Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Universal covers of finite groups

Heiko Dietrich[a], Alexander Hulpke[b]

[a] School of Mathematics, Monash University, VIC 3800, Australia
[b] Department of Mathematics, Colorado State University, Ft. Collins, CO 80523, USA

ARTICLE INFO

Article history:
Received 14 July 2020
Available online xxxx
Communicated by Gerhard Hiss

Keywords:
Computational group theory
Quotient algorithms
Cohomology of groups

ABSTRACT

Motivated by the success of quotient algorithms, such as the well-known p-quotient or solvable quotient algorithms, in computing information about finite groups, we describe how to compute finite extensions $\tilde{H}$ of a finite group H by a direct sum of isomorphic simple $\mathbb{Z}_pH$-modules such that H and $\tilde{H}$ have the same number of generators. Similar to other quotient algorithms, our description will be via a suitable covering group of H. Defining this covering group requires a study of the representation module, as introduced by Gaschütz in 1954. Our investigation involves so-called Fox derivatives (coming from free differential calculus) and, as a by-product, we prove that these can be naturally described via a wreath product construction. An important application of our results is that they can be used to compute, for a given epimorphism $G \to H$ and simple $\mathbb{Z}_pH$-module V, the largest quotient of G that maps onto H with kernel isomorphic to a direct sum of copies of V. For this we also provide a description of how to compute second cohomology groups for the (not necessarily solvable) group H, assuming a confluent rewriting system for H. To represent the corresponding group extensions on a computer, we introduce a new hybrid format that combines this rewriting system with the polycyclic presentation of the module.

© 2020 Elsevier Inc. All rights reserved.

E-mail addresses: heiko.dietrich@monash.edu (H. Dietrich), hulpke@colostate.edu (A. Hulpke).

https://doi.org/10.1016/j.jalgebra.2020.10.032
0021-8693/© 2020 Elsevier Inc. All rights reserved.

Please cite this article in press as:, Universal covers of finite groups, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2020.10.032

1. Introduction

There are three well-established ways to describe a group for a computer: permutations, matrices, and presentations. A detailed account on how to compute with groups is given in the books [15,33,34]. Finite presentations, that is, a finite set of generators together with a finite set of relators, are often a natural and compact way to define groups. For groups given in this form, effective algorithms exist for special kinds of presentations (such as polycyclic presentations) and certain tasks (such as computing abelian invariants). In general, however, due to the undecidability of the word problem for groups (Novikov-Boone Theorem), many problems have been shown to be algorithmically undecidable. What one can do, based on von Dyck's Theorem, is to attempt to investigate such a group via its quotients. This is the idea of so-called *quotient algorithms*, and the main motivation of this paper.

Let G be a finitely presented group and let $\varphi\colon G \to H$ be an epimorphism onto a finite group. By the isomorphism theorem, $G/\ker\varphi \cong H$, so the structure of H has implications for G. For example, if H is non-trivial, then this proves that G is non-trivial – something which is in general undecidable for finitely presented groups. In practice, one attempts to find epimorphisms from G onto groups H that allow practical computations, for example, permutation or polycyclic groups.

The aim of quotient algorithms is to find (largest) quotients of G with certain properties. For example, the largest abelian quotient of G is G/G', where $G' = [G, G]$ is the derived subgroup; the computation of G/G' is straightforward via a Smith-Normal-Form calculation. The well-known p-quotient algorithm of Macdonald [23], Newman & O'Brien [26], and Havas & Newman [10] attempts to construct, for a user-given prime p, the largest quotient of G that is a finite p-group, we refer to [15, Section 9.4] for a detailed discussion and references; see also Remark 2.4 below. Often such a largest quotient does not exist, so the algorithm takes as input a bound on the nilpotency class of the p-quotient that one wants to construct. For a discussion of other quotient algorithms we refer to [15, Section 9.4.3]. For example, using a similar approach as the p-quotient algorithm, the nilpotent quotient algorithm of Nickel [25] tries to compute the largest nilpotent quotient of G. Solvable quotient algorithms, such as described by Plesken [28], Leedham-Green [21], and Niemeyer [27], attempt to construct solvable quotients of G as iterated extensions; generalisations to polycyclic quotients exist, see Lo [20]. For the case of non-solvable groups H, the L^2-quotient algorithm [29], and generalizations in [1], find quotients that are (close to) simple groups in particular classes, but these algorithms do not consider lifts to larger quotients. The concept of lifting epimorphisms by a module, using a presentation for the factor group to produce linear equations that yield 2-cocycles, is suggested already in [28] and used for the case of non-solvable groups in [13]. However, none of these algorithms provides a description of an iterated lifting algorithm for arbitrary non-solvable quotients. Moreover, not all suggested approaches are available in general-purpose implementations (like the p-quotient algorithm is).

Please cite this article in press as:, Universal covers of finite groups, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2020.10.032

We describe a new approach for non-solvable quotients that follows the iteration strategy used in some solvable quotient algorithms. Given an epimorphism $\varphi\colon G \to H$ onto some finite group, we aim to extend it (if possible) to a larger quotient of G via an epimorphism $\alpha\colon G \to K$ that satisfies $\ker\alpha \leqslant \ker\varphi$, that is, α factors through φ. We assume that $\ker\varphi/\ker\alpha$ is a finite semisimple module for H, so by an iteration we can discover *any* quotient of G that is an extension of H with a finite solvable subgroup. This approach assumes that the non-solvable part of the required quotient of G has been supplied as input, which mirrors the view of the *solvable radical paradigm*, see [15, Section 10.3]. This paradigm has been used successfully in modern algorithms for permutation or matrix groups, and relies on the fact that every finite non-solvable group is an extension of a solvable normal subgroup (the *radical*) with a Fitting-free factor group (not affording any non-trivial solvable normal subgroup). We indicate in Section 6.1 how such an initial epimorphism φ can be found.

1.1. Main results

In the following, e is a positive integer and p is a prime. We say a group is e-*generated* if it can be generated by e elements. Our first result is the following.

Theorem 1.1. *Let H be a finite e-generated group. There is a finite e-generated group $\hat{H}_{p,e}$, called the p-cover of H of rank e, such that $\hat{H}_{p,e}$ is an extension of H with an elementary abelian p-group, and any other such e-generated extension of H is a quotient of $\hat{H}_{p,e}$.*

This result is proved in Theorem 3.2 based on a result of Gaschütz. If H is given as a finitely presented group, say $H = F/M$ with F free of rank e, then $\hat{H}_{p,e}$ can be defined as $F/[M,M]M^{[p]}$, where $M^{[p]}$ denotes the subgroup of M generated by all p-th powers. However, the Nielsen-Schreier Theorem shows that the kernel of the projection $\hat{H}_{p,e} \to H$ is an elementary abelian p-group of rank $1 + (e-1)|H|$, which makes an explicit construction of $\hat{H}_{p,e}$ as a finitely presented group, following this definition, infeasible in practice. In Section 3.1 we therefore discuss an alternative description of $\hat{H}_{p,e}$, using Fox derivatives, see Theorem 3.7 for details.

While the definition of $\hat{H}_{p,e}$ is straightforward, it is the new construction in Theorem 3.7 that is our first main result. We do not explain it here, because this would require notation given in Section 3.1.

To make our approach feasible in practice, we consider a further reduction: We say a $\mathbb{Z}_pH$-module A is V-*homogeneous* if A is a direct sum of finitely many copies of a simple $\mathbb{Z}_pH$-module V. In Section 6 we provide some references for the construction of simple $\mathbb{Z}_pH$-modules; all modules we consider here are finite-dimensional.

Theorem 1.2. *Let H be a finite e-generated group with simple $\mathbb{Z}_pH$-module V. There is a finite e-generated group $\hat{H}_{V,e}$, called the (V,e)-cover of H, such that $\hat{H}_{V,e}$ is an extension* *of H with a V-homogeneous module, and any other such e-generated extension of H is a quotient of $\hat{H}_{V,e}$.*

In principle, one can construct $\hat{H}_{V,e}$ from $\hat{H}_{p,e}$, however, doing so would not resolve the issue that $\hat{H}_{p,e}$ is often too big in practice. Instead, we describe a direct construction. For this we show that $\hat{H}_{V,e}$ is a subdirect product of a split and a non-split part, see Theorem 4.5. The former part can be obtained as a modification of our construction for $\hat{H}_{p,e}$; we discuss this in Proposition 5.1. The latter part can be obtained by the cohomological methods described in Section 7; this requires that we have a confluent rewriting system for H. Based on those two parts, in Theorem 5.2 we provide a practically feasible construction of $\hat{H}_{V,e}$. To avoid technical details, the result is formulated here as an existence statement, but the proof will be constructive.

Theorem 1.3. *Let H be a finite, finitely presented, e-generated group and let V be a simple $\mathbb{Z}_pH$-module. If a basis of $H^2(H,V)$ is known, there is an algorithm to construct $\hat{H}_{V,e}$, see Theorem 5.2.*

Assuming a confluent rewriting system for H, we describe a construction algorithm for $H^2(H,V)$ in Section 7; this allows us to apply Theorem 1.3 to construct $\hat{H}_{V,e}$.

Importantly, our results can be used for a non-solvable quotient algorithm. We discuss the details of the following theorem in Section 6.

Theorem 1.4. *Let $\varphi\colon G \to H$ be an epimorphism from a finitely presented group onto a finite, finitely presented, e-generated group. Given a simple $\mathbb{Z}_pH$-module V and a confluent rewriting system for H, there is an algorithm to construct an epimorphism $\alpha\colon G \to K$ where $\ker\alpha \leqslant \ker\varphi$ and K is the largest e-generated quotient of G that maps onto H with V-homogeneous kernel.*

Our last, and practically most relevant, result is a workable implementation of our algorithms for the computer algebra system GAP [4]; we discuss this in Section 8. Our code is available under https://github.com/hulpke/hybrid, and we aim to make it available as part of a standard GAP distribution. What makes our implementation effective is a hybrid computer representation of the non-solvable extensions of H that combines confluent rewriting systems (for the non-solvable factor) and polycyclic presentations (for the solvable normal subgroups); we give details in Section 8.1. We discuss some cost estimates of our algorithm in Section 8.2. Section 8.3 illustrates the scope of the algorithm in some examples. For instance, in Example 8.1 we have been able to compute, in a few minutes, an epimorphism from the infinite Heineken group $\mathcal{H}$ onto $2^4.2^4.(2\times2).2^4.2^4.2.(2\times2^4).A_5$. This quotient had been constructed in a permutation representation of degree 138240 in [35] (with later work of Holt reducing to permutation degree 15360), but our method works generically and avoids large degree permutation representations.

Please cite this article in press as: H. Dietrich, A. Hulpke, Universal covers of finite groups, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2020.10.032

1.2. Comparison with other quotient algorithms

We show in Remark 2.4 that for groups H of p-power order our cover $\hat{H}_{V,e}$ is a generalisation of the p-covering group H^*, and that our algorithm therefore generalises the p-quotient algorithm [26]. For the case of a solvable H, several versions of quotient algorithms have been proposed, for example in [21,27,28].

The method of [21,27] constructs the maximal possible extension with a module in a single step. When starting with an epimorphism $G \to H$ from a free group G, it will in fact construct the maximal cover $\hat{H}_{p,e}$. This approach risks that in the process of forming this module (from relations using vector enumeration) it will encounter a regular module of H (which often is infeasibly large) before reducing it back by further relators. Our approach instead deliberately works with multiple covers, for each of which its kernel is guaranteed to be much smaller than the regular module.

While sharing many ideas with [28], our approach differs in the following ways: first, we construct a universal cover and find the maximal possible lift of a given epimorphism $G \to H$ via a quotient of this cover; in [28], lifts are constructed in steps, each time extending by one copy of the module. Second, our construction of the cover reduces the extensions of H that have to be determined using cohomology to a basis of the corresponding cohomology group, whereas the construction in [28] works with cosets of a subgroup of $H^2(H, M)$.

1.3. Notation

We denote by e a positive integer and by p a prime. We write $\mathbb{Z}_p$ for the integers modulo p. A group G is an extension of Q with N if G has a normal subgroup $M \cong N$ with $G/M \cong Q$; we usually identify $M = N$ and $G/N = Q$. A subgroup $U \leqslant A \times B$ of a direct product is a subdirect product of A and B if U has surjective projections onto both A and B. In this case, [38, Lemma 1.1] shows that for $U_1 = U \cap A$ and $U_2 = U \cap B$ there is an isomorphism $\tau\colon A/U_1 \to B/U_2$, and U is the preimage of $\{(aU_1, \tau(aU_1)) : a \in A\}$ under the natural projection from $A \times B$ to $A/U_1 \times B/U_2$.

Throughout the paper, we use the following notation. We fix a prime p, a finitely presented group G, and an epimorphism $\varphi\colon G \to H$ onto a finite group H. Let F be the free group underlying the presentation of G and denote its rank by e. Since G is a quotient of F by a relation subgroup $R \trianglelefteq F$, the epimorphism φ lifts to a homomorphism $\psi\colon F \to H$. Its kernel $M = \ker\psi$ will map onto the kernel of any extension of H that is a quotient for G. The situation is summarised by the following commutative diagram (whose first row is a short exact sequence).

$$\begin{tikzcd}
1 \arrow[r] & M \arrow[r] & F \arrow[r, "\psi"] \arrow[d] & H \arrow[r] & 1 \\
 & & G \arrow[ru, "\varphi"'] & &
\end{tikzcd}$$

2. Definition of covers and the regular module

In this section we define the covers $\hat{H}_{p,e}$ and $\hat{H}_{V,e}$ of H, and recall some results for the p-modular regular module $\mathbb{Z}_pH$. In later sections we investigate these covers and their construction in detail.

