CONSTRUCTING UNIVERSAL COVERS OF FINITE GROUPS

HEIKO DIETRICH AND ALEXANDER HULPKE

ABSTRACT. Motivated by quotient algorithms, such as the well-known $p$-quotient or solvable quotient algorithms, we describe how to compute extensions $\hat{H}$ of a finite group $H$ by a direct sum of isomorphic simple $\mathbb{Z}_pH$-modules such that $H$ and $\hat{H}$ 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 relation 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. As an application, our results can be used to describe, 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 $V$. 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 $H$.

1. INTRODUCTION

Let $H$ be a finite group that can be generated by $e$ elements, and let $V$ be a finite simple $\mathbb{Z}_pH$-module. We consider the problem of describing extensions $\hat{H}$ of $H$ by a direct sum of copies of $V$ such that $\hat{H}$ can also be generated by $e$ elements. If $H$ happens to be a finite $p$-group, then our description is closely related to the well-known $p$-group generation algorithm. In both situations, the main idea is to construct a suitable covering group that contains every extension of interest as a factor group. While the covering group in $p$-group generation depends only on the isomorphism type of $H$, our cover depends also on the number of generators $e$ and the isomorphism type of $V$.

Our approach is to start with a finite presentation of $H$, say $H = F/M$, with $F$ free of rank $e$, and to consider the largest quotient of $M$ that is an elementary abelian $p$-group, say $M/M_p$. In Section 2, we define the $p$-cover of $H$ of rank $e$ to be the group $\hat{H}_{p,e} = F/M_p$: as shown in Theorem 2.4, if $\hat{H}$ is generated by $e$ elements and maps onto $H$ with elementary abelian kernel, then $\hat{H}$ is a quotient of $\hat{H}_{p,e}$. That the isomorphism type of this cover is independent of the chosen presentation of $H$ will follow from a result of Gaschütz [5], who has investigated the $H$-module structure of $M/M_p$. We discuss relevant details in Section 2.1.

It follows from the Nielsen-Schreier Theorem that $M/M_p$ has rank $1 + (e - 1)|H|$, which is usually too large for computational applications. We therefore study alternative ways to describe $\hat{H}_{p,e}$ and the module $M/M_p$, and also reduce to smaller modules. Our investigation in Section 3 will use results from Fox calculus (see [12, Section 11.4]): We show that Fox derivatives are...
related to a natural wreath product construction. Since Fox calculus has applications in other areas, such as knot theory, this construction might be of broader interest. Importantly, we show in Theorem 3.4 how to describe the covering \( \tilde{H}_{p,e} \) and the module \( M/M_p \) via this wreath product version of Fox derivatives. This is the crucial ingredient in our approach that makes our description computationally feasible. We continue in Section 4 with a discussion of how to work with a smaller quotient of \( M/M_p \), namely, a quotient that is \( V \)-homogeneous (isomorphic to a direct sum of copies of a simple module \( V \)); this leads to what we call the \( (V,e) \)-cover \( \hat{H}_{V,e} \) of \( H \). An explicit construction that does not involve the large module \( M/M_p \) is described in Theorem 5.2.

An interesting application of our work is that it can be used to describe a quotient algorithm: In general, for a finitely presented group \( G \), 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 of \( G \). The well-known \( p \)-quotient algorithm \([11, Section 9.4]\) attempts to construct the largest quotient of \( G \) that is a \( p \)-group. Solvable quotient algorithms, such as described by Plesken \([16]\) and Niemeyer \([15]\), attempt to construct the largest solvable quotient of \( G \). Our description can be used to develop a quotient algorithm for more general groups: Let \( \varphi : G \to H \) be an epimorphism onto a finite group \( H \) as above. We describe how to find a larger quotient \( \hat{H} \) of \( G \) that factors through \( \varphi \), such that the kernel of the projection \( \hat{H} \to H \) is a finite solvable group. Since every finite solvable group has a chief series with elementary abelian sections, we may suppose that the kernel of \( \hat{H} \to H \) is elementary abelian in prime characteristic \( p \), and then iterate. In fact, by also iterating over the isomorphism types of simple \( \mathbb{Z}_pH \)-modules, we may suppose that this kernel is \( V \)-homogeneous for some finite simple \( \mathbb{Z}_pH \)-module \( V \). Thus, we are interested in finding a larger quotient \( \hat{H} \) of \( G \) together with epimorphisms \( \varphi : G \to \hat{H} \) and \( \pi : \hat{H} \to H \) such that \( \varphi = \pi \circ \varphi \) and \( \ker \pi \) is \( V \)-homogeneous. In Section 5 we construct \( \hat{H} \) via a suitable covering group that depends on \( \varphi \) and \( V \).

