Journal of Algebra ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Remarks on proficient groups [☆]

R.M. Guralnick [a,*], W.M. Kantor [b], M. Kassabov [c], A. Lubotzky [d]

[a] Department of Mathematics, University of Southern California, Los Angeles, CA 90089-2532, USA
[b] Department of Mathematics, University of Oregon, Eugene, OR 97403, USA
[c] Department of Mathematics, Cornell University, Ithaca, NY 14853-4201, USA
[d] Department of Mathematics, Hebrew University, Givat Ram, Jerusalem 91904, Israel

ARTICLE INFO

Article history:
Received 29 July 2008
Available online xxxx
Communicated by Peter Webb

Dedicated to the memory of Karl Gruenberg

Keywords:
Presentations of finite groups
Proficient groups
Efficient groups
Profinite groups
Cohomology

ABSTRACT

If a finite group G has a presentation with d generators and r relations, it is well known that $r - d$ is at least the rank of the Schur multiplier of G; a presentation is called *efficient* if equality holds. There is an analogous definition for *proficient* profinite presentations. We show that many perfect groups have proficient presentations. Moreover, we prove that infinitely many alternating groups, symmetric groups and their double covers have proficient presentations.

1. Introduction

For a group H, we denote by $d(H)$ the minimal number of generators of H. If $N \lhd H$, we denote by $d_H(N)$ the minimal number of generators of N as a normal subgroup of H.

A finite group G has a *presentation with d generators and r relations* if there is an exact sequence

$$1 \to R \to F \to G \to 1, \tag{1.1}$$

[☆] The authors were partially supported by NSF grants DMS 0653873, DMS 0242983, DMS 0600244 and DMS 0354731.

[*] Corresponding author.
E-mail addresses: guralnic@usc.edu (R.M. Guralnick), kantor@math.uoregon.edu (W.M. Kantor), kassabov@math.cornell.edu (M. Kassabov), alexlub@math.huji.ac.il (A. Lubotzky).

0021-8693/$ – see front matter © 2009 Elsevier Inc. All rights reserved.
doi:10.1016/j.jalgebra.2009.05.018

where F is a free group on d generators and $d_F(R) = r$. Similarly, G has a *profinite presentation with d generators and r relations* if there is an exact sequence

$$1 \to \widehat{R} \to \widehat{F} \to G \to 1, \tag{1.2}$$

where $\widehat{F}$ is the free profinite group on d generators and $d_{\widehat{F}}(\widehat{R}) = r$; here $d_{\widehat{F}}(\widehat{R})$ is the minimal number of normal generators of $\widehat{R}$ in the topological sense, i.e., as a normal closed subgroup of $\widehat{F}$.

It is known (1.6) that, if G has a (profinite) presentation with d generators and r relations, then $r - d \geqslant d(M(G))$, where $M(G)$ is the Schur multiplier of G. A presentation (resp. profinite presentation) is called *efficient* (resp. *proficient*) if $r - d = d(M(G))$; and G is called *efficient* (resp. *proficient*) if it has an efficient (resp. proficient) presentation. It is also known that if a finite group G has a proficient presentation, then it has a proficient presentation with only $d(G)$ generators (cf. Proposition 2.5). The analogous result in the category of discrete groups is an old open problem (cf. [Gru, p. 2]).

The notion of efficient presentations is relatively old, but the list of perfect groups or 2-generated groups known to have such presentations is very limited. The only infinite family of simple groups presently known to have efficient presentations consists of the groups $\mathrm{PSL}(2, p)$ with $p > 3$ prime [Sun]; $\mathrm{SL}(2, p)$, $p > 3$, also has an efficient presentation [CR1]. In addition, $\mathrm{PSL}(2, p) \times \mathrm{PSL}(2, p)$ has an efficient presentation for each prime $p > 3$ [CRW3], as do $\mathrm{SL}(2, p) \times \mathrm{PSL}(2, p)$, $\mathrm{PSL}(2, p)^3$, $\mathrm{PSL}(2, p) \times A_6$, $\mathrm{PSL}(2, 5)^4$ and most "small" simple groups [Ro,CMRW,CR2,CRW2,CRKMW,CHRR1, CHRR2]. Also $\mathrm{SL}(2, \mathbb{Z}/m)$ is efficient for any odd integer m [CR1, p. 19] (compare [CRW1, p. 70]), and hence so is any quotient by a subgroup of its center. On the other hand, Harlander [Ha, Corollary 5.4] has shown that, for any finite group G, $G \times P$ is efficient for a sufficiently large elementary abelian p-group P (in particular, every perfect group is the derived group of an efficient group). Note that these groups have a very large number of generators and a much larger number of relations. See also [El].

The notion of proficient presentations was introduced by Gruenberg and Kovács in [GrK]. An efficient presentation gives rise to a proficient one, so all efficient groups are proficient. The present note is an offshoot of our result in [GKKL3] that, for primes $p \equiv 11 \bmod 12$, $A_{p+2} \times T$ has an efficient presentation, where T is the subgroup of index 2 in $\mathrm{AGL}(2, p)$. Combined with the cohomological methods of [GKKL2] we will provide further examples of proficient groups which are perfect (or very close to perfect). Indeed, for any $d > 1$ we provide infinitely many examples of perfect groups G such that G has a profinite presentation with $d = d(G)$ generators and d relations (see Corollary 1.16). By contrast, there appear to be no examples known of finite groups that have presentations with $d(G)$ generators and $d(G)$ relations when $d(G) > 3$. By the Golod–Shavarevich Theorem [Se, p. 66], this cannot occur for finite nilpotent groups.

For a finite group G we denote by $r(G)$ (resp. $\hat{r}(G)$) the minimal number of relations needed to define G, i.e., the minimum of $d_F(R)$ over all presentations (1.1) of G (or of $d_{\widehat{F}}(R)$ in (1.2)). Clearly,

$$\hat{r}(G) \leqslant r(G). \tag{1.3}$$

It is a central open problem in the area of presentations of finite groups whether (1.3) is always an equality (cf. [Gru, p. 2]). Indeed, Serre [Se, p. 34] stated that for 30 years he had seen "no reason ... why this should always be an equality". As a special case, in view of the results in this paper it is especially interesting to ask whether there are proficient finite groups that are not efficient.

We recall a cohomological interpretation of $\hat{r}(G)$ (see [GrK,Lu]). If M is a finite-dimensional kG-module for a field k, define

$$\nu_2(M) := \left\lceil \frac{\dim H^2(G, M) - \dim H^1(G, M) + \dim H^0(G, M)}{\dim M} \right\rceil.$$

Then

$$\hat{r}(G) - d(G) = \max_{p,M} \nu_2(M) - 1, \tag{1.4}$$

where p runs over all primes and M runs over all irreducible $\mathbb{F}_pG$-modules. It is well known (see Lemma 2.3) that the rank of the Sylow p-subgroup of $M(G)$ is $\dim H^2(G,\mathbb{F}_p) - \dim H^1(G,\mathbb{F}_p) = \nu_2(\mathbb{F}_p) - 1$, where $\mathbb{F}_p$ is viewed as the trivial $\mathbb{F}_pG$-module. Hence,

$$d\bigl(M(G)\bigr) = \max_p \nu_2(\mathbb{F}_p) - 1. \tag{1.5}$$

Thus (1.4) and (1.5) imply that

$$\hat{r}(G) \geqslant d(G) + d\bigl(M(G)\bigr). \tag{1.6}$$

By definition, a group G is proficient if and only if this inequality is an equality. By (1.4), this happens if and only if

$$\max_{p,M} \nu_2(M) \leqslant \max_p \nu_2(\mathbb{F}_p) = 1 + \max_p\bigl(\dim H^2(G,\mathbb{F}_p) - \dim H^1(G,\mathbb{F}_p)\bigr), \tag{1.7}$$

where p runs over all primes and M over all nontrivial irreducible $\mathbb{F}_pG$-modules. That is, *G is proficient if and only if $\max_{p,M} \nu_2(M)$ is attained when M is the trivial module $\mathbb{F}_p$ for some prime p*. Thus, for proficiency but not efficiency, we have a cohomological interpretation that is crucial in this paper.

While many finite groups are proficient (cf. Proposition 2.1 for all finite nilpotent groups), not all finite solvable groups are (see [Sw] and Section 7).

In [GrK, (2.6)] it is shown that, if G is any finite group and H is not a superperfect group (recall H is superperfect if for all p, $H^1(H,\mathbb{F}_p) = H^2(H,\mathbb{F}_p) = 0$), then $G \times H^k$ is proficient for all sufficiently large k. In particular, every finite group G is a direct factor of a proficient group (by [Ha] in fact every finite group is a direct summand of a finite efficient group). In Section 7, we will see that every finite group is also a direct factor of a nonproficient finite group (and so also a nonefficient one).