2.1. The p-cover of rank e

We start with a discussion of the so-called p-representation module of H. We write

$$M_p = [M, M]M^{[p]}$$

for the smallest normal subgroup of M whose corresponding quotient group is an elementary abelian p-group; here $M' = [M, M]$ is the derived subgroup of M and $M^{[p]}$ is the subgroup generated by all p-th powers. The quotient M/M_p is an H-module where $g \in H$ acts via conjugation by any preimage under ψ; this action is well-defined since M acts trivially on M/M_p by conjugation. The Nielsen-Schreier Theorem [30, (6.1.1)] shows that M is free of rank $s = 1 + (e - 1)|H|$, hence M/M_p is elementary abelian of rank s. Since M_p is characteristic in M, hence normal in F, one can form F/M_p. We show in Theorem 3.2 that the isomorphism type of F/M_p depends only on H, p and e, but not on ψ. In view of Theorem 1.1 (proved with Theorem 3.2), this justifies the following definition:

Definition 2.1. We call

$$\mathcal{M}_{H,p,e} = M/M_p \quad \text{and} \quad \hat{H}_{p,e} = F/M_p$$

the p-representation module of H and the p-cover of H of rank e, respectively.

The structure of $\mathcal{M}_{H,p,e}$ has been described by Gaschütz [5], see also the book of Gruenberg [9] and papers [2,7]. Note that $\hat{H}_{p,e}$ is an extension of H with $\mathcal{M}_{H,p,e}$; we present an explicit construction of $\hat{H}_{p,e}$ in Section 3.1. However, the rank s of the module $\mathcal{M}_{H,p,e}$ is often too large for practical calculations. To reduce the size of the cover, we therefore restrict to the case of semisimple homogeneous modules, that is, modules which are the direct sum of isomorphic copies of a simple module. Doing so does not limit the scope of our techniques, because any other extension with a module can be considered as an iterated extension with semisimple homogeneous modules.

2.2. The (V, e)-cover

Definition 2.2. Let V be a simple $\mathbb{Z}_pH$-module. For a $\mathbb{Z}_pH$-module A let $V(A)$ be the smallest submodule of A such that $A/V(A)$ is V-homogeneous. The (V, e)-cover of H is

$$\hat{H}_{V,e} = \hat{H}_{p,e}/V(\mathcal{M}_{H,p,e});$$

by construction, it is the largest e-generated group that maps onto H with V-homogeneous kernel.

Recall that the radical $\mathrm{rad}(A)$ of an H-module A is the intersection of all maximal submodules, and $\mathrm{rad}(A) = 0$ if no such submodules exist. The following lemma seems well-known, see e.g. [3, Introduction, §5], but we could not find a reference that includes all statements concisely in one place; therefore we include a short proof in Appendix A for completeness. It follows that $\mathrm{rad}(A) \leqslant V(A)$, and therefore the structure of $A/V(A)$ is determined by the radical factor of A.

Lemma 2.3. *Let A and B be H-modules; let $C \leqslant A$ be a submodule.*

a) *We have $\mathrm{rad}(C) \leqslant \mathrm{rad}(A)$ and $\mathrm{rad}(A \oplus B) = \mathrm{rad}(A) \oplus \mathrm{rad}(B)$.*
b) *If $\sigma\colon A \to B$ is an H-module homomorphism, then $\sigma(\mathrm{rad}(A)) \leqslant \mathrm{rad}(B)$.*
c) *We have $\mathrm{rad}(A/C) = (\mathrm{rad}(A)+C)/C$, and A/C is semisimple if and only if $\mathrm{rad}(A) \leqslant C$.*

A practically feasible construction of $\hat{H}_{V,e}$ is discussed in Section 5.3. Here we conclude with a comment on the p-cover in the p-quotient algorithm.

Remark 2.4. If H is a finite p-group, then it is natural to compare $\hat{H}_{p,e}$ with the p-cover of H as defined in the p-quotient algorithm, see [15, Section 9.4] for proofs and background information. If H has rank e (that is, every minimal generating set of H has size e), then its p-cover H^* is an e-generated extension of H with a central elementary abelian p-group N, and every other such extension of H is a quotient of H^*, see [15, Theorem 9.18]. The group H^* is unique up to isomorphism, and if $H = F/M$ with F a free group of rank e, then $H^* \cong F/[F, M]M^{[p]}$. In particular, H^* is a quotient of $\hat{H}_{p,e}$. Since N is the direct sum of copies of the 1-dimensional trivial $\mathbb{Z}_pH$-module $\mathbf{1}$, it follows that $H^* \cong \hat{H}_{\mathbf{1},\mathrm{rank}(H)}$ is a special case of our p-cover $\hat{H}_{V,e}$

2.3. The structure of the regular module

We recall the following results for the regular module $\mathbb{F}H$ where H is a finite group and $\mathbb{F}$ is a finite field. Following [22, Definition 1.5.8], we call an extension field $\underline{\mathbb{F}} \geqslant \mathbb{F}$ a *splitting field* for an $\mathbb{F}$-algebra A, if every simple $\underline{\mathbb{F}}A$-module is absolutely simple. It is proved in [22, Lemma 1.5.9] that if $\dim_{\mathbb{F}} A < \infty$, then there exists a splitting field $\underline{\mathbb{F}}$ such that the extension $\underline{\mathbb{F}} > \mathbb{F}$ has finite degree. This allows us to state the following lemma and theorem, which are consequences of standard results of modular representation theory; due to their importance for this work, proofs of both results are contained in Appendix A.

Lemma 2.5. *Let $\mathbb{F}$ be a finite field and let $\underline{\mathbb{F}}$ be a finite degree splitting field for $\mathbb{F}H$. For an $\mathbb{F}H$-module V let $\underline{\mathbb{F}}V = \underline{\mathbb{F}} \otimes_{\mathbb{F}} V$ be the $\underline{\mathbb{F}}H$-module arising from V by extending scalars.*

a) *If V is a simple $\mathbb{F}H$-module, then $\underline{\mathbb{F}}V$ is a direct sum of non-isomorphic simple $\underline{\mathbb{F}}H$-modules.*
b) *We have $\underline{\mathbb{F}}\,\mathrm{rad}(\mathbb{F}H) = \mathrm{rad}(\underline{\mathbb{F}}H)$.*

Theorem 2.6. *Let H be a finite group. If $\mathbb{F}$ is a field in finite characteristic, then the regular module can be decomposed as*

$$\mathbb{F}H = D_1^{r_1} \oplus \ldots \oplus D_t^{r_t}, \tag{2.1}$$

where each D_i is a module that is indecomposable and projective (as a direct summand of the free module). The factors $D_i/\operatorname{rad}(D_i)$ are simple, mutually non-isomorphic, and t is the number of isomorphism types of simple $\mathbb{F}H$-modules. The isomorphism type of each D_j is determined uniquely by the isomorphism type of $D_j/\operatorname{rad}(D_j)$, and we have

$$\mathbb{F}H/\operatorname{rad}(\mathbb{F}H) = \bigoplus\nolimits_{i=1}^{t} (D_i/\operatorname{rad}(D_i))^{r_i}.$$

Each multiplicity r_i is the dimension of an absolutely simple constituent of $D_i/\operatorname{rad}(D_i)$; if $\mathbb{F}$ is of sufficiently large degree over the prime field or if $\mathbb{F}$ is algebraically closed, then $r_i = \dim(D_i/\operatorname{rad}(D_i))$.

We are particularly interested in the regular module $\mathbb{Z}_pH$; we fix the following notation for the remainder of this paper.

Definition 2.7. We write $R_{H,p}$ for the p-modular regular H-module, that is, $R_{H,p} \cong \mathbb{Z}_pH \cong \mathbb{Z}_p^m$ as H-modules, where $|H| = m$. Applying (2.1), we decompose

$$R_{H,p} = D_1^{r_1} \oplus \ldots \oplus D_t^{r_t}. \tag{2.2}$$

Writing $E_i = D_i/\operatorname{rad}(D_i)$, the set $\{E_1, \ldots, E_t\}$ forms a complete set of representatives of simple $\mathbb{Z}_pH$-modules; we assume $E_1 = \mathbf{1}$ is the 1-dimensional trivial module. Each $r_i = \dim_{\mathbb{Z}_p} C_i$, where C_i is an absolutely simple constituent of E_i over the algebraic closure of $\mathbb{Z}_p$.

3. Uniqueness of the cover and a construction

Recall that $\psi\colon F \to H$ has kernel M and that $\hat{H}_{p,e} = F/M_p$ is an extension of H with the elementary abelian module $\mathcal{M}_{H,p,e} = M/M_p$. The following lemma, due to Gaschütz [6], shows that ψ factors through any e-generated extension of H with an elementary abelian p-group.

Lemma 3.1. ([6, Satz 1]) *Let $N \trianglelefteq K$ be a finite normal subgroup of an e-generated group K. If K/N is generated by $\{k_1N, \dots, k_eN\}$, then there are $n_1, \dots, n_e \in N$ with $K = \langle k_1n_1, \dots, k_en_e\rangle$.*

The next result proves Theorem 1.1 and shows that the cover $\hat{H}_{p,e}$ is independent of the chosen projection $\psi\colon F \to H$; this theorem is largely a corollary to a result of Gaschütz [5]. Similar universal properties hold for covers of other quotient algorithms, cf. Remark 2.4 for the p-cover.

Theorem 3.2. *The group $\hat{H}_{p,e}$ is an e-generated extension of H with an elementary abelian p-group, and every other such extension of H is a quotient of $\hat{H}_{p,e}$. The isomorphism type of $\hat{H}_{p,e}$ depends only on H, p, and e; the same holds for the H-module structure of $\mathcal{M}_{H,p,e}$.*

Proof. The first claim on $\hat{H}_{p,e}$ follows by construction. Now consider an e-generated group L with epimorphism $\tau\colon L \to H$ and $Y = \ker\tau$ an elementary abelian p-group. By Lemma 3.1, we can lift any generating set of H of size e to a generating set of L; since F is free, we can therefore factor ψ through L, that is, there is a homomorphism $\beta\colon F \to L$ such that $\tau \circ \beta = \psi$. Since $\beta(M) \leqslant \ker\tau$ is elementary abelian of exponent p, we have $\beta(M_p) = \beta(M'M^{[p]}) = 1$. This proves that β induces an epimorphism from $\hat{H}_{p,e}$ to L, as required. To prove uniqueness of $\hat{H}_{p,e}$, consider an e-generated group K with the same properties as stipulated for $\hat{H}_{p,e}$. By assumption, there exist epimorphisms $\hat{H}_{p,e} \to K$ and $K \to \hat{H}_{p,e}$; since both groups are finite, $\hat{H}_{p,e} \cong K$. That the isomorphism type of $\mathcal{M}_{H,p,e}$ as H-module is independent from ψ follows from [5, Satz 1]. □

Later we require the following result about the structure of $\mathcal{M}_{H,p,e}$:

Theorem 3.3. ([5, Satz 2 & 3 & 5 & 6]) *Let H be a finite e-generated group. The $\mathbb{Z}_pH$-modules $\mathcal{M}_{H,p,e}$ and $(R_{H,p})^{e-1} \oplus \mathbf{1}$ have the same multiset of simple composition factors. Furthermore, $\mathcal{M}_{H,p,e} \cong \mathcal{A} \oplus \mathcal{B}$ as H-modules, where $\mathcal{A}$ is a direct summand of $(R_{H,p})^e$, and so a projective module, and if $N \trianglelefteq \hat{H}_{p,e}$ such that $N \leqslant \mathcal{M}_{H,p,e}$ and $\hat{H}_{p,e}/N$ splits over $\mathcal{M}_{H,p,e}/N$, then $\mathcal{B} \leqslant N$.*

Remark 3.4. A detailed description of $\mathcal{A}$ and $\mathcal{B}$ is given in [5]. In the following we use the notation of Definition 2.7. If p divides $|H|$, then $\operatorname{rad}(D_1) \neq 0$ and we define integers $s_1, \dots, s_t$ by

$$\operatorname{rad}(D_1)/\operatorname{rad}(\operatorname{rad}(D_1)) = E_1^{s_1} \oplus \ldots \oplus E_t^{s_t}.$$

Now $S = D_1^{s_1} \oplus \ldots \oplus D_t^{s_t}$ is the projective cover of $\operatorname{rad}(D_1)$, cf. [7, p. 256], and $\mathcal{B}$ is defined as the kernel of the projection $S \to \operatorname{rad}(D_1)$. As shown in [5, Satz 5'] and [7, p. 256–258], this kernel is unique up to isomorphism and does not contain a direct summand isomorphic to any $D_1, \dots, D_t$. If $p \nmid |H|$, then $\mathcal{B} = 0$ and each $s_i = 0$. We have $\mathcal{A} = D_1^{e-s_1} \oplus D_2^{(e-1)r_2-s_2} \oplus \ldots \oplus D_t^{(e-1)r_t-s_t}$.

3.1. A construction of the p-cover

The definition of $\hat{H}_{p,e}$ as F/M_p offers a way of constructing it as a finitely presented group. However, the large rank of the module $\mathcal{M}_{H,p,e}$ makes this infeasible in all but the smallest examples. In this section we explore a different way and describe the cover via so-called Fox derivatives and a wreath product construction.

3.2. Fox derivatives

We first recall some results from [19, Section 11.4]. Let F be free on the set $X = \{x_1, \dots, x_e\}$. Since we will be working in the group ring $\mathbb{Z}F$, we denote the identity in F (and in its quotient groups) by $\mathbf{e}$ to avoid confusion with the unit $1 \in \mathbb{Z}$.