Our description of \( \hat{H}_{V,e} \) in Section 5 requires the construction of the 2-cohomology of \( H \) with coefficients in an elementary abelian module. In Section 7 we therefore discuss the construction of extensions of non-polycyclic groups. Assuming confluent rewriting systems for the input groups, our approach for that is closely related to the computation of cohomology for polycyclic groups (using tails and consistency checks).

We conclude in Section 8 with some computational examples and some further remarks.

1.1. Notation and preliminaries. We reserve \( e \) and \( n \) for positive integers and \( p \) for primes. We denote by \( \mathbb{Z}_p \) the integers modulo \( p \) and by \( C_p \) the cyclic group of order \( p \). Throughout, \( \varphi : G \to H \) denotes an epimorphism of a finitely presented group \( G \) onto a finite group \( H \) of order \( m \). We assume that \( G \) (and thus also \( H \)) is \( e \)-generated, that is, \( G \) can be generated by \( e \) elements. Let \( F \) be the free group of rank \( e \) and let \( \psi : F \to H \) be the projection associated with a chosen generating set of \( H \); we set \( M = \ker \psi \) so that \( F/M \cong H \).

For a group \( A \) we define \( A_p = A'[A,p] \), where \( A' = [A, A] \) is the derived subgroup and \( A(p) \) is the subgroup generated by all \( p \)-th powers. With this definition, \( A/A_p \) is the largest \( p \)-elementary abelian quotient of \( A \). When describing extensions of groups, the common usage is to talk about a group \( G \) being an extension of a normal subgroup \( N \trianglelefteq G \) by a factor group \( Q = G/N \). As we will be working with different extensions with isomorphic factor groups, we shall describe these as extensions of \( Q \) with \( N \) to avoiding ambiguity.
A subgroup $U \leq A \times B$ of a direct product is a subdirect product of $A$ and $B$ if $U$ has surjective projections onto $A$ and $B$, respectively. In this case, [22] Lemma 1.1] shows that for $U_1 = U \cap A$ and $U_2 = U \cap B$ there is an isomorphism $\tau: A/U_1 \to B/U_2$, and $U$ is the preimage of the graph of $\tau$ under the projection $A \times B \to A/U_1 \times B/U_2$; in particular, $|U| = |A||U_2| = |B||U_1|$. 

For a module (or ring) $R$ and positive integer $n$ we denote by $R^n$ the direct sum (direct product) of $n$ copies of $R$. We say a module $R$ is $V$-homogeneous if $R$ is isomorphic to a direct sum of copies of a module $V$; unless stated otherwise, all modules are assumed to be finite-dimensional. A module is semisimple if it is a direct sum of simple modules (which do not need to be isomorphic). We write $R_{H,p}$ for the $p$-modular regular $H$ module, that is, $R_{H,p} \cong \mathbb{Z}_p H$ as $H$-modules. To avoid confusion with the unit $1 \in \mathbb{Z}$, we sometimes denote the identity in groups by $e$. The radical $\text{rad}(A)$ of an $H$-module $A$ is the intersection of all maximal submodules, and $\text{rad}(A) = 0$ if no such submodule exist; it is the smallest submodule such that $A/\text{rad}(A)$ is semisimple. The following is well-known, but we include proofs for convenience.

**Lemma 1.1.** Let $A$ and $B$ be $H$-modules; let $C \leq A$ be a submodule.

a) We have $\text{rad}(C) \leq \text{rad}(A)$ and $\text{rad}(A \oplus B) = \text{rad}(A) \oplus \text{rad}(B)$.

b) If $\sigma: A \to B$ is an $H$-module homomorphism, then $\sigma(\text{rad}(A)) \leq \text{rad}(B)$.

c) We have $\text{rad}(A/C) = (\text{rad}(A) + C)/C$, and $A/C$ is semisimple if and only if $\text{rad}(A) \leq C$.

**Proof.** 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, $\text{rad}(C) \leq C \cap D$, so $\text{rad}(C) \leq \text{rad}(A)$. This also implies $\text{rad}(A) \oplus \text{rad}(B) \leq \text{rad}(A \oplus B)$. Conversely, if $W < A$ and $V < B$ are maximal, then $W \oplus B$ and $A \oplus V$ are maximal in $A \oplus B$, so $\text{rad}(A \oplus B) \leq \text{rad}(A) \oplus \text{rad}(B)$.

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

c) As in a), the module $A/\text{rad}(A)$ embeds into a direct sum of simple modules, hence is semisimple. If $\text{rad}(A) \leq C$, then $A/C \cong (A/\text{rad}(A))/(C/\text{rad}(A))$ is a quotient of a semisimple module, hence semisimple. Conversely, if $A/C$ is semisimple, then $\text{rad}(A/C) = 0$ and so $\text{rad}(A) \leq C$.