A method similar to that in [GrK], combined with our quantitative results from [GKKL2], yields

Theorem 1.8.

(a) *If G is a direct product of 2 or more simple alternating groups, then G is proficient.*
(b) *If G is a direct product of finite quasisimple groups and if $d(M(G)) \geqslant 16$, then G is proficient.*
(c) *If G is a direct product of quasisimple groups each of which is a covering group of $\mathrm{PSL}(2,q_i)$ for some prime power $q_i > 3$, then G is proficient.*

A basic related question is the following:

Conjecture 1.9. *Every finite simple group S and its universal cover $\tilde{S}$ are proficient.*

Here it is clear that, if $\tilde{S}$ is efficient or proficient, then so is S (a presentation for $S = \tilde{S}/Z$ is obtained by taking one for $\tilde{S}$ and killing generators for $Z \cong M(S)$ — indeed this observation is also obvious for finite perfect groups).

Since $d(\tilde{S}) = 2$, $\tilde{S}$ is proficient if and only if it has a profinite presentation with 2 generators and 2 relations (cf. Proposition 2.5). Wilson [Wi] conjectured that $\tilde{S}$ even has such a discrete presentation, so his conjecture implies the previous one.

As $H^1(\tilde{S},\mathbb{F}_p) = H^2(\tilde{S},\mathbb{F}_p) = 0$ for all p, (1.7) and (1.4) imply that Conjecture 1.9 is equivalent to:

Conjecture 1.10. *For every finite simple group S, every prime p and every nontrivial irreducible $\mathbb{F}_p\tilde{S}$-module M,*

$$\dim H^2(\tilde{S},M) - \dim H^1(\tilde{S},M) \leqslant \dim M.$$

It is known that $\dim H^1(\tilde{S}, M)$ is relatively small with respect to $\dim M$ (in [GH] it is shown that $\dim H^1(\tilde{S}, M) \leqslant (1/2)\dim M$ for each finite-dimensional $\tilde{S}$-module M). Therefore the following stronger version of the preceding conjecture seems likely:

Conjecture 1.11. *For every finite quasisimple group S, every prime p and every $\mathbb{F}_p S$-module M,*

$$\dim H^2(\tilde{S}, M) \leqslant \dim M.$$

Note that if S is a finite quasisimple group and $\tilde{S}$ satisfies Conjecture 1.11, then it satisfies the two earlier conjectures as well, and so, as noted above, every homomorphic image of $\tilde{S}$ is proficient.

Our general result [GKKL2, Theorem B] approximates this:

Theorem 1.12. *For every finite quasisimple group S, every prime p and every $\mathbb{F}_p S$-module M,*

$$\dim H^2(\tilde{S}, M) \leqslant (17.5)\dim M.$$

Thus, the preceding conjecture drops the constant 17.5 to 1, and in some cases there are even much stronger bounds. However, decreasing 17.5 to 1 in general would need new ideas.

In addition to the simple groups known to be efficient (and hence also proficient), $\mathrm{Sz}(2^{2k+1})$ is proficient and satisfies Conjecture 1.11 [Wi]. By [GKKL2, Theorems 7.2, 7.3], $\mathrm{SL}(2,q)$ and $\mathrm{PSL}(2,q)$ also satisfy Conjecture 1.11, whence they are proficient.

The main results of the present paper add more groups to this list. For example, by Theorem 6.4, if $p \equiv 3 \bmod 4$ is prime then A_{p+2} satisfies Conjecture 1.11:

Theorem 1.13. *If $p \equiv 3 \bmod 4$ is prime and X is a quasisimple group with $X/Z(X) \cong A_{p+2}$, then $\dim H^2(X, M) \leqslant \dim M$.*

In particular, this gives the first known examples of proficient simple groups (and universal covers) where the "rank" goes to infinity — viewing alternating and symmetric groups as groups of Lie type over "the field of order 1" [T].

Theorem 1.14. *Let p be a prime.*

(a) *If $p \equiv 2 \bmod 3$ then S_{p+2} is proficient: it has a profinite presentation with 2 generators and 3 relations;*
(b) *If $p \equiv 3 \bmod 4$ then A_{p+2} and its double cover $2A_{p+2}$ are proficient: A_{p+2} (resp. $2A_{p+2}$) has a profinite presentation with 2 generators and 3 (resp. 2) relations;*
(c) *If $p \equiv 3 \bmod 4$ then S_{p+2} and either double cover $2S_{p+2}$ are proficient: S_{p+2} (resp. $2S_{p+2}$) has a profinite presentation with 2 generators and 3 (resp. 2) relations;*
(d) $\mathrm{SL}(2,q)$ *is proficient for every prime power $q \geqslant 4$;*
(e) $\mathrm{PSL}(3,q)$ *is proficient for every prime power $q \equiv 1 \bmod 3$; and*
(f) $\mathrm{PSL}(4,q)$ *is proficient for every odd q.*

While parts (d)–(f) are immediate applications of our results in [GKKL2, Section 7], parts (a)–(c) require a combination of results on discrete presentations from [GKKL3] together with cohomological arguments. See also [GKKL1]. In particular, we use the following result:

Proposition 1.15. *Let $G = X \times Y$ be a finite group. Suppose G has a profinite presentation with d generators and r relations. If $d(X) = d'$ then X has a profinite presentation with d' generators and $r - (d - d')$ relations.*

We do not know if the analogue of this proposition holds for discrete presentations. This is an interesting subcase of the question whether or not $r(G) = \hat{r}(G)$.

A trivial consequence of the Künneth formula and Theorem 1.14(b), (d) gives the following:

Please cite this article in press as: R.M. Guralnick et al., Remarks on proficient groups, J. Algebra (2009), doi:10.1016/j.jalgebra.2009.05.018

Corollary 1.16. *For $1 \leqslant i \leqslant t$ let G_i be either A_{p_i+2} with $p_i \equiv 3 \bmod 4$ prime or $\mathrm{SL}(2, q_i)$, $q_i > 4$. Let $G = G_1 \times \cdots \times G_t$. Then G has a profinite presentation with $d(G)$ generators and $d(G)$ relations. In particular, for any integer $d > 1$, there exist infinitely many finite perfect groups G that have a profinite presentation with $d = d(G)$ generators and $d(G)$ relations.*

In fact, fix S to be one of the quasisimple groups in the corollary. Then for any integer $d > 1$, there is some t such that $d(S^t) = d$ and so S^t has a profinite presentation with d generators and d relations.

This paper is organized as follows. In Section 2, we give some preliminary results on cohomology. In Section 3, we deduce Proposition 1.15 and prove other results on direct products. Combining this with results in [GKKL2] proves Theorem 1.8. In Section 3 we also prove parts of Theorem 1.14. In Section 4, we give discrete presentations for groups related to covers of alternating groups. In Section 5, we prove further results about cohomology (in particular about the cohomology of amalgamated products). In Section 6, we use our results on discrete presentations and cohomology to prove Theorem 1.13 in characteristic 2; this bound was already proved in odd characteristic in [GKKL2, Theorem 6.2]. We then complete the proof of Theorem 1.14. In the final section, we give a general construction of nonproficient perfect groups.

This paper is dedicated to the memory of Karl Gruenberg whose major contributions to the subject of discrete and profinite presentations have been an inspiration to many.

2. Cohomology and preliminaries

If G is a finite nilpotent group and M is an irreducible $\mathbb{F}_pG$-module, then either M is trivial or some normal p'-subgroup of G acts without fixed points. In the latter case, $H^i(G, M) = 0$ for all i (see [GKKL2, Corollary 3.12(2)]). Thus, we have the following trivial consequence of (1.7):

Proposition 2.1. *All finite nilpotent groups are proficient.*

The *inflation restriction sequence* will be used frequently (see [Gru, 2.6]):

Lemma 2.2. *Let M be a $\mathbb{Z}G$-module for a (possibly infinite) group G. If N is a normal subgroup of G, then there is an exact sequence*

$$0 \to H^1\big(G/N, M^N\big) \to H^1(G, M) \to H^1(N, M)^G \to H^2\big(G/N, M^N\big) \to H^2(G, M).$$

We will most often use this when N acts trivially on M, in which case $M^N = M$ and $H^1(N, M)^G = \mathrm{Hom}_{G/N}(N/[N, N], M)$.