The Fox derivative of $x \in X$ is defined as the unique map

$$\tfrac{\partial}{\partial x} \colon F \to \mathbb{Z}F$$

that maps x to $\mathbf{e}$ and all other generators to zero, and satisfies the *Leibniz' rule*

$$\tfrac{\partial(uv)}{\partial x} = (\tfrac{\partial u}{\partial x})v + \tfrac{\partial v}{\partial x}$$

for all $u, v \in F$. By abuse of notation, we also denote by $\frac{\partial}{\partial x}$ its linear extension to $\mathbb{Z}F$.

Remark 3.5. The Leibniz' rule yields that

$$\tfrac{\partial \mathbf{e}}{\partial x} = 0 \quad \text{and} \quad \tfrac{\partial(s^{-1})}{\partial x} = -\tfrac{\partial s}{\partial x} s^{-1}.$$

The image of $w \in F$ under $\frac{\partial}{\partial x}$ is a sum of terms, one for each occurrence of $x^{\pm 1}$ in w: the term corresponding to $w = axb$ is b, and the term corresponding to $w = ux^{-1}v$ is $-x^{-1}v$. For example, if $w = axbx^{-1}c$ where $a, b, c \in F$ do not contain $x^{\pm 1}$, then $\frac{\partial(w)}{\partial x} = bx^{-1}c - x^{-1}c$.

By abuse of notation, we identify the projection $\psi \colon F \to H$ with the induced homomorphism

$$\psi \colon (\mathbb{Z}F)^e \to (\mathbb{Z}H)^e, \tag{3.1}$$

and combine the Fox derivatives to a map

$$\partial \colon F \to (\mathbb{Z}F)^e, \quad w \mapsto (\tfrac{\partial w}{\partial x_1}, \dots, \tfrac{\partial w}{\partial x_e}).$$

The composition of these maps gives $\psi \circ \partial \colon F \to (\mathbb{Z}H)^e$. The main result on Fox derivatives required in this work is [19, Proposition 5], which states that

$$\ker(\psi \circ \partial) = M'. \tag{3.2}$$

In the next section we will use this fact to describe a group isomorphic to $\hat{H}_{p,e}$.

3.3. A wreath product construction

To remain within the class of groups, we identify the group ring $\mathbb{Z}H$ with a subgroup of the regular wreath product $\mathbb{Z} \wr H$. Suppose we have $|H| = m$, and consider

$$W = \mathbb{Z} \wr H = H \ltimes \mathbb{Z}^m,$$

where the m copies of $\mathbb{Z}$ in $\mathbb{Z}^m$ are labelled by the elements of H. We write $0 = (0, \dots, 0) \in \mathbb{Z}^m$ and, if $h \in H$ and $z \in \mathbb{Z}$, then

$$z(h) \in \mathbb{Z}^m \leqslant W$$

denotes the element of $\mathbb{Z}^m$ with z in position labelled h, and 0s elsewhere. Thus, if $a, b, g, h \in H$, then $(a, 1(g)), (b, 1(h)) \in W$ satisfy

$$(a, 1(g)) \cdot (b, 1(h)) = (ab, 1(gb) + 1(h)) \quad \text{and} \quad (a, 1(\mathbf{e}))^{-1} = (a^{-1}, -1(a^{-1})).$$

For each $i \in \{1, \dots, e\}$ define the homomorphism $\psi_i \colon F \to W$ by

$$\psi_i \colon F \to W, \quad \psi_i(x_j) = \begin{cases} (\psi(x_j), 0) & \text{if } i \neq j \\ (\psi(x_j), 1(\mathbf{e})) & \text{if } i = j. \end{cases}$$

We now prove that ψ_i is closely related to the Fox derivative $\frac{\partial}{\partial x_i}$. For this we identify $\mathbb{Z}H$ with $\mathbb{Z}^m$ via the additive isomorphism $\mathbb{Z}H \to \mathbb{Z}^m$ that maps each $g \in H$ to $1(g) \in \mathbb{Z}^m$; this can be used to let $\psi \colon (\mathbb{Z}F)^e \to (\mathbb{Z}H)^e$ in (3.1) induce a homomorphism

$$\zeta \colon \mathbb{Z}F \to \mathbb{Z}^m.$$

Proposition 3.6. *If $i \in \{1, \dots, e\}$ and $w \in F$, then*

$$\psi_i(w) = (\psi(w), \zeta(\tfrac{\partial w}{\partial x_i})),$$

and $\zeta(\frac{\partial w}{\partial x_i}) = 0$ if and only if $\psi(\frac{\partial w}{\partial x_i}) = 0$.

Proof. For simplicity, write $\tau = \psi_i$ and $x = x_i$. Write $w = w_1 x^{\varepsilon_1} w_2 x^{\varepsilon_2} \dots w_k x^{\varepsilon_k} w_{k+1}$ where each $\varepsilon_j \in \{\pm 1\}$ and each $w_j \in F$ is reduced and does not contain $x^{\pm 1}$. We prove the claim by induction on k. If $k = 0$, then $w = w_1$ and $\tau(w) = (\psi(w), 0) = (\psi(w), \frac{\partial w}{\partial x})$. For $k = 1$ we have $w = w_1 x^{\varepsilon_1} w_2$, which requires a case distinction: if $\varepsilon_1 = 1$, then

$$\tau(w) = (\psi(w_1), 0) \cdot (\psi(x), 1(\mathbf{e})) \cdot (\psi(w_2), 0) = (\psi(w), 1(\psi(w_2))) = (\psi(w), \zeta(\tfrac{\partial w}{\partial x}));$$

if $\varepsilon = -1$, then

$$\begin{aligned}\tau(w) &= (\psi(w_1), 0) \cdot (\psi(x)^{-1}, -1(\psi(x)^{-1})) \cdot (\psi(w_2), 0)\\ &= (\psi(w), -1(\psi(x^{-1}w_2)))\\ &= (\psi(w), \zeta(\tfrac{\partial w}{\partial x})).\end{aligned}$$

Now let $k \geqslant 2$ and write $w = w' x^{\varepsilon_k} w_{k+1}$; by the induction hypothesis, we have

$$\tau(w) = \tau(w')\tau(x^{\varepsilon_k} w_{k+1}) = (\psi(w'), \zeta(\tfrac{\partial w'}{\partial x})) \cdot (\psi(x^{\varepsilon_k} w_{k+1}), \zeta(\tfrac{\partial x^{\varepsilon_k} w_{k+1}}{\partial x})) = (\psi(w), \tfrac{\partial w}{\partial x}),$$

where the last equation follows from the Leibniz' rule. □

Let $W_{(p)} = H \ltimes \mathbb{Z}_p^m$ be the p-modular version of W. We now combine $\psi_1, \ldots, \psi_e$ to

$$\Psi = \psi_1 \times \ldots \times \psi_e \colon F \to W^e,$$

and, induced by the natural projection $\mathbb{Z} \to \mathbb{Z}_p$, define $\Psi_p \colon F \to (W_{(p)})^e$ via

$$\Psi_p \colon F \overset{\Psi}{\to} W^e \overset{\text{proj}}{\to} (W_{(p)})^e. \tag{3.3}$$

The homomorphism Ψ_p can be used to construct the p-cover $\hat{H}_{p,e}$ and the module $\mathcal{M}_{H,p,e}$.

Theorem 3.7. *With the previous notation and Definition 2.1, the following hold.*

a) *We have* $\ker \Psi = M'$ *and* $\ker \Psi_p = M_p$.
b) *The p-cover $\hat{H}_{p,e}$ of H of rank e is isomorphic to $\Psi_p(F)$, and $\mathcal{M}_{H,p,e} \cong \Psi_p(M)$ as H-modules.*

Proof. a) By Proposition 3.6 we have $w \in \ker \Psi$ if and only if $\psi(w) = \mathbf{e}$ and $\zeta(\frac{\partial w}{\partial x_i}) = 0$ for every i, if and only if $w \in M$ and $\psi(\frac{\partial w}{\partial x_i}) = 0$ for every i, if and only if $w \in M$ and $\psi \circ \partial(w) = 0$, if and only if $w \in M'$, see (3.2). It follows from this that $M/M' \cong \Psi(M) \leqslant \mathbb{Z}^{me}$, in particular, Ψ_p induces a map $M/M' \to \mathbb{Z}^{me} \to \mathbb{Z}_p^{me}$ whose kernel is the preimage of $(p\mathbb{Z})^{me}$ under $\Psi|_{M/M'}$, which is $M^{[p]}M'/M'$. In conclusion, $\ker \Psi_p = M_p$, as claimed.

b) It follows from a) and Theorem 3.2 that $\Psi_p(F) \cong F/M_p \cong \hat{H}_{p,e}$. By the isomorphism theorem, Ψ_p yields an isomorphism $\alpha \colon M/M_p \to \Psi_p(M)$, $rM_p \mapsto \Psi_p(r)$. Let $r \in M$, write $g \in H = F/M$ as $g = fM$, and note $(rM_p)^g = r^f M_p$. Since $\Psi_p(M) \leqslant \mathbb{Z}^{me} \leqslant W^e$ is abelian, it follows that the conjugation action of $\Psi_p(f)$ on $\Psi_p(M)$ is conjugation by $\psi(f) = g$. Now $\alpha((rM_p)^g) = \Psi_p(r^f) = \Psi_p(r)^{\Psi_p(f)} = \Psi_p(r)^g = \alpha(rM_p)^g$ shows that α is an H-module isomorphism. □

The construction in Theorem 3.7 uses a wreath product with $|H| = m$ factors $\mathbb{Z}_p$; this makes it practical only for reasonably small groups H.

4. Extensions with homogeneous modules

Let V be a simple $\mathbb{Z}_p H$-module. In this section we study the structure of extensions E of H with a V-homogeneous module $K \trianglelefteqslant E$. We will apply this later to the construction of the cover $\hat{H}_{V,e}$, but the analysis applies to any such extension E.

Since K is V-homogeneous, any simple quotient module of K will be isomorphic to V, the intersection of the maximal H-submodules of K is trivial, and submodules of K correspond to normal subgroups of E contained in K. This implies that E is a subdirect product of extensions of H with V. We (naturally) assume that in each of these extensions the projection onto H is induced by the projection $E \to H$, which allows us to simply identify these factors in the subdirect product.

To fix notation, we recall the basic setup of extension theory [30, Section 11].

Definition 4.1. Every extension of H with V is isomorphic to a group E_γ with underlying element set $H \times V$ and multiplication

$$(g, v) \cdot (h, w) = \big(gh, v^h w \gamma(g, h)\big) \tag{4.1}$$

for a 2-cocycle $\gamma \in Z^2(H, V)$. Note that we write V multiplicatively, but we consider $Z^2(H, V)$ and $H^2(H, V)$ as additive groups. We call E_γ the extension corresponding to γ and call the map

$$\varepsilon_\gamma \colon E_\gamma \to H, \quad (h, v) \mapsto h,$$

its natural epimorphism. Non-split extensions correspond to cocycles in $Z^2(H, V)$ that lie outside the subgroup of 2-coboundaries $B^2(H, V)$.

We first study the interplay between extensions and subdirect products.

Lemma 4.2. *Let $E_1, \ldots, E_n$ be extensions of H with H-modules $V_1, \ldots, V_n$, respectively, and let E be the subdirect product of the E_i, defined by identifying the factor groups isomorphic to H; let $K \trianglelefteq E$ be the kernel of the projection $E \to H$.*

a) *If each E_i is split over V_i, then E is split over K.*

Please cite this article in press as: H. Dietrich, A. Hulpke, Universal covers of finite groups, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2020.10.032

b) *There exists a unique normal subgroup $L \trianglelefteq E$ that is minimal with respect to E/L being split over K/L. In particular, E is a subdirect product of non-split extensions of H with the split extension E/L of H. Every quotient of E that is a split extension of H is a quotient of E/L.*

Proof. a) It is sufficient to prove this for $n = 2$. We can assume that the underlying set of E is $H \times V_1 \times V_2$ and $K = \{(1, v_1, v_2) \mid v_i \in V_i\}$. If $\{(h, 1) : h \in H\}$ is a complement to V in each E_i, then $\{(h, 1, 1) \mid h \in H\}$ is a complement to K in E.

b) Let $\mathcal{N}$ be the collection of all $N \trianglelefteq E$ with $N \leqslant K$ such that E/N is split over K/N. Note that the homomorphism $E \to \prod_{N\in\mathcal{N}} E/N$, $e \mapsto \prod_{N\in\mathcal{N}} eN$ has kernel $L = \bigcap_{N\in\mathcal{N}} N$ and its image is a subdirect product of all E/N, defined by identifying the factor groups isomorphic to H. Since each such E/N splits, part a) shows that E/L is split over K/L. It follows that E is the subdirect product of E/L with those E_i that are non-split. If Q is a quotient of E that is a split extension of H, then $Q \cong E/M$ for some $M \in \mathcal{N}$; this implies the last claim. □

Definition 4.3. The subgroup L in Lemma 4.2b) is called the *split kernel* of the extension E.

We now show that subdirect products of extensions behave well under cocycle arithmetic.