To prove the first claim, let $E \leq A$ be the submodule with $E/C = \text{rad}(A/C)$. Applying b) to the projection $A \to A/C$ yields $(\text{rad}(A) + C)/C \leq \text{rad}(A/C)$, so $\text{rad}(A) + C \leq E$. On the other hand, $B = \text{rad}(A) + C$ is a submodule of $A$ such that $(A/C)/(B/C) \cong A/(C + \text{rad}(A))$ is semisimple. Thus, $\text{rad}(A/C) \leq B/C$. It follows that $E = \text{rad}(A) + C$, as claimed.

The following useful result is due to Gaschütz [8 Proposition 6.14].

**Lemma 1.2.** Let $N \leq H$ be a finite normal subgroup of an $e$-generated group $H$. If $H/N$ is generated by $\{h_1 N, \ldots, h_e N\}$, then there are $n_1, \ldots, n_e \in N$ with $H = \langle h_1 n_1, \ldots, h_e n_e \rangle$.

1.2. The structure of the regular module. We shall need, for a finite group $H$ and a finite field $K$, the $KH$-module structure of the regular module $M = KH$. The Krull-Schmidt Theorem [13 Theorem 1.6.6] shows that $M$ can be written (uniquely) as a direct sum of indecomposable modules. Collecting isomorphic summands, we have a decomposition

$$M = \bigoplus_{i=1}^n D_i^{r_i},$$
where each $D_i$ is a module that is indecomposable and projective (as direct summands of the free module). It follows from [13] Remark 1.6.22(a) and Theorem 1.6.24 that the factors $D_i/\text{rad}(D_i)$ are simple and mutually nonisomorphic, so $n$ is the number of isomorphism types of simple $KH$ modules. It follows from Lemma 1.1 that the semisimple module $M/\text{rad}(M)$ can be decomposed as

$$M/\text{rad}(M) = \bigoplus_{i=1}^{n} (D_i/\text{rad}(D_i))^{r_i}.$$  

It follows from [13] Theorem 1.6.20(b)] that the isomorphism type of $D_j$ is determined uniquely by the isomorphism type of its radical quotient $D_j/\text{rad}(D_j)$. If $K$ is algebraically closed, then the multiplicities satisfy $r_i = \dim D_i/\text{rad}(D_i)$, see [13] Theorem 1.6.24].

Following notation from [13] Definition 1.5.8], an extension field $K \supset K$ is a splitting field for a $K$-algebra $A$, if every simple $K$-module is absolutely simple. It follows from [13], Lemma 1.5.9] that if $\dim_K A < \infty$, then there exists a splitting field $K$ such that the extension $K > K$ has finite degree. This allows us to state the following theorem.

**Theorem 1.3.** Let $M = KH = \bigoplus_{i=1}^{n} D_i^{r_i}$ be the regular module of the finite group $H$ over the finite field $K$, and let $K$ be a finite degree splitting field for $KH$. If $V$ is a $KH$-module, we denote by $KV = K \otimes_K V$ the $KH$-module arising from $V$ by extending the scalar domain.

a) If $V$ is a simple $KH$-module, then $KV$ is a direct sum of nonisomorphic simple $KH$-modules.

b) We have $K\text{rad}(M) = \text{rad}(KH)$.

c) Each $r_i$ is the dimension of an absolutely simple constituent of $D_i/\text{rad}(D_i)$.

**Proof.** a) Since $K$ is a finite extension of a finite field $K$, the extension $K \supset K$ is a Galois extension. Now the claim follows from [13] Theorem 1.8.4]. More precisely, if $W$ is a simple $KH$-submodule of $KV$, then $KV$ is the direct sum of nonisomorphic Galois conjugates of $W$.

b) By a), if $S < M$ is a maximal submodule, then $K(M/S) \cong KKH/KS$ is semisimple, and thus $\text{rad}(KH) \leq K\text{rad}(M)$. Conversely, $KH/K\text{rad}(M) \cong K(M/\text{rad}(M))$ and $M/\text{rad}(M)$ is a direct sum of simple $KH$-modules; now a) shows that $K(M/\text{rad}(M))$ is a semisimple $KH$-module. This implies $\text{rad}(KH) \leq K\text{rad}(M)$. Thus, equality is established.