We next recall a well-known result about the rank of the Schur multiplier $M(G) = H^2(G, \mathbb{C}^*)$ of a finite group G:

Lemma 2.3. *Let G be a finite group and p a prime. Then $\dim H^2(G, \mathbb{F}_p) - \dim H^1(G, \mathbb{F}_p)$ is equal to the rank of the Sylow p-subgroup of $M(G)$. In particular, $\dim H^2(G, \mathbb{F}_p) \geqslant \dim H^1(G, \mathbb{F}_p)$.*

Proof. Consider the short exact sequence $0 \to \mathbb{F}_p \to \mathbb{C}^* \to \mathbb{C}^* \to 0$ of $\mathbb{Z}G$-modules, where the map on $\mathbb{C}^*$ is the pth power map. The long exact sequence for cohomology [Br, III.6.2] gives $0 \to H^1(G, \mathbb{F}_p) \to H^1(G, \mathbb{C}^*) \to H^1(G, \mathbb{C}^*) \to H^2(G, \mathbb{F}_p) \to H^2(G, \mathbb{C}^*) \to pH^2(G, \mathbb{C}^*) \to 0$. Thus, $|H^1(G, \mathbb{F}_p)||H^2(G, \mathbb{C}^*) : pH^2(G, \mathbb{C}^*)| = |H^2(G, \mathbb{F}_p)|$, which completes the proof. □

Serre [Se, Proposition 28] gave a proof of the final statement for finite p-groups (although his proof is valid for all finite groups). Of course, the Golod–Shavarevich Theorem implies that $\dim H^2(G, \mathbb{F}_p) - \dim H^1(G, \mathbb{F}_p)$ is usually very large for finite p-groups.

Lemma 2.4. *Let G be a finite group and $N \trianglelefteqslant G$. Let V be an irreducible $\mathbb{F}_pG$-module with N trivial on V. Assume that there is no nontrivial G-equivariant homomorphism from N onto V. Then*

(1) $\dim H^1(G/N, V) = \dim H^1(G, V)$,
(2) $\dim H^2(G, V) \geqslant \dim H^2(G/N, V)$, *and*
(3) $\dim H^2(G, V) - \dim H^1(G, V) \geqslant \dim H^2(G/N, V) - \dim H^1(G/N, V)$.

Proof. (1) and (2) follow from the inflation restriction sequence (Lemma 2.2):

$$0 \to H^1(G/N, V) \to H^1(G, V) \to \mathrm{Hom}_G(N, V) \to H^2(G/N, V) \to H^2(G, V).$$

Then (3) follows from (1) and (2). □

Finally, we state a very useful consequence of [Lu, Theorem 0.1]:

Proposition 2.5. *If G is a finite group having a profinite presentation with d generators and r relations, then G also has a profinite presentation with $d_0 := d(G)$ generators and r_0 relations for which $r_0 - d_0 \leqslant r - d$.*

This is one of the tools that make profinite presentations easier to work with than discrete presentations — and we do not know whether or not the discrete analogue holds.

3. Direct products

We can now prove Proposition 1.15:

Proof of Proposition 1.15. We are assuming that G has a profinite presentation with d generators and r relations. By Proposition 2.5 we may assume that d and r are both minimal. Assume that X has a profinite presentation with $d' = d(X) \leqslant d$ generators and r' relations with r' minimal (again we use Proposition 2.5).

By (1.4), $r' - d'$ is the maximum of $\nu_2(M) - 1$ as p ranges over all primes and M ranges over all irreducible $\mathbb{F}_p X$-modules. Similarly, $r - d$ is defined by the same formula in terms of irreducible G-modules.

We need to show that $r' - d' \leqslant r - d$, and so it suffices to prove that

$$\dim H^2(G, M) - \dim H^1(G, M) \geqslant \dim H^2(X, M) - \dim H^1(X, M)$$

for every prime p and every irreducible $\mathbb{F}_p X$-module (where we view M as an $\mathbb{F}_p G$-module with Y acting trivially).

First suppose that M is a nontrivial $\mathbb{F}_p X$-module. Then M is not a homomorphic image of Y (since X acts trivially on Y but not on M), whence Lemma 2.4 implies the desired inequality (using $N = Y$ and $V = M$).

If $M = \mathbb{F}_p$, the desired inequality follows from Lemma 2.3 since the Schur multiplier of $X \times Y$ contains the Schur multiplier of X. □

This produces an extension of [GrK, 2.8]:

Corollary 3.1. *If $X \times Y$ is a proficient finite group and $d(M(X)) = d(M(X \times Y))$, then X is proficient.*

Proof. By Proposition 1.15 and hypothesis, $d(M(X \times Y)) = r(X \times Y) - d(X \times Y) \geqslant r(X) - d(X) \geqslant d(M(X)) = d(M(X \times Y))$. □

One can extend the corollary by using the same argument as in the proof of Proposition 1.15 to show the following:

Please cite this article in press as: R.M. Guralnick et al., Remarks on proficient groups, J. Algebra (2009), doi:10.1016/j.jalgebra.2009.05.018

Corollary 3.2. *Let G be a finite group with a normal subgroup Y, and let $X := G/Y$. Assume that there is no G-equivariant homomorphism from Y to a nontrivial irreducible X-module. Then $\hat{r}(X) - d(X) \leqslant \max\{\hat{r}(G) - d(G), d(M(X))\}$.*

In particular, if G is proficient and $d(M(X)) = d(M(G))$, then X is proficient.

Proof of Theorem 1.14(a). By [GKKL3, Corollary 3.13(ii)], for any $p \equiv 2 \bmod 3$ there is a group G of index 2 in $S_{p+2} \times \mathrm{AGL}(1, p)$ surjecting onto both factors that has a presentation with 2 generators and 3 relations. Let Y be the kernel of the projection of G onto S_{p+2}. Now apply the preceding corollary. □

Similarly, we can also prove parts of Theorem 1.14(b). Let T be the subgroup of index 2 in $\mathrm{AGL}(1, p)$ with $p \equiv 11 \bmod 12$. By [GKKL3, Corollary 3.8(i)], $A_{p+2} \times T$ has a presentation with 2 generators and 3 relations. By Proposition 1.15, it follows that A_{p+2} a profinite presentation with 2 generators and 3 relations. The remainder of Theorem 1.14(b) will be proved in Section 4, and in Section 6 we will prove the remaining parts of Theorem 1.14 (e.g., primes $p \equiv 3 \bmod 4$ are dealt with in Theorem 6.4).

The next result is a special case of a result about direct products in [GrK, 2.7].

Lemma 3.3. *Let G_i, $1 \leqslant i \leqslant t$ (for $t \geqslant 2$), be finite perfect groups each of which has a presentation with 2 generators and r_i profinite relations. Set $X = \prod_{i=1}^{t} G_i$. Then*

$$\hat{r}(X) - d(X) \leqslant \max\bigl\{d\bigl(M(X)\bigr), r_i - 2 \bigm| i = 1, \ldots, t\bigr\}. \tag{3.4}$$

In particular, if $d(M(X)) \geqslant \max_i r_i - 2$ then X is proficient.

Proof. Recall by (1.4) that

$$r_i - 2 \geqslant \max_{p,N} \nu_2(N) - 1, \tag{3.5}$$

where p runs over all primes and N over all irreducible $\mathbb{F}_p G_i$-modules. We know from (1.4) that $\hat{r}(X) - d(X) = \max_{p,N} \nu_2(M) - 1$, where M runs over all irreducible $\mathbb{F}_p X$-modules. Thus, we have to prove that, for every such M,

$$\nu_2(M) \leqslant \max\bigl\{d\bigl(M(X)\bigr) + 1, r_i - 1 \bigm| i = 1, \ldots, t\bigr\}. \tag{3.6}$$

If M is the trivial module then, by (1.5), $\nu_2(M) \leqslant d(M(X)) + 1$. So assume that M is nontrivial. By [GKKL2, Lemma 3.2], we may consider modules over a splitting field F for X. Then $M = \bigotimes_{i=1}^{t} M_i$ for irreducible FG_i-modules M_i. If at least 3 of the M_i are nontrivial then, by the Künneth formula (cf. [GKKL2, Lemma 3.1]), $H^2(X, M) = 0 = H^1(X, M)$ and (3.4) holds.

If exactly 2 of the M_i, say M_1 and M_2, are nontrivial then $H^1(X, M) = 0$ and $H^2(X, M) \cong H^1(G_1, M_1) \otimes H^1(G_2, M_2)$, again by the Künneth formula. As the G_i are 2-generated, $\dim H^1(G_i, M_i) \leqslant \dim M_i$ and hence $\dim H^2(X, M) \leqslant \dim M$ and $\nu_2(M) \leqslant 1$, so that (3.4) again holds.