Lemma 4.4. *Let V be a simple $\mathbb{Z}_p H$-module and $\beta, \gamma \in Z^2(H, V)$.*

a) *Let E be the subdirect product of E_β and E_γ defined by identifying $\varepsilon_\beta(E_\beta) = \varepsilon_\gamma(E_\gamma)$. Let $\zeta = \beta + \gamma$. There exists $N \trianglelefteq E$ such that $E/N \cong E_\zeta$ and $N \cap \ker \varepsilon_\beta = 1$. In particular, E is isomorphic to the subdirect product of E_β and E_ζ, defined by identifying $\varepsilon_\beta(E_\beta) = \varepsilon_\zeta(E_\zeta)$.*

b) *The statement of a) holds for $\zeta = r\beta + \gamma$ with arbitrary $r \in \mathbb{Z}_p$.*

c) *Let D be a group with epimorphism $\pi : D \to E_\beta$. Let E be the subdirect product of D with E_γ defined by identifying $\varepsilon_\beta(\pi(D)) = \varepsilon_\gamma(E_\gamma)$. For every $\zeta = r\beta + \gamma$ with $r \in \mathbb{Z}_p$, the group E is isomorphic to the subdirect product of D with E_ζ, defined by identifying $\varepsilon_\beta(\pi(D)) = \varepsilon_\zeta(E_\zeta)$.*

Proof. a) Up to isomorphism, we can identify E with the Cartesian product $H \times V \times V$ with multiplication

$$(a, v, w) \cdot (b, x, y) = \big(ab,\ v^b x\beta(a, b),\ w^b y\gamma(a, b)\big)$$

and natural projections $\tau : E \to E_\beta$, $(a, v, w) \mapsto (a, v)$, and $\sigma : E \to E_\gamma$, $(a, v, w) \mapsto (a, w)$. Let

$$K = (\ker \tau)(\ker \sigma) = 1 \times V \times V \quad \text{and} \quad N = \big\{(1, v, v^{-1}) : v \in V\big\} \leqslant K;$$

Please cite this article in press as: H. Dietrich, A. Hulpke, Universal covers of finite groups, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2020.10.032

note that $K, N \trianglelefteq E$; the latter holds, since the $(a,1,1)$-conjugate of $(1,v,v^{-1})$ is $(1,v^a,(v^a)^{-1})$. Furthermore $K/N \cong V$ as H-modules. Now consider the natural homomorphism $\nu\colon E \to E/N$; note that every element in E/N has the form $(a,v,1)N$, and ν maps (a,v,w) to $(a,vw,1)N$. In particular, the multiplication in E/N is

$$(a,v,1)N \cdot (b,w,1)N = (ab, v^b w\beta(a,b), \gamma(a,b))N = (ab, v^b w\beta(a,b)\gamma(a,b), 1)N,$$

which proves that $(a,v,1)N \to (a,v)$ defines an isomorphism $E/N \cong E_\zeta$ where $\zeta = \beta+\gamma$. By abuse of notation, we consider the epimorphism $\nu\colon E \to E_\zeta$, $(a,v,w) \mapsto (a,vw)$. Since the homomorphism $\tau \times \nu\colon E \to E_\beta \times E_\zeta$ is injective, the claim follows.

b) This follows by an iterative application of a).

c) Write $A = \ker \pi$ and let $A \leqslant B \leqslant D$ such that $D/A \cong E_\beta$ and B/A is the kernel of $\varepsilon_\beta\colon E_\beta \to H$, so $D/B \cong H$. As done in a), we identify E with the Cartesian product $H \times B \times V$ and note that

$$\tilde{D} = \{(h,b,1) : h \in H, b \in B\} \cong D \quad \text{and}$$
$$\tilde{E}_\gamma = \{(h,1,v) : h \in H, v \in V\} \cong E_\gamma,$$

with corresponding natural projections $\pi_{\tilde{D}}\colon E \to \tilde{D}$, $(h,b,v) \mapsto (h,b,1)$, and $\pi_{\tilde{E}_\gamma}\colon E \to \tilde{E}_\gamma$, $(h,b,v) \mapsto (h,1,v)$. Note that $L = \{(1,a,1) : a \in A\}$ is normal in $\tilde{D}$, and $\tilde{D}/L \cong E_\beta$. In particular, $L \trianglelefteq E$, and E/L is isomorphic to the subdirect product of E_β and E_γ defined by identifying the common quotient H. By b), there exists $N/L \trianglelefteq E/L$ such that $(E/L)/(N/L) \cong E/N \cong E_\zeta$ and such that E/L is isomorphic to the subdirect product of E_ζ and E_β defined by identifying the common quotient H. Let $\pi_N\colon E \to E/N$ be the natural projection. It also follows from b) that $\ker \pi_N = N$ and $\ker \pi_{\tilde{D}} = \{(1,1,v) : v \in V\}$ intersect trivially, so $\pi_N \times \pi_{\tilde{D}}\colon E \to E/N \times \tilde{D}$ is injective. Since $E/N \cong E_\zeta$ and $\tilde{D} \cong D$, the claim follows. □

We can now formulate the main result of this section.

Theorem 4.5. *Let V be a simple $\mathbb{Z}_p H$-module and let E be an extension of H with a V-homogeneous module K. Let $L \trianglelefteq E$ be the split kernel of E (Definition 4.3). Then $S = E/L$ is a split extension of H with a V-homogeneous module, and there exist an $n \in \mathbb{N}$ and $\gamma_1, \ldots, \gamma_n \in Z^2(H,V)$ such that the cohomology classes in $H^2(H,V)$ induced by the γ_i are all linearly independent and such that E is the subdirect product of S with $E_{\gamma_1}, \ldots, E_{\gamma_n}$ (defined by identifying the common factor H).*

Proof. The statements about S follow from Lemma 4.2. The kernel of the projection $S \to H$ is K/L; the latter is V-homogeneous since it is a quotient of the V-homogeneous module K. The extension E can be considered as a subdirect product of extensions E_β, corresponding to cocycles $\beta \in Z^2(H,V)$; let $\{\gamma_1, \ldots, \gamma_n\}$ be a minimal sub-multiset of

$Z^2(H,V)$ such that E is a subdirect product of S with all those E_{γ_i}. We need to show that all the cohomology classes $\gamma_i + B^2(H,V)$ are linearly independent (which also shows that $\{\gamma_1,\ldots,\gamma_n\}$ is in fact a *set* of size n). Assume the contrary, that is, without loss of generality we can write

$$\gamma_1 = \sigma + \lambda_2\gamma_2 + \ldots + \lambda_n\gamma_n$$

for some $\lambda_i \in \mathbb{Z}_p$ and $\sigma \in B^2(H,V)$. An iterated application of Lemma 4.4 (where D is the subdirect product of S with $E_{\gamma_2},\ldots,E_{\gamma_n}$ and $\gamma = \gamma_1$) shows that we can write E as the subdirect product of S with E_σ and the $E_{\gamma_2},\ldots,E_{\gamma_n}$. Note that E_σ is split, and Lemma 4.2c) shows that the projection $E \to E_\sigma$ factors through S. We can therefore ignore E_σ in the construction and consider E as the subdirect product of S with $E_{\gamma_2},\ldots,E_{\gamma_n}$, contradicting the minimality of n □

Remark 4.6. In the proof of Theorem 4.5, we could add redundant subdirect factors (stemming from linear combinations of the γ_i) and, because we can choose which factor to eliminate, we can choose the cocycles $\gamma_1,\ldots,\gamma_n$ to correspond to an arbitrary basis of their span in $H^2(H,V)$.

5. Construction of the (V,e)-cover

Let V be a simple $\mathbb{Z}_pH$-module. The results of the previous section show that the cover $\hat{H}_{V,e}$ is a subdirect product of a split part with non-split extensions. Recall that $\hat{H}_{V,e} = \hat{H}_{p,e}/V(\mathcal{M}_{H,p,e})$ by Definition 2.2, and Theorem 3.7 describes $\hat{H}_{p,e}$ using a wreath product construction with $|H|$ factors $\mathbb{Z}_p$. We explain in Proposition 5.1 that the split part of $\hat{H}_{V,e}$ is covered by the image of a homomorphism $\Psi_{V,e}$ on the free group F. However, the definition of $\Psi_{V,e}$ passes through $\mathcal{M}_{H,p,e}$, which again is infeasible in practice. In Section 5.2 we therefore provide an alternative construction that only uses H and V; this construction is based on the fact that the split part of $\hat{H}_{V,e}$ is covered by $H \ltimes (R_{H,p}/V(R_{H,p}))^e$, and $R_{H,p}/V(R_{H,p}) \cong V^r$ is a cyclic H-module.

5.1. *A wreath product construction for the split case*

We reconsider the epimorphism

$$\Psi_p = \mu_1 \times \cdots \times \mu_e \colon F \to (H \ltimes R_{H,p})^e,$$

of (3.3) where $R_{H,p} \cong \mathbb{Z}_pH \cong \mathbb{Z}_p^m$ is the regular module of H in characteristic p. The proof of Theorem 3.7 has shown that

$$\hat{H}_{p,e} = \Psi_p(F) \quad \text{and} \quad \mathcal{M} = \mathcal{M}_{H,p,e} = \Psi_p(M).$$

Each $\mu_j\colon F \to H \ltimes R_{H,p}$ maps the generator $x_k \in X$ of F to $(\psi(x_k), 0)$ if $k \neq j$, and to $(\psi(x_j); 1)$ if $k = j$; here $1 = 1(\mathbf{e})$ is the unit vector supported at the identity of H. This vector also is a generator of the cyclic H-module $R_{H,p}$.

By Definition 2.7, we have $R_{H,p} = D_1^{r_t} \oplus \ldots \oplus D_t^{r_t}$ with each $D_j/\operatorname{rad}(D_j)$ simple, and there is a unique index i such that

$$D_i/\operatorname{rad}(D_i) \cong V;$$

we fix i and set $r = r_i$. Let $V(R_{H,p})$ be as in Definition 2.2; then $R_{H,p}/V(R_{H,p}) \cong V^r$ is the largest V-homogeneous quotient of $R_{H,p}$ and r is the dimension of an absolutely simple summand of V over the algebraic closure of $\mathbb{Z}_p$. Factoring out $V(R_{H,p})$, we get homomorphisms $\mu_{V,j}\colon F \to H \ltimes V^r$ mapping x_k to $(\psi(x_k), 0)$ if $k \neq j$, and to $(\psi(x_j); 1 + V(R_{H,p}))$ if $k = j$; here $1 + V(R_{H,p})$ is a generator of the cyclic module

$$V^r = R_{H,p}/V(R_{H,p}). \tag{5.1}$$

These maps can be combined to

$$\Psi_{V,e} = \mu_{V,1} \times \ldots \times \mu_{V,e}\colon F \to (H \ltimes V^r)^e.$$

By definition $\ker \Psi_p \leqslant \ker \Psi_{V,e}$, which implicitly defines an epimorphism from $\hat{H}_{p,e}$ to $\Psi_{V,e}(F)$. This epimorphism factors through $\hat{H}_{V,e}$, since $\Psi_{V,e}(F)$ is by construction an extension of H with a V-homogeneous module. Recall from Definition 2.2 that $\hat{H}_{V,e} = \hat{H}_{p,e}/V(\mathcal{M})$. If η denotes the natural projection $\hat{H}_{p,e} \to \hat{H}_{V,e}$, then we get the following commutative diagram of successive projections

$$\begin{tikzcd} F \arrow[r, "\Psi_p"] \arrow[rrr, bend right, "\Psi_{V,e}"'] & \hat{H}_{p,e} \arrow[r, "\eta"] & \hat{H}_{V,e} \arrow[r, "\theta"] & \Psi_{V,e}(F) \arrow[r, "\pi"] & H. \end{tikzcd}$$

We now prove that $\Psi_{V,e}(F)$ exhibits the split part of $\hat{H}_{V,e}$.

Proposition 5.1. *Every e-generated split extension of H with a V-homogeneous module is a quotient of $\Psi_{V,e}(F)$.*

Proof. We use the notation introduced above the proposition. By Theorem 3.3, the representation module $\mathcal{M} \leqslant \hat{H}_{p,e}$ is a direct sum $\mathcal{M} = \mathcal{A} \oplus \mathcal{B}$ such that the e-generated quotients of $\hat{H}_{p,e}$ which are split extensions of H are exactly the quotients that have $\mathcal{B}$ in the kernel. Thus, it remains to show that $\hat{H}_{p,e}/V(\mathcal{A})\mathcal{B}$ is a quotient of $\Psi_{V,e}(F)$. Recall from Remark 3.4 that $\mathcal{A}$ is the direct sum of projective indecomposable modules that are direct summands of the free module $R_{H,p}$; this implies that $\mathcal{A}$ is projective itself, cf. [22, Definition 1.6.15]. By [22, p. 18, Example 1.1.46] the group algebra $\mathbb{Z}_pH \cong R_{H,p}$ is a symmetric algebra and for such algebras every projective module is also injective, see [22,

Please cite this article in press as: H. Dietrich, A. Hulpke, Universal covers of finite groups, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2020.10.032

Theorem 1.6.27(d)]. It follows from $\mathcal{M} = \Psi_p(M) \leqslant (R_{H,p})^e$ that $\mathcal{A}$ is a submodule of $(R_{H,p})^e$, and therefore a direct summand by injectivity. This implies that

$$V(\mathcal{A}) = V((R_{H,p})^e) \cap \mathcal{A}.$$

This means that the image of the projection

$$(H \ltimes R_{H,p})^e \to (H \ltimes R_{H,p}/V(R_{H,p}))^e = \Psi_{V,e}(F)$$

exposes all the factors of $\mathcal{A}/V(\mathcal{A})$, which implies that $\hat{H}_{p,e}/V(\mathcal{A})\mathcal{B}$ is a quotient of $\Psi_{V,e}(F)$. □

5.2. A practical construction of $\Psi_{V,e}(F)$

The definition of $\Psi_{V,e}$ is on the free group F and passes through $\mathcal{M}$, which we deemed infeasible in practice. We now provide an alternative, synthetic, description that only uses H and V. We denote the dimension of V by s and the multiplicity of V in the radical factor $R_{H,p}/\operatorname{rad}(R_{H,p}) = (D_1/\operatorname{rad}(D_1))^{r_1} \oplus \ldots \oplus (D_t/\operatorname{rad}(D_t))^{r_t}$ of $R_{H,p}$ by r. By Theorem 2.6, this multiplicity is the dimension of an absolutely simple constituent U of V, and r divides s.