c) Let $D_i$ be an indecomposable direct summand of $KH$, and let $KD_i = C_1 \oplus \cdots \oplus C_k$ be a direct sum of $K$-projective indecomposables; note that the $C_j$ are direct summands of the regular module $KH$. In particular, the radical quotients $C_j/\text{rad}(C_j)$ are simple $KH$-modules and the isomorphism type of $C_j$ is determined uniquely by the isomorphism type of $C_j/\text{rad}(C_j)$. It follows from a,b) that the direct sum constituents of $K(D_i/\text{rad}(D_i))$ are the simple factors $C_j/\text{rad}(C_j)$, and hence they are mutually nonisomorphic. The multiplicity $r_i$ of $D_i$ as a direct summand of $KH$ therefore equals the multiplicity of $C_j$ as a direct summand of $KH$, which is the multiplicity of $C_j/\text{rad}(C_j)$ as a direct summand of $KH/\text{rad}(KH)$. By Wedderburn’s theorem this is equal to $\dim/K(C_j/\text{rad}(C_j))$, see [13] Remark 1.6.22(a) and Theorem 1.6.24].

2. The covering group $\hat{H}_{p,e}$ and the module $M_{H,p,e}$

Recall that $H$ is a finite $e$-generated group and $\psi: F \to H$ is an epimorphism from a free group of rank $e$; we identify $H = F/M$ where $M = \ker \psi$. Let $p$ be a prime and note that $M/M_p$ is an $H$-module where $g \in H$ acts via conjugation by any preimage under $\psi$; this is well-defined since $M$ acts trivially on $M/M_p$ by conjugation. The Nielsen-Schreier Theorem [17] (6.1.1) shows that
Theorem 2.1. Let $H$ be a finite $e$-generated group; let $p$ be a prime.

a) There is a finite $e$-generated group $\hat{H} = \hat{H}_{p,e}$ with the following properties: first, $\hat{H}$ has a normal elementary abelian $p$-subgroup $Z$ with $\hat{H}/Z \cong H$; second, if $L$ is an $e$-generated group such that $L/Y \cong H$ for some normal elementary abelian $p$-subgroup $Y$, then $L$ is a homomorphic image of $\hat{H}$.

b) If $H = F/M$ where $F$ is free of rank $e$, then one can define $\hat{H} = F/M_p$ and $Z = M/M_p$.

c) The isomorphism types of $\hat{H}$ and the $H$-module $Z$ depend only on $H$, $p$, and $e$.

Part c) of this theorem then justifies the following definition:

Definition 2.2. We call $\hat{H}_{p,e}$ the $p$-cover of $H$ of rank $e$; this group exists and is uniquely defined (up to isomorphism) whenever $H$ is a finite $e$-generated group.

The proof of Theorem 2.1 will be given below.

2.1. The module $\mathcal{M}_{H,p,e}$. The structure of the module $M/M_p$ has been described by Gaschütz [5], see also the book of Gruenberg [8] and papers [3, 6]. We recall the relevant definitions and results, starting with the fact that the structure of $F/M_p$ is independent from the choice of $\psi$:

Theorem 2.3. ([5] Satz 1) Let $F$ be free of rank $e$ and let $\psi: F \to H$ be an epimorphism onto a finite group $H$ with kernel $M$. The isomorphism class of the extension (see [17] Section 11.1) for a definition) defined by the short-exact sequence

$$1 \to M/M_p \to F/M_p \to H \to 1$$

depends on $p$, $e$, and $H$, but not on the choice of $\psi: F \to H$. Up to $H$-module isomorphism, the $H$-module

$$\mathcal{M}_{H,p,e} = M/M_p$$

depends on $p$, $e$, $H$, but not on $\psi: F \to H$.

The structure of $\mathcal{M}_{H,p,e}$ is closely related to that of the the regular module $R_{H,p} \cong \mathbb{Z}_p H$. As in Section [1,2] we decompose $R_{H,p}$ into a direct sum of indecomposable submodules, see also [1] pp. 96–111 and [5] p. 281, and we fix the following notation: We have

$$R_{H,p} \cong D_1^{r_1} \oplus \ldots \oplus D_t^{r_t}$$

such that each $D_i/\text{rad}(D_i) = E_i$ is a simple $\mathbb{Z}_p H$-module with $E_i \not\cong E_j$ and $D_i \not\cong D_j$ for $i \neq j$. The list $E_1, \ldots, E_t$ forms a complete set of representatives of simple $\mathbb{Z}_p H$-modules with $E_1 = 1$ (the 1-dimensional trivial module). By Theorem [1,3] each multiplicity is given by $r_i = \dim_{\mathbb{Z}_p} C_i$, where $C_i$ is an absolutely simple constituent of $E_i$ over the algebraic closure of $\mathbb{Z}_p$. 
We now define integers $s_1, \ldots, s_t$ and an $H$-module $\mathcal{B}_{H,e,p}$ as in \cite{5}: If $p$ divides $|H|$, then $\text{rad}(D_1) \neq 0$ and the $s_i$ are defined by
\[ \text{rad}(D_1)/\text{rad}(\text{rad}(D_1)) = E_1^{s_1} \oplus \ldots \oplus E_t^{s_t}; \]
note that $S = D_1^{s_1} \oplus \ldots \oplus D_t^{s_t}$ is the projective cover of $\text{rad}(D_1)$, cf. \cite{6} p. 256. We define $\mathcal{B}_{H,e,p}$ as the kernel of the natural projection $S \to \text{rad}(D_1)$. As shown in \cite{5} Satz 5' and \cite{6} p. 256–258, this kernel is unique up to isomorphism and does not contain a direct summand isomorphic to any $D_1, \ldots, D_t$. If $p \nmid |H|$, then $\mathcal{B}_{H,e,p} = 0$ and each $s_i = 0$. With this notation, we have the following:

**Theorem 2.4.** (\cite{5} Satz 2 & 3 & 5) Let $H$ be a finite $e$-generated group and let $p$ be a prime. The $\mathbb{Z}_p H$-modules $\mathcal{M}_{H,e,p}$ and $(R_{H,p})^{e-1} \oplus 1$ have the same multiset of simple composition factors. Furthermore, $\mathcal{M}_{H,e,p} \cong A_{H,e,p} \oplus \mathcal{B}_{H,e,p}$ as $H$-modules, where
\[ A_{H,e,p} = D_1^{e-1} \oplus D_2^{(e-1)r_2-s_2} \oplus \ldots \oplus D_t^{(e-1)r_t-s_t}. \]

Note that if $p \nmid |H|$, then $\mathcal{M}_{H,e,p} \cong (R_{H,p})^{e-1} \oplus 1$. An alternative characterisation of $A_{H,p,e}$ and $\mathcal{B}_{H,p,e}$ is given in \cite{5} Section 8. For this we recall some notation. Let $1 \to N \to W \xrightarrow\pi G \to 1$ be an extension of a group $G$ with a $G$-module $N$. The extension is split if there is a subgroup $U \leq W$ such that $\pi|_U: U \to G$ is an isomorphism; alternatively, the extension is split if there is a homomorphism $f: G \to W$ such that $\pi \circ f$ is the identity on $G$. Recall that the Frattini subgroup of $W$ is the intersection of all maximal subgroups of $W$; it is well-known that it consists of all nongenerators of $W$, see \cite{11} Proposition 2.44. The extension $W$ is a Frattini extension of $G$ if $N$ is contained in the Frattini subgroup of $W$. In \cite{5}, such an extension is called nicht-zerspaltend.

Let $\mathcal{U}$ be a split extension of $H$ that is maximal with respect to the properties that $\mathcal{U}$ is $e$-generated and the kernel of $\mathcal{U} \to H$ is an elementary abelian $p$-subgroup. Let $\mathcal{V}$ be a Frattini extension of $H$ that is maximal with respect to the property that the kernel of $\mathcal{V} \to H$ is $p$-elementary abelian; note that $\mathcal{V}$ is also $e$-generated. Thus, there exist epimorphisms from $F/M_p$ to $\mathcal{U}$ and to $\mathcal{V}$, respectively, that is, we have
\[ \mathcal{U} \cong (F/M_p)/B \quad \text{and} \quad \mathcal{V} \cong (F/M_p)/A \]
for some normal subgroups $A, B \leq F/M_p$.

**Theorem 2.5.** (\cite{5} Satz 6) As $H$-modules, $\mathcal{M}_{H,e,p} \cong A \oplus B$ with $A \cong A_{H,e,p}$ and $B \cong \mathcal{B}_{H,e,p}$.

Thus, up to isomorphism, $\hat{H}_{p,e}/\mathcal{B}_{H,e,p}$ is the largest $e$-generated split extension of $H$ with an elementary abelian $p$-group, and $\hat{H}_{p,e}/A_{H,e,p}$ is the largest Frattini extension of $H$ with an elementary abelian $p$-group, see also \cite{6} p. 256; here “largest” means that any other such extension is an epimorphic image. The module $\mathcal{B}_{H,e,p}$ has also been studied in \cite{3} \cite{6}: a simple $\mathbb{Z}_p H$-module $V$ is a direct factor of $\mathcal{B}_{H,e,p}/\text{rad}(\mathcal{B}_{H,e,p})$ if and only if $H^2(H,V) \neq 0$, see \cite{6} p. 256.