Finally, if only M_1 is nontrivial, then the Künneth formula gives $H^2(X, M) \cong H^2(G_1, M_1)$, $H^1(X, M) \cong H^1(G_1, M_1)$ since $\dim H^0(G_i, M_i) = 1$ and $H^1(G_i, M_i) = 0$ for $i > 1$. Thus, this time $\nu_2(M) = \nu_2(M_1)$. By (3.5), $\nu_2(M_1) \leqslant r_1 - 1$, and so again (3.4) holds. □

Proof of Theorem 1.8. By [GKKL2, Theorem B], every finite quasisimple group G has a profinite presentation with 2 generators and 18 relations. In particular, $r - d(G) \leqslant 16$ for any finite quasisimple group. Similarly, by [GKKL2, Theorem D], every alternating group has a profinite presentation with 2 generators and 4 relations. Also, $\mathrm{SL}(2, q)$ has a profinite presentation with 2 generators and 2 relations by [GKKL2, Section 7]. Thus, Theorem 1.8 follows from Lemma 3.3. □

4. Some discrete presentations

Carmichael [Car] proved that A_{n+2} has a presentation

$$\langle x_1,\dots,x_n \mid x_i^3=1,\ (x_ix_j)^2=1,\ 1\leqslant i\neq j\leqslant n\rangle. \tag{4.1}$$

We first observe that this can be modified to give a presentation for the double cover $2A_{n+2}$:

Proposition 4.2. *If $n\geqslant 3$ and $J=\langle x_1,\dots,x_n \mid x_i^3=(x_ix_j)^2,\ 1\leqslant i\neq j\leqslant n\rangle$, then $J\cong 2A_{n+2}$.*

Proof. There is a surjection $\phi: J\to 2A_{n+2}$ sending x_i to the element $(i,n+1,n+2)z$ of order 6 for $1\leqslant i\leqslant n$, where z is the central involution in $2A_{n+2}$. Namely, x_ix_j is a product of two disjoint transpositions as an element of A_{n+2}, and hence has order 4 in $2A_{n+2}$.

Set $w:=x_1^3=(x_1x_2)^2$ and $Q:=\langle x_1,x_2\rangle\leqslant J$. Then $\phi(Q)=2A_4=\mathrm{SL}(2,3)$. Since w commutes with x_1 and x_1x_2 it is central in Q. Also, in $Q/[Q,Q]$ we have $x_1\equiv x_2^2$ and $x_2\equiv x_1^2$, and hence $x_1\equiv x_1^4$, so that $w=x_1^3\in[Q,Q]$. Now $Q/\langle w\rangle$ is generated by 2 elements of order 3 whose product is an involution. By (4.1), $Q/\langle w\rangle\cong A_4$. Thus, Q is a cover of A_4 and so $Q\cong\mathrm{SL}(2,3)$. In particular, x_1 has order 6 and $x_2^3=x_1^3$.

Consequently, $w=x_i^3$ for all i and so w is a central involution in J. Also, w is contained in $[Q,Q]\leqslant[J,J]$. By (4.1), $J/\langle w\rangle$ is a homomorphic image of A_{n+2}, and so is isomorphic to A_{n+2}. Thus $J\cong 2A_{n+2}$. □

We use this to give a presentation for a group having as a direct factor the double cover of a suitable alternating group (cf. [GKKL3, Corollary 3.8(i)]):

Proposition 4.3. *For a prime $p\equiv 11 \bmod 12$, let*

$$J:=\langle g,u \mid u^p=v^{(p-1)/2},\ (u^s)^v=u^{s-1},\ (ww^u)^2=w^3\rangle,$$

where $s(e-1)\equiv -1 \bmod p$ for an integer e having multiplicative order $(p-1)/2 \bmod p$, while $v:=g^6$ and $w:=g^{(p-1)/2}$. Then $J\cong 2A_{p+2}\times T$, where T is the subgroup of index 2 in $\mathrm{AGL}(1,p)$.

Proof. Throughout this section we view A_p as acting on $\mathbb{F}_p$ and A_{p+2} as acting on $\mathbb{F}_p\cup\{p+1,p+2\}$. By [Neu],

$$T=\langle u_0,v_0 \mid u_0^p=v_0^{(p-1)/2},\ (u_0^s)^{v_0}=u_0^{s-1}\rangle, \tag{4.4}$$

where u_0 corresponds to $x\mapsto x+1$ and v_0 corresponds to $x\mapsto ex$, acting on $\mathbb{F}_p$.

We first show that there is a surjection $\phi: J\to 2A_{p+2}\times T$. Let z be the central involution of $2A_{p+2}$. Write $T=\langle u_0,v_0\rangle$ as above; since it has odd order, its preimage in $2A_p$ has a subgroup we can identify with T. Consequently, we can view $T<2A_{p+2}$ with T fixing $p+1$ and $p+2$, while v_0 fixes 0 as well. Now define ϕ by $\phi(u)=(u_0,u_0)$ and $\phi(g)=(v_0g_0,v_0)$, where $g_0:=(0,p+1,p+2)z\in 2A_{p+2}$ has order 6 and commutes with v_0. Since $g^6\mapsto(v_0^6,v_0^6)$ and $|v_0^6|=|v_0|$ (recall that $p\equiv 11 \bmod 12$), this embeds T diagonally into $\phi(J)$; and since $g^{p-1}\mapsto(g_0^{-1},1)$ ϕ is a surjection.

Now consider the group J. By (4.4) we can identify T with the subgroup $\langle u,v\rangle$. Since v centralizes w, $\Omega:=w^T$ has size at most p, and hence the size is p since $|\phi(\Omega)|\geqslant p$. Thus, T acts on Ω as it does on $\mathbb{F}_p$. In particular, since $p\equiv 3 \bmod 4$, T acts transitively on the 2-element subsets of Ω.

There is an integer k such that $-k$ and $k-1$ are nonzero squares mod p. We claim that $x:=w$, $y:=w^u$ and $z:=w^{u^k}$ satisfy the relations

$$x^6=y^6=z^6=1,\qquad x^3=(xy)^2=(yx)^2,\qquad y^3=(yz)^2=(zy)^2,\qquad z^3=(zx)^2=(xz)^2. \tag{4.5}$$

The first 3 of these follow from $w^6 = 1$, which holds since $v^{(p-1)/2} = 1$ by (4.4). Moreover, in view of the last relation defining J, w centralizes $w^3 = (ww^u)^2$ and conjugates $(ww^u)^2$ to $(w^u w)^2$, so $(xy)^2 = (yx)^2$. Note that T has an element sending the ordered pair (w, w^u) to (w^{u^i}, w^{u^j}) if and only if $j - i$ is a (nonzero) square mod p. In view of our choice of k, (w^{u^k}, w) and (w^u, w^{u^k}) are both in the T-orbit of (w, w^u). This proves the last 2 relations in (4.5).

The group $\langle x, y, z\rangle$ given by the relations (4.5) is isomorphic to $\mathrm{SL}(2,5) = 2A_5$; this was checked using GAP (by A. Hulpke) and using Magma. Thus, $x^3 = y^3$ is the unique involution in $\mathrm{SL}(2,5)$, so that $(w^u)^3 = w^3 = (ww^u)^2 = (w^u w)^2$ in J.

Since T is 2-homogeneous on Ω, the preceding proposition now implies that $N := \langle\Omega\rangle \cong 2A_{p+2}$. Clearly, T and w normalize N, whence N is normal in J. So $J = NT$ and hence $|J| \leqslant |2A_{p+2}||T|$, as required. □

Since either T or $T \times \mathbb{Z}/2$ can be generated by a single conjugacy class, we can add one extra relation to obtain:

Corollary 4.6. *For any prime $p \equiv 11 \bmod 12$, both A_{p+2} and $2A_{p+2}$ have presentations with 2 generators and 4 relations.*

For A_{p+2}, this is already proved in [GKKL3].

Proposition 1.15 now implies that there is even a profinite presentation of $2A_{p+2}$ with 2 generators and only 3 relations, proving part of Theorem 1.14(b) when $p \equiv 11 \bmod 12$. For the more general case $p \equiv 3 \bmod 4$ we will need more tools (see Theorem 6.5).

We finish this section by restating and generalizing some of our earlier results, as well as [GKKL3, Corollary 3.8], in terms of amalgamated products.

Lemma 4.7. *Let $p \equiv 3 \bmod 4$ be prime. Let T be the subgroup of index 2 in $\mathrm{AGL}(1,p)$. Then $A_{p+2} \times T = X/N$, where*

(i) *X is the (free) amalgamated product of A and T with $A \cap T = C$ cyclic of order $(p-1)/2$ and $A \cong \mathbb{Z}/(3) \times C$, and*
(ii) *N is the normal closure in X of a single element x^2, $x \in X$.*

Proof. Let X be the given amalgamated product. Write $A = \langle a\rangle \times \langle c\rangle$ where $a^3 = 1$ and c generates C. Let $T = \langle u, v\rangle$ where $u^p = 1$, v normalizes $\langle u\rangle$ and v has order $(p-1)/2$. We identify v with c, so that X has the presentation

$$X = \bigl\langle a, u, v \bigm| a^3 = v^{(p-1)/2} = [a, v] = 1,\ u^p = 1,\ u^v = u^e\bigr\rangle$$

for an integer e of order $(p-1)/2$ mod p. We identify T with a subgroup of $A_p < A_{p+2}$ acting on $\mathbb{F}_p$, fixing $\{p+1, p+2\}$, and such that v fixes $0 \in \mathbb{F}_p$.