As seen in (5.1), the H-module V^r is isomorphic to a quotient of the cyclic module $R_{H,p}$, so V^r is cyclic as well. Suppose we have a cyclic generator $z \in V^r$, then one can define $H \ltimes V^r$ and homomorphisms

$$\psi'_j \colon F \to H \ltimes V^r$$

that map the generator $x_j \in X$ of F to $(\psi(x_j), z)$ and $x_k \neq x_j$ to $(\psi(x_k), 0)$. It follows that, up to automorphisms,

$$\Psi_{V,e} = \psi'_1 \times \ldots \times \psi'_e \colon F \to (H \ltimes V^r)^e. \tag{5.2}$$

Thus, all that remains is to find a cyclic generator of V^r; we now describe how to do that.

Recall that here we have the field $\mathbb{F} = \mathbb{Z}_p$. As in Theorem 2.6, let $\underline{\mathbb{F}}$ be a splitting field for $\mathbb{F}H$ and let U be an absolutely simple $\underline{\mathbb{F}}H$-module that is a direct summand of $\underline{\mathbb{F}}V$. We obtain U from V using MeatAxe [12] methods; this also determines the value of r.

Let $\nu \colon \underline{\mathbb{F}}V \to U$ be the natural projection onto that summand. We choose vectors $w_1, \ldots, w_r \in V$ such that their images $\nu(w_1), \ldots, \nu(w_r)$ form an $\underline{\mathbb{F}}$-basis of U. Since the images of the standard $\mathbb{F}$-basis of V span U as an $\underline{\mathbb{F}}$-vector space, we can take $\{w_1, \ldots, w_r\}$ as a subset of such a standard basis. Since U is absolutely simple, it follows from [22, Corollary 1.3.7] that $\underline{\mathbb{F}}H$ acts as a full matrix algebra on U. This means that we can find elements $a_i \in \underline{\mathbb{F}}H$ such that $\nu(w_i)^{a_j} = \delta_{i,j}\nu(w_i)$ for all i, j, where $\delta_{i,j}$ is the

Kronecker-delta. We now consider U^r as a quotient of $(\underline{\mathbb{F}}V)^r$ and let $\underline{\mathbb{F}}H$ act diagonally. For $w \in U$, denote by $[w]_i$ the vector w in the i-th component of U^r, and define

$$z = [\nu(w_1)]_1 + [\nu(w_2)]_2 + \cdots + [\nu(w_r)]_r \in U^r.$$

By construction, each $z^{a_i} = [\nu(w_i)]_i$. Since U is simple, each $\nu(w_i)$ generates U as $\underline{\mathbb{F}}H$-module; this shows that z generates U^r as $\underline{\mathbb{F}}H$-module. Since V is a simple $\mathbb{F}H$-module, this implies that the pre-image $[w_1]_1 + \cdots + [w_r]_r \in V^r$ of z generates V^r as $\mathbb{F}H$-module. We have therefore found a cyclic generator.

5.3. A practical construction of $\hat{H}_{V,e}$

We combine the results of Theorem 4.5 with the construction in Section 5.2 and get the following construction of the epimorphism $\eta \circ \Psi_p \colon F \to \hat{H}_{V,e}$.

Theorem 5.2. *Let V be a simple $\mathbb{Z}_p H$-module. Let F be the free group on $\{x_1, \ldots, x_e\}$ with associated epimorphism $\psi \colon F \to H$. Let $\gamma_1, \ldots, \gamma_d \in Z^2(H, V)$ such that their images in $H^2(H, V)$ form a basis. For each i, let $E_i = E_{\gamma_i}$ with projections $\varepsilon_i \colon E_i \to H$, and let $\varrho_i \colon F \to E_i$ be defined by $\varrho_i(x_k) = (x_k, 1) \in E_i$ for all k, that is, $\varepsilon_i(\varrho_i(x_k)) = \psi(x_k)$. If we define*

$$\rho = \Psi_{V,e} \times \varrho_1 \times \cdots \times \varrho_d \colon F \to (H \ltimes V^r)^e \times E_1 \times \cdots \times E_d$$

with $\Psi_{V,e}$ as in (5.2), then $\ker \rho = \ker(\eta \circ \Psi_p)$ and $\rho(F) \cong \hat{H}_{V,e}$.

Proof. Since F is free, each ϱ_i is a homomorphism whose image covers all of $E_i/V \cong H$. Since each E_i is non-split and V is simple, each ϱ_i is surjective. The image of ρ therefore is an extension of H with a V-homogeneous module, and therefore it is a quotient of $\hat{H}_{V,e}$. On the other hand, Theorem 4.5 and Remark 4.6 show that $\hat{H}_{V,e}$ is a subdirect product of a split extension (which is $\Psi_{V,e}(F)$ by Proposition 5.1), with extensions corresponding to a basis of a subspace of $H^2(H, V)$. A basis of all $H^2(H, V)$ will suffice, which shows that ρ exposes all of $\hat{H}_{V,e}$. □

The last ingredient that is required in order to construct $\hat{H}_{V,e}$ in practice is to be able to calculate $H^2(H, V)$ and to construct the extension associated to a particular cocycle. A method for this has been given in [11]. Here we use an alternative approach, utilizing confluent rewriting systems; we will describe this method and its advantages in Section 7.

6. Quotient algorithm: lifting epimorphisms

As an application of the results established so far, we describe a quotient algorithm that does not require the initial factor group to be solvable. We assume that $G = F/R$ is a finitely presented group and that an epimorphism $\varphi \colon G \to H$ onto a finite group is given. (Section 6.1 below gives a sketch how such a homomorphism φ could be found.) We assume that we can determine a confluent rewriting system for H, as well as a faithful representation in characteristic p, or a permutation representation. This is a reasonable assumption, because if we cannot compute with H, then it seems unlikely that φ can be used to deduce information about G.

Our goal is to extend φ to an epimorphism $\tau\colon G \to \tilde{H}$ such that $\tilde{H}$ is an extension of H with a semisimple $\mathbb{Z}_pH$-module and such that τ factors through φ. As discussed in the introduction, imposing the requirement of semisimplicity is not a restriction, because any such extension with a solvable normal subgroup can be built as an iterated extension with semisimple modules.

We first classify the irreducible $\mathbb{Z}_pH$-modules. Following [15, Section 7.5.5], we do so by starting with the composition factors of a faithful $\mathbb{Z}_p$-representation of H and then iteratively computing composition factors of tensor products until no new factors arise; see also [28] for a description for solvable H.

When lifting epimorphisms for a second time, we do not need to recompute modules, as long as we work with the same prime, as any normal subgroup of p-power order lies in the kernel of any irreducible representation in characteristic p. (The latter follows because the set of fixed points of the normal p-subgroup is a non-trivial submodule.) Since semisimple modules are the direct sum of homogeneous modules, we now iterate over the simple modules, and for each such module V, we construct the group $\tilde{H}_V$ that is the largest extension of H that is a quotient of G and whose projection onto H has a V-homogeneous kernel. As a quotient of G, this group $\tilde{H}_V$ will also be a quotient of F and therefore a quotient of $\hat{H}_{V,e}$. Indeed, because G is defined as a quotient of F by a relator set R, we obtain $\tilde{H}_V$ (and the associated epimorphism) as a factor of $\hat{H}_{V,e}$ by the normal closure of the relators R evaluated in the generators of $\hat{H}_{V,e}$. The cover $\tilde{H}$ (and the epimorphism on H) then will be the subdirect product of all these extensions.

6.1. *Finding the initial homomorphism*

While it is not the main subject of this paper, we briefly sketch how one can find candidates for the initial epimorphism $\varphi\colon G \to H$. Since our algorithm constructs extensions with solvable groups, it is sufficient for H to be Fitting-free. Thus H embeds in the automorphism group of its socle, and therefore is a subdirect product of groups Q satisfying $T^n \leqslant Q \leqslant \mathrm{Aut}(T^n) \cong \mathrm{Aut}(T) \wr \mathrm{Sym}_n$ for some finite simple group T and integer $n > 0$. Given a choice of n and T (respectively, using the classification of finite simple groups, a choice of n and $|T|$) we can find all such quotients, albeit at a cost that is exponential in n and $|T|$. This will provide a choice of candidates for epimorphisms $\varphi\colon G \to H$ to seed our algorithm with:

Using the low-index algorithm [34, §5.6], we first search for subgroups of G of index up to n. For each such subgroup S, we search for homomorphisms $\tau\colon S \to \mathrm{Aut}(T)$ such that $T \leqslant \tau(S)$; the representation of G induced by τ then exposes the desired quotient Q, see [16]. By the proof of Schreier's Conjecture, $\mathrm{Aut}(T)/T$ is solvable of derived length at most 3. Thus the third (or less, depending on T) derived subgroup of S maps onto T. It therefore remains to find such epimorphisms τ from (derived subgroups of) S onto T, respectively onto almost simple groups with socle T. A basic way of doing this is a generic epimorphism search such as described in [15, Section 9.1.1]. For T being a classical group with particular parameters, there are algorithms that find epimorphisms, utilizing the underlying geometry, see [1,17,18,29].

7. Computing cohomology via rewriting systems

To make the construction of $\hat{H}_{V,e}$ in Theorem 5.2 concrete and effective, we need to be able to calculate 2-cohomology groups and extensions for the given finite quotient H. A general method for this task has been described in [11], which finds a cohomology group as a subgroup of the cohomology for a Sylow p-subgroup of H (here p is the characteristic of V), and returns non-split extensions through presentations. We introduce a different approach that assumes a confluent rewriting system for the group H, but also returns a confluent rewriting system for the resulting extensions, making it easier to find the structure of subgroups given by generators. The method we shall employ is a natural generalisation of the method used in the polycyclic case [15, Section 8.7.2], and already arises implicitly in [28], in [13], in Groves [8], as well as in [31]. A brief description is also given in an (unpublished) manuscript of Stein [36]. We describe this method in detail here, as we were not able to find a complete and rigorous treatment in the literature.

In this section, as before, let H be a finite group with e generators[1] $\{h_1, \dots, h_e\}$. We shall also assume that we have rules for a confluent rewriting system for H in these generators; see [15, Chapter 12] and [34, Section 2.5] for details on rewriting systems. Such a rewriting system can be composed from rewriting systems for the simple composition factors of H; for non-abelian simple groups it can be found by using subgroups forming a BN-pair (or similar structures) [32]. Such a rewriting system allows us to compute normal forms of elements in H, given as words in the generators. In the following, V is a d-dimensional $\mathbb{Z}_p H$-module with $\mathbb{Z}_p$-basis $\{v_1, \dots, v_d\}$.

7.1. *Extending the rewriting system*

Starting with a confluent rewriting system for H and the $\mathbb{Z}_p H$-module V, we explain how extensions of H with V can be described by *extending* the original rewriting systems. This will lead to a method for computing $H^2(H, V)$ via solving homogeneous linear equation systems. We first consider the quotient H, then the module V, and then the extensions.

[1] We use the same variable e here, although it is not necessary to use the same generating set as in the quotient algorithm. The choice (and number) of generators used for the cohomology calculation does not need to agree with the images of free generators used for the construction of $\hat{H}_{V,e}$; it is sufficient that we can translate between different generating systems.

Please cite this article in press as: H. Dietrich, A. Hulpke, Universal covers of finite groups, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2020.10.032

The group H. By introducing formal inverses, H can be considered as a monoid with $2e$ monoid generators $\{h_1^{\pm 1}, \dots, h_e^{\pm 1}\}$. The latter is a quotient of the free monoid A on $\underline{\mathbf{a}} = \{a_1^{\pm 1}, \dots, a_e^{\pm 1}\}$, with natural epimorphism $\alpha\colon A \to H$ defined by $a_i^{\pm 1} \mapsto h_i^{\pm 1}$. Note that a_i^{-1} is a formal symbol, while h_i^{-1} is the inverse of h_i. Using a Knuth-Bendix procedure [34, Section 2.5], we assume that we have a confluent rewriting system (with respect to a reduction order $\prec_a$) for the monoid H on this generating set. This rewriting system consists of a set of rules $\mathcal{R}_H$ each of the form $l \to r$ for certain words l and r in the generators of A, such that $r \prec_a l$. Since we introduced extra generators to represent inverses, we assume that $\mathcal{R}_H$ contains rules that reflect this mutual inverse relation and that become trivial (or redundant) when considering the relations as group relations: these are the rules of the form $a_i a_i^{-1} \to \emptyset$ and $a_i^{-1} a_i \to \emptyset$, which we collect in a subset $\overline{\mathcal{R}}_H \subset \mathcal{R}_H$; here $\emptyset$ denotes the empty word. We note that this assumption holds automatically if $\prec_a$ is based on length and all generators have order 2. If the order of a generator h_i is 2, then these rules will change shape: Without loss of generality, after possibly switching a_i and a_i^{-1}, the inversion rule becomes $a_i^{-1} \to a_i$, which we collect in $\overline{\mathcal{R}}_H$. The rule $a_i^2 \to \emptyset$ (which must exist, since otherwise a_i^2 cannot be reduced) however will not be part of $\overline{\mathcal{R}}_H$. We now set $\widetilde{\mathcal{R}}_H = \mathcal{R}_H - \overline{\mathcal{R}}_H$, so that our rules are partitioned as

$$\mathcal{R}_H = \overline{\mathcal{R}}_H \cup \widetilde{\mathcal{R}}_H.$$

The module V. We write the elements of the $\mathbb{Z}_p H$-module V multiplicatively as $\underline{\mathbf{v}}^{\underline{\mathbf{e}}} = v_1^{e_i} \cdots v_d^{e_d}$ with $\underline{\mathbf{e}} = (e_1, \dots e_d) \in \mathbb{Z}_p^e$. Let $\tau\colon H \to \mathrm{Aut}_{\mathbb{Z}_p}(V)$ describe the $\mathbb{Z}_p H$-action on V. Correspondingly, we choose an alphabet of d generators $\underline{\mathbf{b}} = (b_1, \dots, b_d)$, and consider the set of rules

$$\mathcal{R}_V = \{b_i^p \to \emptyset,\;\; b_j b_j \to b_i b_j : i \in \{1, \dots, d\}, j > i\}. \tag{7.1}$$

These rules form a reduced confluent rewriting system with respect to the ordering $\prec_b$, which is the iterated wreath product ordering of length-lex orderings on words in a single symbol b_i. They define a normal form $\underline{\mathbf{b}}^{\underline{\mathbf{e}}} = b_1^{e_1} b_2^{e_2} \cdots b_d^{e_d}$ with $\underline{\mathbf{e}} \in \mathbb{Z}_p^d$. The set $\mathcal{R}_V$ therefore describes a monoid isomorphic to V via $b_i \to v_i$.