We conclude this section with a proof of Theorem 2.1:

\footnote{Following \cite{5}, the extension is zerspaltend if there is a proper subgroup $U < W$ such that $\pi(U) = G$; it is nicht-zerspaltend if every subgroup $U \leq W$ with $\pi(U) = G$ satisfies $U = W$. It follows that $W$ is nicht-zerspaltend if and only if the elements in $N$ are all nongenerators, if and only if $W$ is a Frattini extension: If $W$ is nicht-zerspaltend and $\langle X, N \rangle = W$ for some $X \subseteq W$, then $\langle X \rangle$ maps onto $G$, hence $\langle X \rangle = W$ by assumption; this shows that $N$ consists of nongenerators. Conversely, if $N$ consists of nongenerators and $U \leq W$ maps onto $G$, then $\langle U, N \rangle = W$; by assumption, $\langle U \rangle = \langle U, N \rangle = W$, so $W$ is nicht-zerspaltend.}
Proof of Theorem 2.1 a+b) Recall that $\psi : F \to H$ has kernel $M$. As in the theorem, let $\tau : L \to H$ be an epimorphism with $p$-elementary abelian kernel $Y$. By Lemma 1.2 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 $\psi$ through $L$, that is, there is a homomorphism $\beta : F \to L$ such that $\tau \circ \beta = \psi$. Since $\beta(M) \leq \ker \tau = Y$ is $p$-elementary abelian, we have $\beta(M_p) = \beta(M'M(p)) = 1$. Thus, if we define $\hat{H} = F/M_p$, then $\beta$ induces an epimorphism from $\hat{H}$ to $L$, as required. Clearly, $Z = M/M_p$ is a normal elementary abelian $p$-subgroup of $\hat{H}$ with quotient $H$. By the Nielsen-Schreier Theorem, $Z$ has rank $1 + (e - 1)|H|$, which proves that $\hat{H}$ is finite.

c) Suppose $H = F/M$ and let $\hat{H} = F/M_p$ with kernel $Z = M/M_p$ as in a). Let $K$ be an $e$-generated group with the same properties as stipulated for $\hat{H}$. By assumption, there exist epimorphisms $\hat{H} \to K$ and $K \to \hat{H}$; since both groups are finite, $\hat{H} \cong K$ follows. If $U$ is the kernel of the projection $K \to H$, then $U$ is isomorphic to $Z$ as $H$-module. It follows from Theorem 2.3 that the $\hat{H}$-module structure on $Z$ depends only on $H$, $p$, and $e$; the claim follows. $\square$

3. The covering group via Fox derivatives

Throughout this section, let $H$ be a finite $e$-generated group. Let $F$ be free on $X = \{x_1, \ldots, x_e\}$, and choose an epimorphism $\psi : F \to H$ with kernel $M$; we identify $H = F/M$ and let $\psi$ be the natural projection. The definition of the cover $\hat{H} = F/M_p$ offers in principle a way of constructing a finitely presented group. However, the large rank of the module $M_{H,e,p} = M/M_p$ makes this infeasible in all but the smallest examples. We thus shall explore a different way of describing an isomorphic group: The aim of this section is to describe $\hat{H}$ and $M_{H,e,p}$ via so-called Fox derivatives and a wreath product construction. Since we work with group rings, such as $\mathbb{Z}F$, we denote the identity in $F$ (and in its quotient groups) by $e$ to avoid confusion with the unit $1 \in \mathbb{Z}$.

3.1. Fox derivatives. We first recall some results from [12, Section 11.4]. The Fox derivative of $x \in X$ is defined as the unique map
\[
\hat{\partial} : F \to \mathbb{Z}F
\]
that satisfies the Leibniz’ rule
\[
\hat{\partial}(uv) = (\hat{\partial}u)v + u\hat{\partial}v
\]
for all $u, v \in F$ and that maps $x \in X$ to $e$ and every other generator to $0$. The Fox derivative can be extended linearly to $\mathbb{Z}F$; by abuse of notation, we call it $\hat{\partial}$ as well.

Remark 3.1. The Leibniz’ rule yields that
\[
\frac{\partial x}{\partial x} = 0 \quad \text{and} \quad \frac{\partial(s^{-1})}{\partial x} = -\frac{\partial s}{\partial x}s^{-1}.
\]
The image of $w \in F$ under $\hat{\partial}$ 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 $\hat{\partial}(w) = bx^{-1}c - x^{-1}c$.

By abuse of notation, we identify the projection $\hat{\psi} : F \to H$ with the induced homomorphism
\[
\hat{\psi} : (\mathbb{Z}F)^e \to (\mathbb{Z}H)^e,
\]
and combine the Fox derivatives to a map
\[
\hat{\partial} : F \to (\mathbb{Z}F)^e, \quad w \mapsto (\hat{\partial}w_{\partial x_1}, \ldots, \hat{\partial}w_{\partial x_e}).
\]
The next lemma describes the kernel of the composition $\psi \circ \partial : F \to (\mathbb{Z}H)^e$.