There is a surjection $\phi : X \to A_{p+2} \times T$ sending $u \mapsto (u, u)$, $v \mapsto (v, v)$ and $a \mapsto (a_0, 1)$ with $a_0 = (0, p+1, p+2) \in A_{p+2}$. We can identify T with the subgroup $\langle u, v\rangle$ of X.

Let $N := \langle (x^2)^X\rangle$ with $x := aa^u$. Since $\phi((aa^u)^2) = ((a_0 a_0^{u_0})^2, 1) = 1$, X/N surjects onto $A_{p+2} \times T$.

Since v centralizes a, as in the proof of Proposition 4.3 we again see that $|a^T| = p$, and hence that T acts transitively on the 2-element subsets of a^T since $p \equiv 3 \bmod 4$. Thus, $(a_1 a_2)^2 \in N$ for every pair of distinct elements $a_1, a_2 \in a^T$. Clearly $\langle a^T\rangle$ is normal in X, so that $\langle a^T\rangle = \langle a^X\rangle$. By (4.1), $\langle a^T\rangle \cong A_{p+2}$. Since $X/\langle a^X\rangle \cong T$, we have $|X/N| \leqslant |A_{p+2}||T|$ and hence $X/N \cong A_{p+2} \times T$, as claimed. □

5. More cohomology

We first prove a result for cohomology of amalgamated products (by which we will always mean *free* amalgamated products). One can prove a more precise version, but we will be only need that $H^2(G, M) = 0$ in restricted situations.

Lemma 5.1. *Let G be the amalgamated product of the groups A and B over C. Let M be a finite-dimensional kG-module. Then*

$$\dim H^2(G, M) \leqslant \dim H^2(A, M) + \dim H^2(B, M) + \dim H^1(C, M).$$

Proof. Let U be the kernel of the natural map $H^2(G, M) \to H^2(A, M) \oplus H^2(B, M)$. Clearly $\dim H^2(G, M) - \dim U \leqslant \dim H^2(A, M) + \dim H^2(B, M)$. Thus, it suffices to show that there is an embedding of U into $H^1(C, M)$.

Let $u \in U$. There is a corresponding extension $1 \to M \to E \xrightarrow{f} G \to 1$, and f splits over both A and B: there are injections $\psi_A : A \to E$ and $\psi_B : B \to E$ such that

$$f\psi_A = 1_A \quad \text{and} \quad f\psi_B = 1_B. \tag{5.2}$$

Let $A_1 := \psi_A(A)$ and $B_1 := \psi_B(B)$.

The maps ψ_A and ψ_B produce splittings of $1 \to M \to f^{-1}(C) \to C \to 1$, and hence also define derivations δ_A and δ_B from C to M. Replacing A_1 by A_1^m with $m \in M$ changes δ_A by an inner derivation, and hence we obtain a well-defined linear map $U \to H^1(C, M)$. Consequently, $u \mapsto \delta := \delta_A - \delta_B$ induces a linear map $U \to H^1(C, M)$.

We claim that this map is injective. Assume that δ is an inner derivation on C. This means that the splitting $\psi_A|_C$ is obtained from $\psi_B|_C$ by conjugating by an element of M. Therefore, replacing B_1 by a conjugate we may assume that $\psi_A|_C = \psi_B|_C$. By the universal property of $G = A *_C B$, there is a homomorphism $\psi : G \to E$ such that $\psi|_A = \psi_A$ and $\psi|_B = \psi_B$. Since $f\psi = 1_G$ by (5.2), this completes the proof. □

We will use the previous result in the following form:

Corollary 5.3. *Let X be an amalgamated product of finite groups A and B of order prime to p. If V is a finite-dimensional kX-module over a field k of characteristic p, then $H^2(X, V) = 0$.*

Lemma 5.4. *Let $G = X/N$ and let M be a kX-module for some field k, with N acting trivially. View M as a kG-module. Assume that N can be generated by s elements as a normal subgroup of G. Then*

$$\dim H^2(G, M) \leqslant \dim H^2(X, M) + s \dim M.$$

Proof. By the inflation restriction sequence (Lemma 2.2), there is an exact sequence

$$H^1(N, M)^X \to H^2(X/N, M) \to H^2(X, M).$$

Since N acts trivially on M, $H^1(N, M)^X \cong \mathrm{Hom}_X(N, M) \cong \mathrm{Hom}_G(N/[N, N], M)$. Since N can be generated as a normal subgroup by s elements, $N/[N, N]$ can be generated as a G-module by s elements, whence $\dim H^1(N, M)^X \leqslant s \dim M$. □

Lemmas 5.1 and 5.4 imply the following (using $X = A * B$ in Lemma 5.4):

Lemma 5.5. *Let G be a group with subgroups A and B such that $G = \langle A, B \mid w_i = 1,\ 1 \leqslant i \leqslant t\rangle$ for words w_i in $A \cup B$. Let M be a finite-dimensional kG-module over a field k. Then*

$$\dim H^2(G, M) \leqslant \dim H^2(A, M) + \dim H^2(B, M) + t \dim M.$$

We will also need the following result [GKKL2, Lemma 4.1(3)] about covering groups (this is stated there for quasisimple groups, but the proof does not use this):

Please cite this article in press as: R.M. Guralnick et al., Remarks on proficient groups, J. Algebra (2009), doi:10.1016/j.jalgebra.2009.05.018

Lemma 5.6. *Let G be a finite group with center Z. Let M be a nontrivial irreducible kG-module with Z trivial on M, where k is a field of characteristic r. Then*

$$\dim H^2(G, M) \leqslant \dim H^2(G/Z, M) + c \dim H^1(G, M),$$

where c is the r-rank of Z.

The next observation is trivial:

Lemma 5.7. *Let G be a finite perfect group and $\tilde{G}$ its universal cover. If $\tilde{G}$ is proficient, then so is G.*

Corollary 5.8. *Let S be a finite perfect group with cyclic Schur multiplier, trivial center and universal cover $\tilde{S}$. If $\dim H^2(S, M) \leqslant \dim M$ for all irreducible S-modules M, then any central quotient of $\tilde{S}$ is proficient.*

Proof. By the previous lemma, it suffices to show that $\tilde{S}$ is proficient. Suppose that M is an irreducible $\mathbb{F}_p\tilde{S}$-module. If $Z(\tilde{S})$ acts nontrivial on M, then $H^j(\tilde{S}, M) = 0$ for all $j \geqslant 0$ by [GKKL2, Corollary 3.12]. In particular, $\nu_2(M) = 0$.

Otherwise, we may also view M as an S-module. By Lemma 5.6 and the hypotheses, $\dim H^2(\tilde{S}, M) - \dim H^1(\tilde{S}, M) \leqslant \dim H^2(S, M) \leqslant \dim M$ for any irreducible $\mathbb{F}_p\tilde{S}$-module M. Thus $\tilde{S}$ is proficient by (1.7). □

6. Cohomology of some alternating groups

In this section, we fix a prime $p \equiv 3 \bmod 4$ and consider A_{p+2} and S_{p+2}. We first improve a bound [GKKL2, Theorem 6.2] for H^2:

Theorem 6.1. *Set $G = A_{p+2}$. Let M be a kG-module for a field k of characteristic r.*

(1) $\dim H^2(G, M) \leqslant \dim M$, *with equality if and only if $r = 2$ and G acts trivially on M.*
(2) *If M is nontrivial and irreducible, then* $\dim H^2(G, M) \leqslant \frac{p-1}{p+1} \dim M$.
(3) *Both A_{p+2} and its double cover are proficient.*

Proof. If $r > 3$, then $\dim H^2(G, M) \leqslant (\dim M)/(r-2) \leqslant \frac{p-1}{p+1} \dim M$ by [GKKL2, Theorem 6.4]. Suppose that $r = 3$. Since $p + 2 \neq 7$ or 8, $\dim H^2(G, M) \leqslant (21/25) \dim M \leqslant \frac{p-1}{p+1} \dim M$ unless $p = 3$ or 7, by [GKKL2, Theorem 6.5]. If $p = 3$, by inspection $\dim H^2(G, M) \leqslant 1$ and the result holds. If $p = 7$, then $\dim H^2(G, M) \leqslant (3/5) \dim M$ by [GKKL2, Theorem 6.5], and the result again holds.

So assume that $r = 2$. Since the Schur multiplier has order 2, we may also assume that M is irreducible and nontrivial, so we need to consider (2).

