exist diagonal elements t_i, t_j in L such that*

(1) *$\langle t_i \rangle$ centralizes F_j, and*
(2) *$\langle t_i \rangle$ has boundedly many orbits in its action on F_i.*

Proof. Since P is isomorphic to a maximal parabolic subgroup $P_{\{\alpha_1\}}$ of $A_2(q)$ (cf. [Ca] or [GLS3]), it will be convenient to do all the calculations inside $G = SL_3(q)$.

The group L can identified with a subgroup of G:

$$L \cong \begin{bmatrix} L & 0 \\ 0 & * \end{bmatrix} \leq G$$

and F_1 and F_2 with:

$$F_1 \cong \begin{bmatrix} 1 & 0 & F_1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \text{ and } F_2 \cong \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & F_2 \\ 0 & 0 & 1 \end{bmatrix}$$

Now, take

$$t_1 = \begin{bmatrix} \lambda & 0 & 0 \\ 0 & \lambda^{-2} & 0 \\ 0 & 0 & \lambda \end{bmatrix} \text{ and } t_2 = \begin{bmatrix} \lambda^{-2} & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{bmatrix}$$

Clearly, the desired conclusions hold. □

Assuming the lemma, let $\{x_i, y_i, ...\}$ be representatives of the orbits of $\langle t_i \rangle$ on F_i, $i = 1, 2$. Then for $i \neq j$, the relations $1 = [x_i, x_j] = [y_i, y_j] = [x_i, y_j] = ...$ imply all the relations $[x_i^{t_i^r}, x_j^{t_j^s}]$, $[y_i^{t_i^r}, y_j^{t_j^s}]$, $[x_i^{t_i^r}, y_j^{t_j^s}]$, etc., for all r and s, since t_i commutes with t_j and also with x_j and y_j, etc. This shows that all the relations in (c) can be replaced by boundedly many.

Finally, the action of L on $U = F_1 \times F_2$ given by relations (d) is also bounded. Indeed, if $g \in L$, and $u = x_i^{t_i^s}$ as before, then conjugating by g amounts to give

$$g^{-1}t_i^{-s}x_i t_i^s g = (g^{-1}t_i^{-s}g)(g^{-1}x_i g)(g^{-1}t_i^s g)$$

The factors $g^{-1}t_i^{\pm s}g$ are defined by the relations in (a) defining L, so to define the action we need only to specify the way the generators of L act on x_1, y_1, x_2, y_2, etc., again a bounded number of relations. The proposition is now proved. □

Proposition 3.7. *$A_2(q)$ has a bounded presentation.*

Proof. The result follows immediately for $SL_3(q)$ as the minimal parabolics of it are isomorphic to P of Proposition 3.5. To obtain it for $PSL_3(q)$, one can simply quotient out the appropriate central elements. Since $|Z(SL_3(q))| \leq 3$, the result follows. □

General Case.

Again, for general facts about the structure of parabolic subgroups, we refer a reader to either [Ca] or [GLS3].

Let G be a universal version of a rank 2 untwisted quasisimple group, $G \ncong A_2(q)$. If P is its minimal parabolic, then $P = MHU$ ([GLS3], 2.6.5), where MH is a Levi complement of P, and H is a Cartan subgroup of G (see p. 41, 50 of [GLS3]). Then MH is isomorphic either to $GL_2(q)$, or to a central product of $SL_2(q)$ and a cyclic group. So, in any case, it is boundedly presented by Lemma 3.2. Now, U is the unipotent radical of P, and thus is a product of at most 5 root subgroups:

$$U = \Pi_{i=1}^{e} X_i \text{ with } e \leq 5.$$

As in $A_2(q)$-case, P has a presentation with boundedly many generators and unboundedly many relations of the following types:

(a) Boundedly many relations giving a presentation for MH.

(b) For every $i \leq e$, unboundedly many relations expressing the fact that X_i is abelian of exponent r.
(c) For every $1 \leq i \neq j \leq e$, commutator relations giving the commutators of elements of X_i and X_j.
(d) The relations expressing the action of MH on U.

Now, we can find for every $i \leq e$, an element $h_i \in H$ such that $X_i.\langle h_i \rangle$ is isomorphic to a Borel subgroup of $SL_2(q)$, and use the CRW-trick to deduce that the relations of type (b) can be replaced by boundedly many.

Lemma 3.8. *For $1 \leq i \neq j \leq e$, we can find elements $t_i, t_j \in H$ such that the following conditions hold:*

(1) *$\langle t_i \rangle$ acts trivially on X_j, and*
(2) *$\langle t_i \rangle$ has boundedly many orbits in its action on X_i.*

Proof. Let us say that $X_i = X_\alpha$ and $X_j = X_\beta$ where $\alpha, \beta \in \Sigma^+$, $\alpha \neq \beta$.

Proof 1: The roots α and β being linearly independent generate a subgroup of finite index in the group of all algebraic characters of the torus of $\bar{G}$ (the algebraic group corresponding to G) which is isomorphic to $\mathbb{Z}^2$. This index is bounded independently of the type of the group or the characteristic. This implies that $\ker(\chi_\alpha) \cap \ker(\chi_\beta)$ is of bounded order and so $\ker(\chi_\alpha) + \ker(\chi_\beta)$ is of bounded index. Thus $\ker(\chi_\alpha)$ acts with boundedly many orbits on X_β.

It now follows that $\ker(\chi_\alpha)$ acts trivially on X_α and with boundedly many orbits on X_β. The same holds also over every finite field $\mathbb{F}$. We can take there h_i to be an element which generates a bounded index subgroup in the $\mathbb{F}$-points of $\ker(\chi_\alpha)$.