**Lemma 3.2.** ([12] Proposition 5) If $v \in F$, then $\psi \circ \partial(v) = 0$ if and only if $v \in M'$.

### 3.2. A wreath product construction.

Recall that $|H| = m$, and consider the wreath product

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

where the $m$ copies of $\mathbb{Z}$ in $\mathbb{Z}^m$ are labelled by the elements of $H$. As $H$-modules, we have $\mathbb{Z}^m \cong R_{H,p}$, the regular $H$-module. We write $0 = (0,\ldots,0) \in \mathbb{Z}^m$ and, if $h \in H$ and $z \in \mathbb{Z}$, then

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

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

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

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

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

We now prove that $\psi_i$ is closely related to the Fox derivative $\frac{\partial}{\partial x_j}$. For this we need to identify $\mathbb{Z}H$ with $\mathbb{Z}^m$ via the additive isomorphism $\alpha : \mathbb{Z}H \to \mathbb{Z}^m$ that maps each $g \in H$ to $1(g) \in \mathbb{Z}^m$; this allows us to define $\zeta = \alpha \circ \psi : \mathbb{Z}F \to \mathbb{Z}^m$.

**Proposition 3.3.** If $i \in \{1,\ldots,e\}$ and $w \in F$, then

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

**Proof.** For simplicity, write $\tau = \psi_i$ and $x = x_i$. Write $w = w_1x_1w_2x_2\ldots w_kx^k_wk+1$ where each $w_j \in F$ is reduced and does not contain $x^\pm$. We prove the claim by induction on $k$. If $k = 0$, then $w = w_1$ and $\tau(w) = (\psi(w), 0) = (\psi(w), \frac{\partial w}{\partial x_i})$.

For $k = 1$ we have $w = w_1x^1w_2$, which requires a case distinction: if $\varepsilon_1 = 1$, then

$$\tau(w) = (\psi(w_1), 0) \cdot (\psi(x), 1(\epsilon)) \cdot (\psi(w_2), 0) = (\psi(w_1), 1(\psi(w_2))) = (\psi(w), \zeta(\frac{\partial w}{\partial x_i}));$$

if $\varepsilon = -1$, then

$$\tau(w) = (\psi(w_1), 0) \cdot (\psi(x), 1(\epsilon)) \cdot (\psi(w_2), 0) = (\psi(w), -1(\psi(x)^{-1})) \cdot (\psi(w_2), 0)$$

$$= (\psi(w), 1(\psi(x^{-1}w_2)))$$

$$= (\psi(w), \zeta(\frac{\partial w}{\partial x_i})).$$

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

$$\tau(w) = \tau(w')\tau(x^kw_{k+1}) = (\psi(w'), \zeta(\frac{\partial w'}{\partial x_i})) \cdot (\psi(x^kw_{k+1}), \zeta(\frac{\partial x^kw_{k+1}}{\partial x_i})) = (\psi(w), \frac{\partial w}{\partial x_i}),$$

where the last equation follows from the observations in Remark 3.1. 

□
We use $\psi_1, \ldots, \psi_e$ to define the homomorphism
\[
\Psi = \psi_1 \times \ldots \times \psi_e : F \to W^e.
\]

For a prime $p$ let $W(p) = H \times \mathbb{Z}_p^{\times}$ be the modular version of $W$, and define
\[
\Psi_p : F \overset{\Psi}{\rightarrow} W^e \rightarrow W(p)
\]
where the last map is induced by the natural projection $\mathbb{Z} \to \mathbb{Z}_p$. The next theorem shows that $\Psi_p$ can be used to construct the $p$-cover $\hat{H} = \hat{H}_{p,e}$ of $H$ of rank $e$ and the $H$-module $\mathcal{M}_{H,e,p}$.

**Theorem 3.4.** With the previous notation, 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 $\Psi_p(F)$.

c) The $H$-modules $\mathcal{M}_{H,e,p}$ and $\Psi_p(M)$ are isomorphic.

**Proof.**

a) By Proposition 3.3 we have $w \in \ker \Psi$ if and only if $\psi(w) = e$ and $\zeta(\frac{2w}{\ell \epsilon_i}) = 0$ for every $i$, if and only if $w \in M$ and $\psi(w) = 0$ for every $i$, if and only if $w \in M$ and $\psi \circ \vartheta(w) = 0$, if and only if $w \in M'$, see Lemma 3.2. It follows from this that $M/M' \cong \Psi(M) \leq \mathbb{Z}_p^{me}$, in particular, $\Psi_p$ induces a map $M/M' \to \mathbb{Z}_p^{me} \to \mathbb{Z}_p^{me}$ 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 2.1 that $\Psi_p(F) \cong F/M_p \cong \hat{H}_{p,e}$.