Write $G = X/N$ with A, T and x^2 as in Lemma 4.7. Since A and T have odd order, $H^2(X, M) = 0$ by Corollary 5.3. By Lemma 2.2, we then have $\dim H^2(G, M) \leqslant \dim \operatorname{Hom}_G(N/[N, N], M)$. Since $N/[N, N]$ is a cyclic G-module, the last term is at most $\dim M$. However, since a (normal) generator $x^2[N, N]$ of $N/[N, N]$ is fixed by the nontrivial element xN, we see that $\dim \operatorname{Hom}_G(N/[N, N], M)$ is at most the dimension of the space $C_M(x)$ of fixed points of x on M.

If $p = 3$, one can verify (2) using Magma. If $p > 3$, by [GuS, Lemma 6.1] G can be generated by $(p+1)/2$ conjugates of any nontrivial element. In particular, G is generated by conjugates $x_1, \ldots, x_{(p+1)/2}$ of x. Then $\dim M = \operatorname{codim} \bigcap_i C_M(x_i) \leqslant \frac{p+1}{2} \operatorname{codim} C_M(x)$, so that $\dim C_M(x) \leqslant \dim M - \frac{2}{p+1}(\dim M) = \frac{p-1}{p+1} \dim M$.

This proves (2) and hence (1), and (3) follows from Corollary 5.8. □

We have now proved Theorem 1.14(b). We still need to prove Theorem 1.14(c), for which we need more information concerning A_{p+2}. We first record a special case of [GuK, Theorem 1].

Lemma 6.2. *If M is a kA_{p+2}-module for any field k, then* $\dim H^1(A_{p+2}, M) \leqslant (\dim M)/(p-1)$.

The same bound holds for kS_{p+2}-modules such that A_{p+2} has no fixed points — for then $H^1(S_{p+2}, M)$ embeds into $H^1(A_{p+2}, M)$ (see [GKKL2, Lemma 3.8(1)]).

Combining the previous two results gives:

Lemma 6.3. *Let k be a field of characteristic r. Let M be a nontrivial irreducible kA_{p+2}-module. Then*

$$\dim H^2(A_{p+2}, M) + \dim H^1(A_{p+2}, M) \leqslant \frac{p^2-p+2}{p^2-1} \dim M \leqslant \dim M.$$

Note that unless $p = 3$, we have a strict inequality above. We can now prove

Theorem 6.4. *Let k be a field of characteristic r. Let G be either S_{p+2} or $2A_{p+2}$. If M is an irreducible kG-module, then* $\dim H^2(G, M) \leqslant \dim M$. *In particular, S_{p+2} and $2A_{p+2}$ are proficient.*

Proof. If M is trivial the result is clear. So assume this is not the case. First suppose that $r \neq 2$. If $G = 2A_{p+2}$, it follows by [GKKL2, Theorem 6.2] that $\dim H^2(G, M) < \dim M$ (noting that the trivial module has trivial H^2). If $G = S_{p+2}$, then M restricted to A_{p+2} is either irreducible or the direct sum of 2 irreducible modules. Since r is odd, $H^2(S_{p+2}, M)$ embeds in $H^2(A_{p+2}, M)$ by [Gru, p. 91], and the result follows.

Now consider $r = 2$. First suppose that $G = S_{p+2}$ with M a nontrivial irreducible S_{p+2}-module. Then M is a direct sum of nontrivial irreducible A_{p+2}-modules. By [GKKL2, Lemma 2.8(2)], $\dim H^2(G, M) \leqslant \dim H^2(A_{p+2}, M) + \dim H^1(A_{p+2}, M)$. By Lemma 6.3, this implies that $\dim H^2(G, M) \leqslant \dim M$.

Similarly, using Lemmas 5.6 and 6.3, if $G = 2A_{p+2}$ then

$$\dim H^2(G, M) \leqslant \dim H^2(A_{p+2}, M) + \dim H^1(A_{p+2}, M) \leqslant \dim M.$$

The result follows by Corollary 5.8. □

Moreover, any double cover of S_{p+2} (which is nonsplit when restricted to A_{p+2}) is proficient:

Theorem 6.5. *Let X be a double cover of S_{p+2} that is nonsplit over A_{p+2}. Then X is proficient: it has a profinite presentation with 2 generators and 2 relations.*

Proof. Let $Z = Z(X)$, and so $|Z| = 2$. Let k be a field of characteristic r with M a nontrivial irreducible kX-module. If $r \neq 2$, then the restriction map from $H^2(X, M)$ to $H^2(2A_{p+2}, M)$ is injective by [Gru, p. 91]. Arguing as above, we see that $\dim H^2(2A_{p+2}, M) = 0$ if Z acts nontrivially and that $\dim H^2(2A_{p+2}, M) = \dim H^2(A_{p+2}, M) \leqslant \dim M$ if Z acts trivially. Thus, $\nu_2(M) \leqslant 1$ for all such M.

If $r = 2$, then Z is trivial on M. Then $\dim H^2(X, M) \leqslant \dim H^2(S_{p+2}, M) + \dim H^1(X, M)$ by Lemma 5.6. Thus, by Corollary 5.8 and definition, $\nu_2(M) \leqslant 1$ for any nontrivial irreducible kX-module.

Suppose that $M = k$ is the trivial module. We claim that $\dim H^2(X, k) = 1$. Since the derived subgroup Y of X is the universal cover of A_{p+2}, we have $H^2(Y, k) = 0$; and since Y is perfect, $H^1(Y, k) = 0$. By [GKKL2, Lemma 3.11], these imply the claim. Clearly, $\dim H^1(X, k) = 1$, whence the result follows. Thus, considering all cases we have $\max_{p,M} \nu_2(M) \leqslant 1$, and hence $\hat{r}_2(X) = 2$ by (1.7). □

Completion of the proof of Theorem 1.14. We have already proved (a). Parts (b) and (c) follow from the two previous results. We now prove (d), (e) and (f). Let k be a field.

(d) By [GKKL2, Theorems 7.2, 7.3], if $q \geqslant 4$ then $\dim H^2(G, M) \leqslant \dim M$ for any $k\,\mathrm{SL}(2, q)$-module M and so $\mathrm{SL}(2, q)$ is proficient by Corollary 5.8.

(e), (f) Let $G = \mathrm{PSL}(3, q)$ with $q \equiv 1 \bmod 3$ or $\mathrm{PSL}(4, q)$ with q odd. Then G has a nontrivial Schur multiplier. Thus, by (1.4) and (1.5), it suffices to observe that $\dim H^2(G, M) \leqslant 2 \dim M$ for any irreducible kG-module M. This is [GKKL2, Theorem E]. □

Finally, we show how our methods can be used to give very good estimates on some second cohomology groups: we give a new and simpler proof of a result of Kleshchev and Premet [KP].

Theorem 6.6. *Let $G = A_n$, $n > 4$. Let M be the nontrivial irreducible composition factor of the permutation module P of dimension n over a field k of characteristic r. Assume that $n > 5$ if $r = 5$ and $n > 9$ if $r = 3$. Then $H^2(G, M) = 0$.*

Proof. We will need a variant of the presentation (4.1) for G. Let $I = \{1, \ldots, n\}$. If J is a subset of I, let G_J be the subgroup which acts on $I \setminus J$ as the alternating group and is trivial on J.

Let X be the free amalgamated product of G_1 and G_n over $G_{1,n}$. Let R be the normal subgroup of X generated by the element $w := (uv)^2$, where $u = (1, 3, 4) \in G_n$ and $v = (3, 4, n) \in G_1$. Let Ω be the set of 3-cycles of the form $(i, 3, 4)$. Note that $u, v \in \Omega$ and that every other element of Ω is in $G_{1,n}$. Then $X/R \cong A_n$ by (4.1).

If $n > 5$, let Y be the free amalgamated product of $G_{1,2}$ and $G_{2,n}$ over $G_{1,2,n}$. We may view Y as a subgroup of X. Then $w \in Y$, and the image of Y in $X/R \cong A_n$ is A_{n-1}. Let S be the normal closure of w in Y. Again, by (4.1), $Y/S \cong A_{n-1}$. Since $S \leqslant R$ we have $R \cap Y = S$.

First suppose that r does not divide n. Then $P = k \oplus M$. By Shapiro's Lemma (e.g., [GKKL2, Lemma 3.3]), $\dim H^2(G, P) = \dim H^2(A_{n-1}, k)$. Thus, $\dim H^2(G, M) = \dim H^2(A_{n-1}, k) - \dim H^2(G, k)$. If $r = 2$, both of the latter quantities are 1. If $r > 3$, or if $r = 3$ and $n > 9$, then both of those quantities are 0 (since $M(A_m) = \mathbb{Z}_2$ if $m = 5$ or $m > 7$ and $M(A_6) = M(A_7) = \mathbb{Z}_6$). Thus, $H^2(G, M) = 0$.