Extensions of H with V. We now take the combined alphabet $\mathcal{A} = \{a_1^{\pm 1}, \dots, a_e^{\pm 1}\} \cup \{b_1, \dots, b_d\}$ and denote by $\prec$ the wreath product ordering $\prec_b \wr \prec_a$, see [34, p. 46]. We define $\mathcal{R}_M$ to be the set of all rules

$$\mathcal{R}_M = \{b_j a_i^\sigma \to a_i^\sigma \underline{\mathbf{b}}^{(f_{i,j,\sigma,1}, \dots, f_{i,j,\sigma,d})} : \sigma \in \{\pm 1\}, i \in \{1, \dots, e\}, j \in \{1, \dots, d\}\}$$

where the exponents $f_{i,j,\sigma,k}$ are defined by $v_j^{\tau(a_i^\sigma)} = \underline{\mathbf{v}}^{(f_{i,j,\sigma,1}, \dots, f_{i,j,\sigma,d})}$.

If $\widetilde{\mathcal{R}}_H$ has r rules, then corresponding to those we define an ordered set of indeterminates over $\mathbb{Z}_p$, namely

$$\underline{\mathbf{x}} = (x_{1,1}, \dots, x_{1,d},\; x_{2,1}, \dots, x_{2,d},\; \dots,\; x_{r,1}, \dots, x_{r,d}),$$

and define a set of new rules $\mathcal{R}_H(\underline{\mathbf{x}})$ that consists of the rules in $\widetilde{\mathcal{R}}_H$ modified by a co-factor (or *tail*), which is an element of V given as a word in $\underline{\mathbf{b}}$ that is parameterized by the values of the variables $\underline{\mathbf{x}}$:

$$\mathcal{R}_H(\underline{\mathbf{x}}) = \{l_i \to r_i \underline{\mathbf{b}}^{(x_{i,1},\dots,x_{i,d})} : (l_i \to r_i) \in \widetilde{\mathcal{R}}_H\}. \tag{7.2}$$

Lastly, we set

$$\mathcal{R} = \mathcal{R}(\underline{\mathbf{x}}) = \mathcal{R}_H(\underline{\mathbf{x}}) \cup \mathcal{R}_V \cup \mathcal{R}_M \cup \overline{\mathcal{R}}_H.$$

In conclusion: the rules in $\mathcal{R}_H(\underline{\mathbf{x}})$ (together with $\overline{\mathcal{R}}_H$) are the original rules of the rewriting system of the quotient H, with appended parametrised tails; the rules in $\mathcal{R}_V$ encode the group structure of V, and the rules in $\mathcal{R}_M$ encode its H-module structure. By the definition of the wreath product ordering, for all rules in $\mathcal{R}$ we have that the left hand side is larger than the right hand side; thus $\mathcal{R}$ is a rewriting system. Since $\mathcal{R}_V$ is always reduced, it follows that $\mathcal{R}$ is reduced if $\mathcal{R}_H$ is.

We aim to find conditions on the variables $\underline{\mathbf{x}}$ that make $\mathcal{R}(\underline{\mathbf{x}})$ confluent, and first observe that in this case the rewriting system describes a group extension as desired. We denote any particular assignment of values to $\underline{\mathbf{x}}$ by $\underline{\mathbf{y}} \in \mathbb{Z}_p^{dr}$.

Lemma 7.1. *For any $\underline{\mathbf{y}} \in \mathbb{Z}_p^{dr}$, the monoid presentation $\langle \mathcal{A} \mid \mathcal{R}(\underline{\mathbf{y}})\rangle$ defines a group.*

Proof. It is sufficient to show that every generator has an inverse. The rules $b_i^p \to \emptyset$ in (7.1) show that every generator b_i has an inverse. As H is a group, $\mathcal{R}_H$ must contain rules that allow for free cancellation. If the order of h_i is not 2, these rules must be of the form $a_i a_i^{-1} \to \emptyset$ and $a_i^{-1} a_i \to \emptyset$. These rules imply that a_i and a_i^{-1} are mutual inverses and they must lie in $\overline{\mathcal{R}}_H \subseteq \mathcal{R}(\underline{\mathbf{y}})$. If the order of h_i is 2, then there will be a rule $a_i^{-1} \to a_i$ in $\overline{\mathcal{R}}_H$ (thus the generator a_i^{-1} is a redundant, duplicate, generator) and a rule $a_i^2 \to \emptyset$ in $\widetilde{\mathcal{R}}_H$; this last rule implies by (7.2) the existence of a rule $(a_i^2 \to w) \in \mathcal{R}_H(\underline{\mathbf{y}}) \subset \mathcal{R}(\underline{\mathbf{y}})$, with w a word in the generators $\{b_1, \dots, b_d\}$ only. Thus w represents an invertible element, and $a_i w^{-1}$ will be an inverse for a_i. □

Thus we can consider $\mathcal{R}(\underline{\mathbf{y}})$ as relations of a group presentation with abstract generators

$$\mathcal{A}' = \{a_1, \dots, a_e, b_1, \dots, b_d\};$$

note that some of the relations might become vacuously true in a group. Since H acts linearly on V, the set of values of $\underline{\mathbf{x}}$ that make the rewriting system confluent is a subspace of $\mathbb{Z}_p^{dr}$, denoted by

$$X = \{\underline{\mathbf{y}} \in \mathbb{Z}_p^{dr} : \mathcal{R}(\underline{\mathbf{y}}) \text{ confluent}\}. \tag{7.3}$$

Lemma 7.2. *If $\underline{\mathbf{y}} \in X$, then $\langle \mathcal{A}' \mid \mathcal{R}(\underline{\mathbf{y}})\rangle$ defines a group that is an extension of H with V where the conjugation action of H equals the module action.*

Proof. The relations in $\mathcal{R}_V$ and $\mathcal{R}_M$ show that $N = \langle b_1, \dots, b_d\rangle$ is abelian and normal. As the only relations in $\mathcal{R}$ whose left side only involves the generators $b_1, \dots, b_d$ are the relations in $\mathcal{R}_V$, confluence of $\mathcal{R}$ implies that no other rules apply to a word in these generators, thus N is isomorphic to V. The factor group can be described by setting all b_i to 1 in the relations; this produces the rules $\mathcal{R}_H$, and those define H. The rules in $\mathcal{R}_M$ prove the claim about the action. □

Cohomology. Vice versa, consider an extension E of H with V defined by $\gamma \in Z^2(H,V)$. Note that E has underlying set $H \times V$ with multiplication $(g,v)(h,w) = (gh, v^h w\gamma(g,h))$, see (4.1). For the chosen generators h_i of H, corresponding to the rewriting system $\mathcal{R}_H$, we set $u_i = (h_i, 1)$, and let $\underline{\mathbf{u}} = (u_1, \dots, u_e)$. We also choose a basis $\underline{\mathbf{v}}$ for (the image in E of) V. The elements in $\underline{\mathbf{u}} \cup \underline{\mathbf{v}}$ satisfy the relations in $\mathcal{R}_V \cup \mathcal{R}_M \cup \overline{\mathcal{R}}_H$. Furthermore, for any rule $l_i \to r_i \mathbf{b}^{(x_{i,1},\dots,x_{i,d})}$ in $\mathcal{R}_H(\underline{\mathbf{x}})$, we can find an assignment for the $\{x_{i,j}\}_j$ to values in $\mathbb{Z}_p$, such that this rule evaluated at $\underline{\mathbf{u}} \cup \underline{\mathbf{v}}$ holds. Thus there exists $\underline{\mathbf{y}} \in \mathbb{Z}_p^{rd}$, such that the rules in $\mathcal{R}(\underline{\mathbf{y}})$ hold in E. Since these rules imply a normal form for the H-part and for the V-part, we know that this rewriting system is confluent, that is, $\underline{\mathbf{y}} \in X$. Because of Lemma 7.2, this process defines a surjective map

$$\xi \colon Z^2(H,V) \to X,$$

such that E_γ is isomorphic to the group $\langle \mathcal{A}' \mid \mathcal{R}(\xi(\gamma))\rangle$ determined by $\xi(\gamma) \in \mathbb{Z}_p^{dr}$. By construction, the dr entries in $\xi(\gamma)$ are products of elements of the form $\gamma(a,b)^c$ with $a, b, c \in H$, so ξ is a linear map. Finally, if $\gamma \in \ker \xi$, then $\xi(\gamma) = \underline{\mathbf{0}}$ and the group given by $\mathcal{R}(\underline{\mathbf{0}})$ is a split extension (as the elements representing H form a subgroup), thus $\gamma \in B^2(H,V)$. We summarize:

Theorem 7.3. *The tuples $\underline{\mathbf{x}}$ that make $\mathcal{R}$ confluent form a $\mathbb{Z}_p$-vector space $X = \xi(Z^2(H,V))$ and $\ker \xi \leqslant B^2(H,V)$, hence $H^2(H,V) \cong \xi(Z^2(H,V))/\xi(B^2(H,V))$.*

7.2. Making the system confluent

We now describe how to compute the images of $Z^2(H,V)$ and $B^2(H,V)$ under ξ, leading to a construction of $H^2(H,V)$ via Theorem 7.3.

We start with $Z^2(H,V)$ and recall that $\xi(Z^2(H,V)) = X$ as in (7.3). Using the Knuth-Bendix method as described in [34, Section 2.3], to compute X we need to consider overlaps of left hand sides of rules in $\mathcal{R}(\underline{\mathbf{x}})$. Set $\overline{\mathcal{R}}_H(\underline{\mathbf{x}}) = \mathcal{R}_H(\underline{\mathbf{x}}) \cup \overline{\mathcal{R}}_H$, so

$$\mathcal{R}(\underline{\mathbf{x}}) = \overline{\mathcal{R}}_H \cup \mathcal{R}_M \cup \mathcal{R}_V$$

is the union of three sets. Thus, there will be six kinds of overlaps, which we now consider separately. Overlaps of left hand sides of rules in $\mathcal{R}_V$ reduce uniquely by the definition of $\mathcal{R}_V$. The left hand sides of two rules in $\mathcal{R}_M$ cannot overlap because of their specific form. Similarly, rules in $\mathcal{R}_V$ and $\overline{\mathcal{R}}_H$ cannot overlap as their left hand sides are on disjoint alphabets. The overlap of a left hand side in $\mathcal{R}_V$ and in $\mathcal{R}_M$ will have the form $w_{\underline{\mathbf{b}}}a_i^{\pm 1}$ (where $w_{\underline{\mathbf{b}}}$ is a word expression in $\underline{\mathbf{b}}$) and reduces uniquely as the action on V is linear. A left hand side in $\mathcal{R}_M$ and one in $\overline{\mathcal{R}}_H$ will overlap in the form $w_{\underline{\mathbf{b}}}w_{\underline{\mathbf{a}}}$; such expressions reduce uniquely as the action on a module is a group action. This leaves overlaps of left hand sides in $\overline{\mathcal{R}}_H$. For this we note that the rules in $\mathcal{R}_V \cup \mathcal{R}_M$ allow us to transform any word expression into a form $w = ab$ (called *clean*) where a is a word in $\underline{\mathbf{a}}$, and b a reduced word in $\underline{\mathbf{b}}$. We call these factors the $\underline{\mathbf{a}}$-part and $\underline{\mathbf{b}}$-part, respectively. Furthermore, the $\underline{\mathbf{a}}$-part of the clean form of a word is simply the image of the word when setting all generators in $\underline{\mathbf{b}}$ to one. As every rule in $\overline{\mathcal{R}}_H$ corresponds to a rule in $\mathcal{R}_H$, and since $\mathcal{R}_H$ is confluent, this together shows that the $\underline{\mathbf{a}}$-part of any reduced word will be unique. If we write a word as a product (in arbitrary order) of elements in $\underline{\mathbf{a}}$ with powers of generators in $\underline{\mathbf{b}}$, the $\underline{\mathbf{b}}$-part of a clean form of a word will be a normal form $\underline{\mathbf{b}}^{(e_1,\dots,e_d)}$, where the e_i are homogeneous linear functions in the exponents of the $\underline{\mathbf{b}}$-generators in the original word. Reduction with rules in $\overline{\mathcal{R}}_H$ will introduce powers of $\underline{\mathbf{b}}$ with exponents given by variables in $\underline{\mathbf{x}}$. By reducing the overlap of two left hand sides of rules in $\overline{\mathcal{R}}_H$, and by reducing the resulting two words further to (arbitrary) reduced forms, we obtain clean words with equal $\underline{\mathbf{a}}$-parts and whose $\underline{\mathbf{b}}$-parts are in normal form $\underline{\mathbf{b}}^{(e_1,\dots,e_d)}$, where the e_i are homogeneous linear expressions in the variables $\underline{\mathbf{x}}$.