Proof 2: Consider $K := \langle X_\alpha, X_{-\alpha}, X_\beta, X_{-\beta} \rangle$. Let us show that K is centralized by boundedly many elements of H. Assume there exists a non-identity element $h \in C_H(K)$. Let m be such that $o(h^m)$ is a prime. Then Theorem 4.1.9 of [GLS3] implies that $o(h^m) = s \in \{2, 3\}$, and in fact, $|C_G(K)| \leq s \cdot |Z(G)| \leq 6$.

Consider $C_H(X_i)$. Using Theorems 1.12.7 and 2.2.6 of [GLS3], we obtain that $C_H(X_i) \geq H_i$ where $H_i = \langle t_i \rangle \cong \mathbb{F}_q^*$. Now, using the previous paragraph, we see that the number of orbits of H_i on X_j is bounded. $\square$

Assuming the lemma, let $\{x_i, y_i, ...\}$ be representatives of the orbits of $\langle t_i \rangle$ on X_i, $1 \leq i \leq e$. Since t_i commutes with t_j and also with x_j and y_j, etc., for $i \neq j$ and for all r and s, we have

$$[x_i^{t_i^r}, x_j^{t_j^s}] = [x_i^{t_i^r t_j^s}, x_j^{t_j^s t_i^r}] = [x_i, x_j]^{t_i^r t_j^s}$$

$$[y_i^{t_i^r}, y_j^{t_j^s}] = [y_i^{t_i^r t_j^s}, y_j^{t_j^s t_i^r}] = [y_i, y_j]^{t_i^r t_j^s}, \text{ etc.}$$

Thus the relations $[x_i, x_j]$, $[y_i, y_j]$, $[x_i, y_j]$, etc., imply all the relations $[x_i^{t_i^r}, x_j^{t_j^s}]$, $[y_i^{t_i^r}, y_j^{t_j^s}]$, $[x_i^{t_i^r}, y_j^{t_j^s}]$, etc., provided that the action of H on U is

defined. We define $[x_i, x_j]$, $[y_i, y_j]$, $[x_i, y_j]$, etc., appropriately, i.e., to look like the appropriate Chevalley relations of Theorem 1.12.1(b) of [GLS3]. In particular, $[x_i, x_j], [y_i, y_j,], ... \in \{1, x_k, y_k, z_k, ...\}$ for some $k \in \{1, ..., e\} - \{i, j\}$. This shows that all the relations in (c) can be replaced by boundedly many, provided that (d) can be done using boundedly many relations.

Therefore, consider the action of MH on $U = \Pi_{i=1}^{e} X_i$. If $g \in MH$, and $u = x_i^{t_i^s}$ as before, then conjugating by g amounts to giving

$$g^{-1}t_i^{-s}x_i t_i^s g = (g^{-1}t_i^{-s}g)(g^{-1}x_i g)(g^{-1}t_i^s g)$$

The factors $g^{-1}t_i^{\pm s}g$ are defined by the relations in (a) defining MH, so to define the action we need only to specify the way the generators of LH act on x_1, y_1, x_2, y_2, etc., again a bounded number of relations. Hence, we can now prove:

Proposition 3.9. *If G is an untwisted group of rank 2, G has a bounded presentation.*

Proof. Let G_u be the universal version of G. We have shown above that a minimal parabolic of G_u has a bounded presentation. Thus, by Theorem 3.4, G_u is boundedly presented. Now, a bounded presentation of G follows immediately, since $|Z(G_u)|$ is bounded. □

References

[AG] M. Aschbacher, R. Guralnick. Some applications of the first cohomology group. J. Algebra **90** (1984), no. 2, 446–460.

[BGKLP] L. Babai, A.J. Goodman, W.M. Kantor, E.M. Luks, P.P. Plfy. Short presentations for finite groups. J. Algebra **194** (1997), no. 1, 79–112.

[Ca] R.W. Carter. Simple groups of Lie type. Pure and Applied Mathematics, Vol. 28 (1972).

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

[CRW] C.M. Campbell, E.F. Robertson, P.D. Williams. On presentations of $\mathrm{PSL}(2, p^n)$. J. Austral. Math. Soc. Ser. A **48** (1990), no. 2, 333–346.

[GLS1] D. Gorenstein, R. Lyons, R. Solomon. The Classification of the Finite Simple Groups, Number 1. Amer. Math. Soc. Surveys and Monographs **40**, #**1** (1995).

[GLS3] D. Gorenstein, R. Lyons, R. Solomon. The Classification of the Finite Simple Groups, Number 3. Amer. Math. Soc. Surveys and Monographs **40**, #**3** (1998).

[H] D.F. Holt. On the second cohomology group of a finite group. Proc. London Math. Soc. **55** (1987), no. 1, 22–36.

[H1] D.F. Holt. Computation of cohomology groups and enumeration of finite perfect groups. Computers in algebra (Chicago, IL (1985)), 67–70, Lecture Notes in Pure and Appl. Math., 111, (1988).

[Lu1] A. Lubotzky. Enumerating boundedly generated finite groups. J. Algebra **238** (2001), no. 1, 194–199.

[Lu2] A. Lubotzky. Pro-finite presentations. J. Algebra **242** (2001), no. 2, 672–690.

[Lu3] A. Lubotzky. Finite presentations of adelic groups, the congruence kernel and cohomology of finite simple groups. Quaterly Journal of Pure and Applied Mathematics **1** (2005). To appear.

[Se] J.-P. Serre. Trees. Springer Monographs in Mathematics. Springer-Verlag, Berlin (2003).

Inna Korchagina
School of Mathematics
University of Birmingham
Birmingham
UK B15 2TT
innako@for.mat.bham.ac.uk

Alexander Lubotzky
Einstein Institute of Mathematics
The Hebrew University of Jerusalem
Jerusalem
Israel 91904
alexlub@math.huji.ac.il