Now assume that $r|n$. By our hypotheses, this implies that $n > 5$ (and $n \geqslant 12$ if $r = 3$). We view M as a kX-module with R acting trivially. Note that M restricted to A_{n-1} is the nontrivial composition factor of the permutation module for A_{n-1}. Thus, by induction, $H^2(A_{n-1}, M) = 0$. Also, by Frobenius reciprocity, $H^1(A_{n-1}, M) = H^1(A_{n-2}, k) = 0$. By the inflation restriction sequence,

$$0 \to H^1(Y/S, M) \to H^1(Y, M) \to \mathrm{Hom}_Y(S, M) \to H^2(Y/S, M) \to H^2(Y, M).$$

Since $Y/S = A_{n-1}$, we know that $H^i(Y/S, M) = 0$ for $i = 1, 2$. Thus, $H^1(Y, M) \cong \mathrm{Hom}_Y(S, M)$.

We claim that $H^1(Y, M) = 0$, and so also $\mathrm{Hom}_Y(S, M) = 0$. Let $D := \mathrm{Der}(Y, M)$. Let $f : D \to \mathrm{Der}(G_{1,2}, M)$ be the restriction map. Note that M is the permutation module for $G_{1,2} \cong A_{n-2}$. Thus, $H^1(G_{1,2}, M) = 0$ and so any element of $\mathrm{Der}(G_{1,2}, M)$ is inner. Since $G_{1,2}$ has a 1-dimensional fixed space on M, it follows that the image of f has dimension $n - 3$ (clearly the map is onto and the space of inner derivations for H acting on M is isomorphic to M/M^H).

Let $K = \ker(f)$. Since $Y = \langle G_{1,2}, G_{2,n} \rangle$, the restriction mapping $f_1 : K \to \mathrm{Der}(G_{2,n}, M)$ is injective. As already noted, $\mathrm{Der}(G_{2,n}, M)$ consists of inner derivations. Thus, the image of f_1 are those inner derivations of $G_{2,n}$ which vanish on $G_{1,2,n}$. Since M is the permutation module for $G_{1,2}$, it follows that $G_{1,2}$ has a 1-dimensional fixed space and $G_{1,2,n}$ has a 2-dimensional fixed space. Thus, the image of f_1 is 1-dimensional. Hence $\dim D = n - 2$. Since Y acts irreducibly and nontrivially on M, the space of inner derivations of Y on M also has dimension $n - 2$. Thus, $\mathrm{Der}(Y, M)$ consists of inner derivations and so $H^1(Y, M) = 0$, as claimed.

Also by the inflation restriction sequence,

$$0 \to H^1(X/R, M) \to H^1(X, M) \to \mathrm{Hom}_X(R, M) \to H^2(X/R, M) \to H^2(X, M).$$

Since $H^2(A_{n-1}, M) = H^1(A_{n-2}, M) = 0$, it follows by Lemma 5.1 that $H^2(X, M) = 0$. Thus, to complete the proof, it suffices to show that $\mathrm{Hom}_X(R, M) = 0$. This follows since the restriction mapping $\mathrm{Hom}_X(R, M) \to \mathrm{Hom}_Y(S, M)$ is injective (as $w \in S$ generates R as a normal subgroup of X). □

Please cite this article in press as: R.M. Guralnick et al., Remarks on proficient groups, J. Algebra (2009), doi:10.1016/j.jalgebra.2009.05.018

It is straightforward to compute $H^2(G,M)$ in the cases omitted in the theorem. In fact, they are all 1-dimensional except that $H^2(A_7,M)=0$ in characteristic 3.

7. Nonproficient groups

There have been many constructions of nonproficient groups, starting with Swan [Sw]. See also [GrK] and [Ko].

Let V be a nontrivial irreducible $\mathbb{F}_pH$-module for a finite perfect group H. Let $W=V^e$ for some positive integer e, so that $X:=W\rtimes H$ is perfect. Let Y be the universal cover of X. Then:

Proposition 7.1. *If $e>\dim V$, then $G:=Y\times Y$ is not proficient.*

Proof. Consider the irreducible $\mathbb{F}_pG$-module $M=V\otimes V$. By the Künneth formula, $\dim H^2(G,M)=e^2>\dim M$ and $H^1(G,M)=0$. Since G is perfect and Y has trivial Schur multiplier, so does G. Thus, $\nu_2(M)>1=\nu_2(\mathbb{F}_r)$ for any prime r and so G is not proficient by (1.7). □

Similarly:

Proposition 7.2. *Any finite group S is a direct summand of a finite nonproficient group.*

Proof. Let G,M and e be as in the previous proposition. We may also assume that e is sufficiently large so that $\nu_2(M)>d(M(S))$ and that p does not divide $|S|$.

Let $X:=S\times G$. We may view M as an $\mathbb{F}_pX$-module. Since p does not divide the order of S, by the Künneth formula $\dim H^i(X,M)=\dim H^i(G,M)$. Thus, the computation of $\nu_2(M)$ is the same for X and G. In particular, $\nu_2(M)>d(M(S))=d(M(X))$. Thus, X is not proficient. □

We now give additional examples of nonproficient groups. We first compute H^2 for certain semidirect products.

Lemma 7.3. *Let p be a prime. Let G be a finite group with a normal elementary abelian p-subgroup L. Assume that G/L has order prime to p. Let r be a prime and U be an irreducible $\mathbb{F}_rG$-module.*

(1) *If $r=p$, then $\dim H^2(G,U)=\dim \mathrm{Hom}_G(L,U)+\dim \mathrm{Hom}_G(\bigwedge^2(L),U)$.*
(2) *If $r\neq p$ and $U^L=0$, then $H^j(G,U)=0$ for all $j\geqslant 0$.*
(3) *If $r\neq p$ and $U^L\neq 0$, then $H^j(G,U)\cong H^j(G/L,U)$ for all $j\geqslant 0$.*

Proof. Note that $G=L\rtimes H$ for some subgroup H, by the Schur–Zassenhaus Theorem.

First assume that $r=p$. Let $w_1,\dots,w_d$ be a basis for L. Let X be the universal nilpotent group of class 2 generated by elements $x_1,\dots,x_d$ satisfying $x_i^{p^2}=1$. Since H has order prime to p, H acts naturally on X so as to make $x_i\to w_i$ induce an H-equivariant map. Note that $\bigwedge^2(L)\cong[X,X]\leqslant Y:=Z(X)$ (as H-modules). If $X_1:=\langle x_1^p,\dots,x_d^p\rangle\leqslant Y$, then $X_1\cong L$ as H-modules. Clearly, $X/X_1[X,X]\cong L$ and so $Y=[X,X]\times X_1$. In particular, $Y\cong\bigwedge^2(L)\oplus L$ as H-modules.

Consider any element of $H^2(L,U)^G$. By the universality of X, this corresponds to an extension $1\to Y/M\to X/M\to L\to 1$ with M an H-invariant subgroup of Y with $Y/M\cong U$ as H-modules. Clearly this lifts to an element of $H^2(G,U)$, giving a map $H^2(L,U)^G\to H^2(G,U)$. Composing with the restriction map gives the identity on $H^2(L,U)^G$. Since p does not divide $|G/L|$, restriction is an injection and so $H^2(L,U)^G\cong H^2(G,U)$.

Since G/L has order prime to p, taking fixed points in (i) of Lemma 7.4 gives $H^2(L,U)^G=\mathrm{Hom}_H(L,U)+\mathrm{Hom}_H(\bigwedge^2(L),U)$, and (1) follows.

Finally, if $r\neq p$, then (2) and (3) are [GKKL2, Corollary 3.12]. □

Let H be a finite group, and let V be an irreducible $\mathbb{F}_pH$-module for some prime p not dividing the order of H. Let $W=V^e$ and set $G=W\rtimes H$. Assume that V is not self-dual and $\dim V=s>1$.

Let U be an irreducible $\mathbb{F}_p H$-module that is a homomorphic image of $\bigwedge^2(V)$. Since V is not self dual, U is nontrivial.

By Lemma 7.3, $\dim H^2(G,U) = \dim \operatorname{Hom}_H(V^e, U) + \dim \operatorname{Hom}_H(\bigwedge^2(V^e), U)$. Also, by Lemma 2.4, $\dim H^1(G,U) = \dim \operatorname{Hom}_H(V^e, U)$.

Thus, $\dim H^2(G,U) - \dim H^1(G,U) = \dim \operatorname{Hom}_H(\bigwedge^2(V^e), U)$. Since U is a homomorphic image of $\bigwedge^2(V)$, its multiplicity as a composition factor in $\bigwedge^2(V^e) = \bigwedge^2(V)^e + (V \otimes V)^{e(e-1)/2}$ is at least $e(e+1)/2$. Thus,

$$\nu_2(U) \geqslant \frac{e(e+1)}{2d} > \left(\frac{e}{s}\right)^2,$$

where $d = \dim U$.