In conclusion, we have shown that the equality of the reduced forms of an overlap is equivalent to a homogeneous linear equation in $\underline{\mathbf{x}}$; by processing all overlaps, we obtain a homogeneous system of linear equations. Confluence of $\mathcal{R}(\underline{\mathbf{x}})$ for a particular set of values of $\underline{\mathbf{x}}$ then is equivalent to $\underline{\mathbf{x}}$ satisfying this system over $\mathbb{Z}_p$; this allows us to compute $X = \xi(Z^2(H,V))$ as the solution space of a homogeneous linear equation system.

We can calculate $\xi(B^2(H,V))$ in a way similar to the establishment of the equations. For a function $\lambda\colon H \to V$ we replace a_i by $a_i\lambda(a_i)$ in the rules in $\mathcal{R}_H(\underline{\mathbf{0}})$, and use the rules in $\mathcal{R}_M$ and $\mathcal{R}_V$ to bring left and right side into a clean form. Comparison of the remaining $\underline{\mathbf{b}}$-parts gives exponent vectors that combine to the image of the associated cocycle under ξ.

8. Practical aspects

8.1. Hybrid groups

We comment on the new data structure we have introduced to make our algorithm more efficient. Recall that once the respective module(s) V are chosen, our process to construct $\hat{H}_{V,e}$ builds on algorithms to perform the following calculations:

(1) Calculate $H^2(H,V)$ and construct extensions for particular cocycles.

(2) Construct semidirect products of H with elementary abelian subgroups V^r.
(3) Construct direct products of the groups computed in Step (2).
(4) Construct subgroups of the groups computed in Step (3) that map onto the full factor group H.
(5) Form factor groups of the groups computed in Step (4), by factoring out evaluated relators.

In most of these constructions, the result will always be a group that is the extension of H with an elementary abelian subgroup. We represent such groups as formal polycyclic-by-finite extensions, given as a finitely presented group. Contrary to the more general construction in [35], we form a confluent rewriting system for the whole group, which is used to calculate normal forms. Such a rewriting system can be combined easily from a rewriting system for H (which we anyhow have for the purposes of computing the cohomology group), a polycyclic generating set for the normal subgroup, and cocycle information that describes the extension structure. We call such a computer representation a *hybrid group*. We also assume that we are able to translate between the generators for H arising as image of the generators of F, and the generators of the rewriting system.

In practice, we split the rewriting system for a hybrid group E into a rewriting system for the non-solvable factor $H = E/N$, a polycyclic generating set for the normal subgroup N, automorphisms of N that represent the action of factor group generator representatives, and cofactors (in N) associated to the rewriting rules for the factor. Arithmetic in E then uses the built-in arithmetic for polycyclic elements, as this will be faster than an alternative rewriting implementation. Indeed, if H has a solvable normal subgroup, arithmetic will be faster if, in a given hybrid group, we modify the extension structure to have the solvable normal subgroup as large as possible.

As for the algorithmic requirements listed above, the information available from the cohomology computation is exactly what is needed to represent extensions as hybrid groups. The construction of (sub)direct products or semidirect products is similarly immediate. For a subgroup S of a hybrid group, given by generators, such that $SN = E$ (this holds for all subgroups we encounter), we can calculate generators for $S \cap N$ from the presentation for the factor group, and then determine an induced polycyclic generating set for $S \cap N$. This allows us to represent S by its own hybrid representation. In the same way, a polycyclic generating set for factor groups can be used to represent factors by normal subgroups contained in N. All calculations of the quotient algorithm therefore can take place in hybrid groups, all for the same factor H. Since the order of these groups is known, and since a rewriting system is a special case of a presentation, we could use representations induced by the abelianization of subgroups (as suggested in [16]) to find faithful permutation representations.

It clearly would be of interest to study the feasibility of these hybrid groups for general calculations. Doing so will require significant more infrastructure work for these groups than we have currently done. While we are optimistic about the general practical feasibility of such a representation (e.g. following [35]), we do not want to make any such claim at this point.

8.2. *Cost estimates*

It seems difficult to obtain complexity statements that reflect practical behaviour. For example, even proving that computing with polycyclic groups has a favourable complexity is difficult because of the challenges involving *collection*, see [24]. Despite these obstacles, it is still clearly beneficial to be able to study a finitely presented group via a polycyclic quotient. The algorithmic framework considered in this work faces similar obstacles. Nevertheless, below we briefly discuss some cost estimates of some of the tasks required for the construction of $\hat{H}_{V,e}$.

Following [32], obtaining a confluent rewriting system for H essentially means to determine a composition series of H, and to look up precomputed rewriting systems for the simple composition factors; the system will asymptotically have $r \leqslant \sqrt{|H|}$ rules, though in many cases this bound is far from reality. Determining $H^2(H, V)$ then requires solving a linear system with $r \dim(V)$ variables and r^2 equations. If H is simple with BN-pair, then the maximal length ℓ of a word in normal form for this rewriting system (created in [32]) is bounded by $\mathcal{O}(\log(|H|))$, but it could be as large as $|H|/2$ if H is cyclic of prime order. Assuming $|H|$ has only small prime divisors, we get $\ell = \mathcal{O}(\log |H|)$.

We now estimate the cost of multiplication in a hybrid group E with $E/N = H$ and N abelian. Calculating the image of an element in N under a word (of length up to ℓ) representing an element of H requires taking ℓ images of elements of N under homomorphisms, and each such image requires $\log |N|$ multiplications in N. Considering elements in E as pairs, the first step of multiplying $h_1 \cdot n_1$ and $h_2 \cdot n_2$ in E is to compute $n_1^{h_2} n_2$, at the cost of $\ell \log |N| + 1$ multiplications in N. Computing the product $h_1 \cdot h_2$ then involves a reduction sequence, say of length up to s, using the rewriting system for H. Applying such an extended rewriting rule, say $w \to u \cdot n$ with (potential) tail n, to a word $a \cdot w \cdot b$ results in $a \cdot u \cdot b \cdot n^b$ and requires another homomorphic image computation. Multiplication in E therefore requires up to $(s + 1)\ell \log |N|$ products in N.

For constructing $\hat{H}_{V,e}$ via Theorem 5.2, we form (for $\Psi_{V,e}(F)$ and the extensions E_i) an extension of H with $e \dim(V) + \dim(H^2(H, V))$ copies of V. Even if the cohomology group is small, we work in an extension with a normal subgroup of order $\approx p^{\dim(V)^2}$, so $\log(|N|) \sim \dim(V)^2$. The cost of lifting an epimorphism $\varphi \colon G \to H$ to $\tau \colon G \to \tilde{H}$ with a maximal V-homogeneous kernel is therefore proportional to $v(s + 1)\ell \dim(V)^2$, where v is the sum of the lengths of the relators defining G.

In practical calculations, the main bottleneck for the algorithm currently lies in the application of rewriting rules. At the moment, this is done by a generic rewriting routine, operating on words. This could clearly be improved, for example by moving code from the system library into the kernel, and by changing the order in which rules are applied, in particular for cases with large elementary abelian subgroups. Doing so, however is a substantial task on its own.

Please cite this article in press as: H. Dietrich, A. Hulpke, Universal covers of finite groups, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2020.10.032

8.3. Example computations

As a proof of concept and to illustrate the capabilities of our methods, we have implemented the algorithms described here in the computer algebra system GAP [4]. The implementation of the 2-cohomology group and the construction of extensions will be available with release 4.11. Our code for hybrid groups, the construction of $\hat{H}_{V,e}$, and for lifting of epimorphisms is available at github.com/hulpke/hybrid. We illustrate the scope of the algorithm and the performance of its implementation in a number of examples; the code for those examples can be found in the file `example.g` in the same GitHub repository. Calculation times are in seconds on a 3.7 GHz 2013 Mac Pro with 16 GB of memory available. We write extensions as $A.B.C = A.(B.C)$, etc.

The examples we consider here are all not solvable. While our implementation also works for solvable groups, it becomes non-competitive in comparison to a dedicated solvable quotient implementation: The reason for this is, at least in part, that element arithmetic in the constructed covers, as well as the calculation of cohomology groups, both go through a generic rewriting system in the routines library, instead of using dedicated kernel routines for groups with a polycyclic presentation.

Example 8.1. The *Heineken group* $\mathcal{H} = \langle a, b, c \mid [a, [a, b]] = c, [b, [b, c]] = a, [c, [c, a]] = b\rangle$ is infinite and 2-generated. By von Dyck's Theorem [15, Theorem 2.53], there is, up to automorphisms, a unique epimorphism $\varphi\colon \mathcal{H} \to H$ onto the alternating group $H = A_5$, defined by $\varphi(a) = (1, 2, 4, 5, 3)$ and $\varphi(b) = (1, 2, 3, 4, 5)$. It has been shown in [14, p. 725] that the largest finite nilpotent quotient of $\ker\varphi$ has order 2^{24}. We now apply our algorithm: A_5 has three irreducible modules over $\mathbb{Z}_2$. The trivial module yields a cover $2^3.A_5$ and lifts φ to a quotient of type $2.A_5$. The absolutely irreducible module of dimension 4 yields a cover $2^{4\cdot 4}.A_5$ (we write $p^{a\cdot b}$ for a b-fold direct product of an a-dimensional module) and lifts φ to a quotient $2^4.A_5$, and the other module of dimension 4 yields a cover $2^4.A_5$ that does not lift φ. Table 1 shows results and timings when iterating the lifting process until the maximal quotient for prime $p = 2$ has been found and confirmed as maximal. The whole calculation took under 4 minutes on a 3.7 GHz 2013 Mac Pro with 16 GB of memory available.

Example 8.2. The group $G = G_{(3,4,15;2)} = \left\langle a, b \mid a^3, b^4, (ab)^{15}, [a, b]^2\right\rangle$ is an example of presentations of type "$(m, n, p; q)$" going back to Coxeter, and it is known that G is infinite, see [37]. The group G has a unique quotient isomorphic to A_6. For characteristic 3 we obtained the quotients in Table 1.

Example 8.3. The group $G = G_{(3,7,15;10)} = \left\langle a, b \mid a^3, b^7, (ab)^{10}, [a, b]^{10}\right\rangle$ is also known to be infinite. It has four different epimorphisms $\varphi_i\colon G \to A_{10}$, distinguished by having different kernels. Contrary to the previous two examples, it is hard to find usable presentations for the corresponding kernels, as the index $10!/2$ is large. This example is therefore intractable with traditional methods. Here we only considered the modules

Table 1
Isomorphism types of the iterated quotients of the Heineken group (left) and $G_{(3,4,15;2)}$ (right); computations were carried out on a 3.7 GHz 2013 Mac Pro with 16 GB of memory available; times are given in seconds.

Isomorphism type of quotient	Time
$2.(2 \times 2^4).A_5$	1
$2^4.2.(2 \times 2^4).A_5$	2
$2^4.2^4.2.(2 \times 2^4).A_5$	5
$(2 \times 2).2^4.2^4.2.(2 \times 2^4).A_5$	11
$2^4.(2 \times 2).2^4.2^4.2.(2 \times 2^4).A_5$	18
$2^4.2^4.(2 \times 2).2^4.2^4.2.(2 \times 2^4).A_5$	51
No larger quotient for $p = 2$	118

Isomorphism type of quotient	Time
$(3 \times 3^6).A_6$	7
$3^{4\cdot 2}.(3 \times 3^6).A_6$	35
$(3^4 \times 3^{6\cdot 2} \times 3^9).3^{4\cdot 2}.(3 \times 3^6).A_6$	171

of small dimensions, as the next smallest dimension would be 26, resulting in the construction of an (abelian) polycyclic group with $2 \cdot 26^2 = 1352$ generators. Working with automorphisms of such a group would end up being unreasonably slow, because GAP currently has no special treatment of abelian polycyclic groups. The given runtimes also exclude the cost of determining the irreducible modules. For φ_1, the algorithm finds a lift to a group $(2 \times 2^{8\cdot 3}).A_{10}$ in 36 seconds. Lifting again produces a larger quotient $2^{1\cdot 5}.(2 \times 2^{8\cdot 3}).A_{10}$ in 11 minutes.

In characteristic 3, we find a quotient $(3^{9\cdot 2}).A_{10}$ in 49 sec., in characteristic 5 a quotient $5^{8\cdot 1}.A_{10}$ in 33 sec. For φ_2 and φ_4, we find a quotient of type $2^{8\cdot 1}.A_{10}$, for φ_3 a quotient of type $(2 \times 2^{8\times 1}).A_{10}$, thus showing that these A_{10} quotients fall in at least three different equivalence classes.

Example 8.4. To illustrate the behaviour with larger quotients, we consider prime 2 and the group

$$G = \left\langle a, b \mid a^3, b^6, (ab)^6, (a^{-1}b)^6 \right\rangle,$$

which is example P_{10} in [27]; this group has a quotient of isomorphism type A_7.