Since $\mathbb{F}_p$ is not an image of either V or $\bigwedge^2(V)$, it follows by Lemma 7.3 that $H^2(G, \mathbb{F}_p) = 0$. Thus p does not divide $M(H)$ or $M(G)$. Also, by Lemma 7.3, if $r \neq p$ then $H^i(G, \mathbb{F}_r) = H^i(H, \mathbb{F}_r)$ for all i. Hence, by Lemma 2.3, $d(M(G)) = d(M(H))$. Since G is not proficient as long as $\nu_2(U) > d(M(H)) + 1$, we see that G is not proficient for e sufficiently large. In particular, if H has a trivial Schur multiplier, then G is not proficient as long as $e(e+1) > 2d$.

Note that G is solvable if and only if H is solvable.

We can be a bit more precise. The argument above shows that

$$\hat{r}(G) - d(G) = \max\bigl\{\hat{r}(H) - d(H), \nu_2(U) - 1\bigr\}.$$

where U ranges over all $\mathbb{F}_p H$ composition factors of $V \otimes V$.

One can also compute $d(G)$ easily. If $s' = \dim_E V$, where E is the field $\operatorname{End}_{\mathbb{F}_p H}(V)$, then [AG, Corollary 2] implies that

$$d(G) = \max\left\{d(H), 2 + \left\lfloor \frac{e-1}{s'} \right\rfloor\right\}.$$

Corrections

Finally, we take this opportunity to correct two minor errors in [GKKL2] pointed out to us by Serre.

The first is [GKKL2, Lemma 3.11] (and as restated in [GKKL2, Lemma 3.12(i)]), which we quoted incorrectly from [Ba]. The correct hypothesis is that $H^i(N, M) = 0$ for $0 < i < r$, which always held whenever the result was applied.

The second is [GKKL2, Lemma 3.16], the correct version of which is

Lemma 7.4. *Let G be a finite group with a normal abelian p-subgroup L. Let $L[p]$ denote the p-torsion subgroup of L. Let V be an irreducible $\mathbb{F}_p G$-module.*

(1) *There is an exact sequence of G-modules,*

$$0 \to \operatorname{Ext}^1_{\mathbb{Z}}(L, V) \to H^2(L, V) \to \bigwedge^2\bigl(L^*\bigr) \otimes V \to 0.$$

(2) $\dim H^2(L,V)^G \leqslant \dim(L[p]^* \otimes V)^G + \dim_F(\bigwedge^2(L/pL)^* \otimes V)^G$.

(3) *If $G = L$, then* $\dim H^2(G, \mathbb{F}_p) = d(d+1)/2$ *where* $d = d(G)$.

The only change is (2), where $L[p]$ replaces L/pL. Again, this has no effect on the proofs in [GKKL2].

Acknowledgments

We thank J.-P. Serre for pointing out the errors just discussed, and A. Hulpke for his assistance with Proposition 4.3. We also thank the referee for his careful reading and useful comments.

References

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

[Ba] A. Babakhanian, Cohomological Methods in Group Theory, Marcel Dekker, New York, 1973.

[Br] K. Brown, Cohomology of Groups, Grad. Texts in Math., vol. 87, Springer-Verlag, New York, 1982.

[CR1] C.M. Campbell, E.F. Robertson, A deficiency zero presentation for $SL(2,p)$, Bull. London Math. Soc. 12 (1980) 17–20.

[CR2] C.M. Campbell, E.F. Robertson, The efficiency of simple groups of order $< 10^5$, Comm. Algebra 10 (1982) 217–225.

[CRKMW] C.M. Campbell, E.F. Robertson, T. Kawamata, I. Miyamoto, P.D. Williams, Deficiency zero presentations for certain perfect groups, Proc. Roy. Soc. Edinburgh Sect. A 103 (1986) 63–71.

[CRW1] C.M. Campbell, E.F. Robertson, P.D. Williams, Efficient presentations for finite simple groups and related groups, in: Groups—Korea 1988, Pusan, 1988, in: Lecture Notes in Math., vol. 1398, Springer-Verlag, Berlin, 1989, pp. 65–72.

[CRW2] C.M. Campbell, E.F. Robertson, P.D. Williams, On presentations of $\mathrm{PSL}(2,p^n)$, J. Aust. Math. Soc. 48 (1990) 333–346.

[CRW3] C.M. Campbell, E.F. Robertson, P.D. Williams, Efficient presentations of the groups $PSL(2,p) \times PSL(2,p)$, p prime, J. London Math. Soc. (2) 41 (1990) 69–77.

[CHRR1] C.M. Campbell, G. Havas, C. Ramsay, E.F. Robertson, Nice efficient presentations for all small simple groups and their covers, LMS J. Comput. Math. 7 (2004) 266–283.

[CHRR2] C.M. Campbell, G. Havas, C. Ramsay, E.F. Robertson, On the efficiency of the simple groups with order less than a million and their covers, Experiment. Math. 16 (2007) 347–358.

[Car] R.D. Carmichael, Introduction to the Theory of Groups of Finite Order, Ginn, Boston, 1937.

[CMRW] C.M. Campbell, I. Miyamoto, E.F. Robertson, P.D. Williams, The efficiency of $PSL(2,p)^3$ and other direct products of groups, Glasg. Math. J. 39 (1997) 259–268.

[El] G. Ellis, Embeddings into k-efficient groups, J. Algebra 243 (2001) 497–503.

[Gru] K. Gruenberg, Relation Modules of Finite Groups, CBMS Reg. Conf. Ser. Math., vol. 25, Amer. Math. Soc., Providence, RI, 1976.

[GrK] K. Gruenberg, L.G. Kovács, Proficient presentations and direct products of finite groups, Bull. Austral. Math. Soc. 60 (1999) 177–189.

[GH] R.M. Guralnick, C. Hoffman, The first cohomology group and generation of simple groups, in: Proceedings of a Conference on Groups and Geometry, Siena, in: Trends Math., Birkäuser Verlag, 1998, pp. 81–90.

[GKKL1] 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.

[GKKL2] R.M. Guralnick, W.M. Kantor, M. Kassabov, A. Lubotzky, Presentations of finite simple groups: A cohomological and profinite approach, Groups Geom. Dyn. 1 (2007) 469–523.

[GKKL3] R.M. Guralnick, W.M. Kantor, M. Kassabov, A. Lubotzky, Presentations of finite simple groups: A computational approach, J. Eur. Math. Soc., forthcoming.

[GuK] R.M. Guralnick, W. Kimmerle, On the cohomology of alternating and symmetric groups and decomposition of relation modules, J. Pure Appl. Algebra 69 (1990) 135–140.

[GuS] R.M. Guralnick, J. Saxl, Generation of finite almost simple groups by conjugates, J. Algebra 268 (2003) 519–571.

[Ha] J. Harlander, Closing the relation gap by direct product stabilization, J. Algebra 182 (1996) 511–521.

[KP] A. Kleshchev, A. Premet, On second degree cohomology of symmetric and alternating groups, Comm. Algebra 21 (1993) 583–600; Comm. Algebra 21 (1993) 583–600 (Corrigendum).

[Ko] L. Kovács, Finite groups with trivial multiplicator and large deficiency, in: Groups—Korea '94, Pusan, de Gruyter, Berlin, 1995, pp. 211–225.

[Lu] A. Lubotzky, Pro-finite presentations, J. Algebra 242 (2001) 672–690.

[Neu] B.H. Neumann, On some finite groups with trivial multiplicator, Publ. Math. Debrecen 4 (1956) 190–194.

[Ro] E.F. Robertson, Efficiency of finite simple groups and their covering groups, in: Finite Groups—Coming of Age, in: Contemp. Math., vol. 45, Amer. Math. Soc., Providence, RI, 1985, pp. 287–294.

[Se] J.-P. Serre, Galois Cohomology, Springer-Verlag, Berlin, 2002.

[Sw] R.G. Swan, Minimal resolutions for finite groups, Topology 4 (1965) 193–208.

[Sun] J.G. Sunday, Presentations of the groups $SL(2,m)$ and $PSL(2,m)$, Canad. J. Math. 24 (1972) 1129–1131.

[T] J. Tits, Les groupes de Lie exceptionnels et leur interprétation géométrique, Bull. Soc. Math. Belg. 8 (1956) 48–81.

[Wi] J.S. Wilson, Finite axiomatization of finite soluble groups, J. Lond. Math. Soc. 74 (2006) 566–582.

Please cite this article in press as: R.M. Guralnick et al., Remarks on proficient groups, J. Algebra (2009), doi:10.1016/j.jalgebra.2009.05.018