The maximal lift of this quotient with an elementary abelian kernel in characteristic 2 is

$$(2 \times 2^{4\cdot 2} \times 2^{4\cdot 2} \times 2^{14\cdot 3} \times 2^{20\cdot 7}).A_7,$$

and is found in about 8 minutes on a 3.7 GHz 2013 Mac Pro with 16 GB of memory available. If we restrict to simple modules of dimension < 5, then we find a lift to $(2 \times 2^{4\cdot 2} \times 2^{4\cdot 2}).A_7$ in 2 seconds. Under the same restrictions, we can lift this to $(2^{1\cdot 5} \times 2^{4\cdot 2} \times 2^{4\cdot 2}).(2 \times 2^{4\cdot 2} \times 2^{4\cdot 2}).A_7$, in 48 seconds. The third lift to

$$(2^{1\cdot 6} \times 2^{4\cdot 2} \times 2^{4\cdot 2}).(2^{1\cdot 5} \times 2^{4\cdot 2} \times 2^{4\cdot 2}).(2 \times 2^{4\cdot 2} \times 2^{4\cdot 2}).A_7,$$

is found in 194 seconds, and the fourth lift to a quotient of size $2^{84} \cdot |A_7|$ is found after about 46 minutes:

Please cite this article in press as: H. Dietrich, A. Hulpke, Universal covers of finite groups, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2020.10.032

$$(2^{1\cdot 8} \times 2^{4\cdot 2} \times 2^{4\cdot 2}).(2^{1\cdot 6} \times 2^{4\cdot 2} \times 2^{4\cdot 2}).(2^{1\cdot 5} \times 2^{4\cdot 2} \times 2^{4\cdot 2}).(2 \times 2^{4\cdot 2} \times 2^{4\cdot 2}).A_7.$$

In characteristic 3, the maximal lift of the A_7 quotient with an elementary abelian kernel is

$$(3^{1\cdot 3} \times 3^{6} \times 3^{13} \times 3^{15\cdot 4} \times 3^{20\cdot 3}).A_7,$$

and is found in about 2 minutes on a 3.7 GHz 2013 Mac Pro with 16 GB of memory available. If we restrict to simple modules of dimension < 13, then we find a lift to $(3^{1\cdot 3} \times 3^{6} \times 3^{13}).A_7$ in 22 seconds. Under the same restrictions, we can lift this to a quotient of size $3^{134} \cdot |A_7|$ in 42 minutes:

$$(3^{1\cdot 3} \times 3^{6\cdot 3} \times 3^{13\cdot 7}).(3^{1\cdot 3} \times 3^{6} \times 3^{13}).A_7.$$

Acknowledgments

Both authors thank the anonymous referee for their very careful reading. Dietrich was supported by an Australian Research Council grant, identifier DP190100317. Hulpke was supported in part by National Science Foundation grant DMS-1720146. Parts of the research were performed during visits of the second author at Hausdorff Institute in Bonn, Germany in autumn 2018 and at Monash University in Melbourne, Australia in autumn 2019. The hospitality of both institutions is gratefully acknowledged.

Appendix A. Proofs of some representation theory results

For the sake of completeness, we provide the proofs missing in Section 2.

Proof of Lemma 2.3. a) If $D < A$ is a maximal submodule, then $C/(C \cap D)$ embeds in the simple module A/D, so $C \cap D = C$ or $C \cap D < C$ is maximal. In both cases, $\mathrm{rad}(C) \leqslant C \cap D$, so $\mathrm{rad}(C) \leqslant \mathrm{rad}(A)$. This also shows $\mathrm{rad}(A) \oplus \mathrm{rad}(B) \leqslant \mathrm{rad}(A \oplus B)$. Conversely, if $W < A$ and $V < B$ are maximal, then $W \oplus B, A \oplus V < A \oplus B$ are maximal, so $\mathrm{rad}(A \oplus B) \leqslant \mathrm{rad}(A) \oplus \mathrm{rad}(B)$.

b) Let $D = \sigma(A)$, so $\sigma\colon A \to D$ is surjective and $\mathrm{rad}(D) \leqslant \mathrm{rad}(B)$ by a). If $V < D$ is maximal and W is the full preimage of V under σ, then σ induces an isomorphism $A/W \cong D/V$, and $W < A$ is maximal. Thus, $\mathrm{rad}(A) \leqslant W$, and so $\sigma(\mathrm{rad}(A)) \leqslant V$. Thus, $\sigma(\mathrm{rad}(A)) \leqslant \mathrm{rad}(D)$.

c) The module $A/\mathrm{rad}(A)$ embeds into a direct sum of simple modules, hence is semisimple. If $\mathrm{rad}(A) \leqslant C$, then $A/C \cong (A/\mathrm{rad}(A))/(C/\mathrm{rad}(A))$ is semisimple. Conversely, if A/C is semisimple, then $\mathrm{rad}(A/C) = 0$ and so $\mathrm{rad}(A) \leqslant C$. To prove the first claim, let $E \leqslant A$ be the submodule with $E/C = \mathrm{rad}(A/C)$. Applying b) to the projection $A \to A/C$ yields $(\mathrm{rad}(A) + C)/C \leqslant \mathrm{rad}(A/C)$, so $\mathrm{rad}(A) + C \leqslant E$. Now

$B = \operatorname{rad}(A) + C$ is a submodule of A with $(A/C)/(B/C) \cong A/(C + \operatorname{rad}(A))$ semisimple. Thus, $\operatorname{rad}(A/C) \leqslant B/C$, and so $E = \operatorname{rad}(A) + C$. □

Proof of Lemma 2.5. Write $N = \mathbb{F}H$. Being finite fields, $\underline{\mathbb{F}} \geqslant \mathbb{F}$ is a Galois extension, so [22, Theorem 1.8.4] proves a). If $S < N$ is a maximal submodule, then $\underline{\mathbb{F}}(N/S) \cong \underline{\mathbb{F}}H/\underline{\mathbb{F}}S$ is semisimple, so $\operatorname{rad}(\underline{\mathbb{F}}H) \leqslant \underline{\mathbb{F}}\operatorname{rad}(N)$. Conversely, $\underline{\mathbb{F}}H/\underline{\mathbb{F}}\operatorname{rad}(N) \cong \underline{\mathbb{F}}(N/\operatorname{rad}(N))$ and $N/\operatorname{rad}(N)$ is a direct sum of simple $\mathbb{F}H$-modules; now a) shows that $\underline{\mathbb{F}}(N/\operatorname{rad}(N))$ is a semisimple $\underline{\mathbb{F}}H$-module. This implies $\operatorname{rad}(\underline{\mathbb{F}}H) \leqslant \underline{\mathbb{F}}\operatorname{rad}(N)$, and therefore equality is established. This proves b). □

Proof of Theorem 2.6. Most of this follows from the Krull-Schmidt Theorem [22, Theorem 1.6.6] and Remark 1.6.22(a), Theorem 1.6.24, Theorem 1.6.20(b) in [22]. It remains to provide a proof for the multiplicity r_i in the case that $\mathbb{F}$ is not algebraically closed. Let $\underline{\mathbb{F}}D_i = C_1 \oplus \cdots \oplus C_k$ be a direct sum of $\underline{\mathbb{F}}$-projective indecomposables; note that the C_j are direct summands of the regular module $\underline{\mathbb{F}}H$. By Lemma 2.5, each $C_j/\operatorname{rad}(C_j)$ is a simple $\underline{\mathbb{F}}H$-modules and the isomorphism type of C_j is determined by the isomorphism type of $C_j/\operatorname{rad}(C_j)$; in particular, the direct sum constituents of $\underline{\mathbb{F}}(D_i/\operatorname{rad}(D_i))$ are the simple factors $C_j/\operatorname{rad}(C_j)$ and they are mutually non-isomorphic. The multiplicity r_i of D_i as a direct summand of $\mathbb{F}H$ thus equals the multiplicity of C_j as a direct summand of $\underline{\mathbb{F}}H$, which is the multiplicity of $C_j/\operatorname{rad}(C_j)$ as a direct summand of $\underline{\mathbb{F}}H/\operatorname{rad}(\underline{\mathbb{F}}H)$. Wedderburn's theorem implies $r_i = \dim_{\underline{\mathbb{F}}}(C_j/\operatorname{rad}(C_j))$, see [22, Remark 1.6.22(a), Theorem 1.6.24]. □

References

[1] M.R. Bridson, D.M. Evans, M.W. Liebeck, D. Segal, Algorithms determining finite simple images of finitely presented groups, Invent. Math. 218 (2019) 623–648.
[2] J. Cossey, O.H. Kegel, L.G. Kovacs, Maximal Frattini extensions, Arch. Math. 35 (1980) 210–217.
[3] C.W. Curtis, I. Reiner, Methods of Representation Theory, Vol. I, Wiley, 1981.
[4] The GAP Group, GAP – groups, algorithms, and programming, available at gap-system.org.
[5] W. Gaschütz, Über modulare Darstellungen endlicher Gruppen, die von freien Gruppen induziert werden, Math. Z. 60 (1954) 274–286.
[6] W. Gaschütz, Zu einem von B. H. und H. Neumann gestellten Problem, Math. Nachr. 14 (1955) 249–252.
[7] R.L. Griess, P. Schmid, The Frattini module, Arch. Math. (Basel) 30 (1978) 256–266.
[8] R.J.R. Groves, An algorithm for computing homology groups, J. Algebra 194 (1977) 331–361.
[9] K.W. Gruenberg, Relation Modules of Finite Groups, Conference Board of the Mathematical Sciences Regional Conference Series in Mathematics, vol. 25, American Mathematical Society, Providence, R.I., 1976.
[10] G. Havas, M.F. Newman, Application of computers to questions like those of Burnside, in: Burnside Groups, Proc. Workshop, Univ. Bielefeld, Bielefeld, 1977, in: Lecture Notes in Math., vol. 806, Springer, Berlin, 1980, pp. 211–230.
[11] D.F. Holt, The mechanical computation of first and second cohomology groups, J. Symb. Comput. 1 (1985) 351–361.
[12] D.F. Holt, The Meataxe as a tool in computational group theory, in: The Atlas of Finite Groups: Ten Years on, Birmingham, 1995, in: London Math. Soc. Lecture Note Ser., vol. 249, Cambridge Univ. Press, 1998, pp. 74–81.
[13] D.F. Holt, W. Plesken, Perfect Groups, Oxford University Press, New York, 1989.
[14] D.F. Holt, S. Rees, Computing with Abelian sections of finitely presented groups, J. Algebra 214 (1999) 714–728.

Please cite this article in press as: H. Dietrich, A. Hulpke, Universal covers of finite groups, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2020.10.032

[15] D.F. Holt, B. Eick, E.A. O'Brien, Handbook of Computational Group Theory, Discrete Mathematics and Its Applications, (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2005.

[16] A. Hulpke, Representing subgroups of finitely presented groups by quotient subgroups, Exp. Math. 10 (2001) 369–381.

[17] S. Jambor, An L_2-quotient algorithm for finitely presented groups on arbitrarily many generators, J. Algebra 423 (2015) 1109–1142.

[18] S. Jambor, An L_3-U_3-quotient algorithm for finitely presented groups, PhD thesis, RWTH Aachen University, 2012, see math.auckland.ac.nz/~jambor/#thesis.

[19] D.L. Johnson, Presentations of Groups, Cambridge University Press, 1997.

[20] E.H. Lo, A polycyclic quotient algorithm, J. Symb. Comput. 25 (1998) 61–97.

[21] C.R. Leedham-Green, A Soluble Group Algorithm, in: Computational Group Theory, Durham 1982, Academic Press, 1984, pp. 85–101.

[22] K. Lux, H. Pahlings, Representations of Groups. A Computational Approach, Cambridge Studies in Advanced Mathematics, vol. 124, Cambridge University Press, Cambridge, 2010.

[23] I.D. Macdonald, A computer application to finite p-groups, J. Aust. Math. Soc. 17 (1974) 102–112.

[24] M.F. Newman, A. Niemeyer, On complexity of multiplication in finite soluble groups, J. Algebra 421 (2015) 425–430.

[25] W. Nickel, Computing nilpotent quotients of finitely presented groups, in: Geometric and Computational Perspectives on Infinite Groups, 1994, in: DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 25, Amer. Math. Soc., 1996, pp. 175–191.

[26] M.F. Newman, E.A. O'Brien, Application of computers to questions like those of Burnside. II, Int. J. Algebra Comput. 6 (1996) 593–605.

[27] A. Niemeyer, A finite soluble quotient algorithm, J. Symb. Comput. 18 (1994) 541–561.

[28] W. Plesken, Towards a soluble quotient algorithm, J. Symb. Comput. 4 (1987) 111–122.

[29] W. Plesken, A. Fabiańska, An L_2-quotient algorithm for finitely presented groups, J. Algebra 322 (2009) 914–935.

[30] D.J.S. Robinson, A Course in the Theory of Groups, Springer-Verlag, 1982.

[31] J. Schmidt, Rewriting systems for finite groups, Thesis (Ph.D.), University of Kentucky, 2008.

[32] J. Schmidt, Finite groups have short rewriting systems, in: Computational Group Theory and the Theory of Groups, II, in: Contemp. Math., vol. 511, Amer. Math. Soc., Providence, RI, 2010, pp. 185–200.

[33] Á. Seress, Permutation Group Algorithms, vol. 152, Cambridge University Press, Cambridge, 2003.

[34] C.C. Sims, Computation with Finitely Presented Groups, Cambridge University Press, 1994.

[35] S.K. Sinanan, D.F. Holt, Algorithms for polycyclic-by-finite groups, J. Symb. Comput. 79 (2017) 269–284.

[36] A. Stein, Zur Berechnung der zweiten Kohomologie, Unpublished notes, Martin-Luther-Universität Halle, 1997.

[37] R.M. Thomas, Group presentations where the relators are proper powers, vol. 2, in: Groups '93 Galway/St. Andrews, in: London Math. Soc. Lecture Note Ser., vol. 212, Cambridge Univ. Press, Cambridge, 1995, pp. 549–560.

[38] J. Thévenaz, Maximal subgroups of direct products, J. Algebra 198 (1997) 352–361.

Please cite this article in press as: H. Dietrich, A. Hulpke, Universal covers of finite groups, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2020.10.032

Sponsor names

Do not correct this page. Please mark corrections to sponsor names and grant numbers in the main text.

Australian Research Council, *country*=Australia, *grants*=`DP190100317`

National Science Foundation, *country*=United States, *grants*=`DMS-1720146`

Please cite this article in press as: H. Dietrich, A. Hulpke, Universal covers of finite groups, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2020.10.032