c) By the isomorphism theorem, $\Psi_p$ yields an isomorphism $\alpha : M/M_p \to \Psi_p(M), rM_p \mapsto \Psi_p(r)$. Let $r \in M$, write $g \in H = F/M$ as $g = fM$, and note $(rM_p)^g = r^fM_p$. Since $\Psi_p(M) \leq \mathbb{Z}_p^{me} \leq W^e$ is abelian, $\Psi_p(f)$ acts on $\Psi_p(M)$ via conjugation by $\psi(f) = g$. Now $\alpha((rM_p)^g) = \Psi_p(r^f) = \Psi_p(r)^{\Psi_p(f)} = \Psi_p(f)^{\psi(f)} = \Psi_p(f)^g$ shows that $\alpha$ is an $H$-module isomorphism. \hfill \Box

### 4. A Reduction to Homogeneous Modules

We continue with the previous notation. Since the rank of the module $\mathcal{M} = \mathcal{M}_{H,p,e}$ is too large for practical applications, we would like to replace it by a smaller module. This is not a restriction since any finite extension of $H$ could be constructed iteratively by forming extensions with simple modules. Any such extension, considered as factor of $\hat{H} = \hat{H}_{p,e}$, will have a kernel containing $\text{rad}(\mathcal{M})$. The semisimple quotient $\mathcal{M}/\text{rad}(\mathcal{M})$ is the direct sum of homogeneous modules, and so $\hat{H}_{p,e}/\text{rad}(\mathcal{M})$ is the subdirect product of extensions of $H$ with these homogeneous summands. This motivates the following definition:

**Definition 4.1.** For a finite-dimensional $\mathbb{Z}_pH$-module $A$ and a simple $\mathbb{Z}_pH$-module $V$ let $V(A)$ be the smallest submodule of $A$ such that $A/V(A)$ is $V$-homogeneous.

An explicit construction follows with Lemma 1.1. Since $A/V(A)$ is semisimple, we must have $\text{rad}(A) \leq V(A)$; note that $A/\text{rad}(A) = \bigoplus B_i$ is a direct sum of simple modules and its unique $V$-homogeneous direct summand is the direct sum of all $B_i \cong V$. It follows that $V(A)$ can be constructed as the full preimage of all $B_i \not\cong V$ under the projection $A \to A/\text{rad}(A)$.
Definition 4.2. Let $V$ be a simple $\mathbb{Z}_p H$-module. The $(V, e)$-cover of $H$ is
\[ \hat{H}_{V,e} = \hat{H}_{p,e}/V(\mathcal{M}_{H,p,e}); \]
it is the largest $e$-generated group that maps onto $H$ with $V$-homogeneous kernel.

Recall from Section 2.1 that $\mathcal{M} \cong \mathcal{A}_{H,e,p} \oplus \mathcal{B}_{H,e,p}$ such that $\hat{H}/\mathcal{B}_{H,e,p}$ is the largest split extension and $\hat{H}/\mathcal{A}_{H,e,p}$ is nonsplit. We shall therefore describe a construction of $\hat{H}_{V,e}$ as a subdirect product of a split and a nonsplit extension. In the remainder of this section we consider the split part; the nonsplit part will be discussed in Section 5.

Remark 4.3. 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 [11, Section 9.4] for proofs and background information. If $H$ has rank $e$ (that is, every minimal generating set of $G$ has size $e$), then its $p$-cover is an $e$-generated finite $p$-group $H^*$ such that $H^*/N \cong H$ for some central abelian normal subgroup $N$, and such that every $e$-generated $p$-group $L$ with $L/Y \cong H$ for some central abelian $Y \leq L$ is a homomorphic image of $H^*$, see [11, Theorem 9.18]. The group $H^*$ is unique up to isomorphism; if $H = F/M$ with $F$ a free group of rank $e$, then one can define $H^* = F/M^{(p)}[F, M]$; in particular, $H^*$ is a quotient of $\hat{H}_{p,e}$. Since $N$ is the direct sum of copies of the 1-dimensional trivial $\mathbb{Z}_p H$-module 1, it follows that $H^* \cong \hat{H}_{1, \text{rank}(H)}$.

4.1. A wreath product construction for the split case. We reconsider the homomorphism
\[ \psi_p = \psi_1 \times \ldots \times \psi_e : F \rightarrow (H \rtimes R_{H,p})^e \]
of Section 3.2, recall that
\[ \hat{H} = \Psi_p(F) \quad \text{and} \quad \mathcal{M} = \Psi_p(M). \]
Each $\psi_j : F \rightarrow H \rtimes R_{H,p}$ maps the generator $x_k \in X$ to $(\psi(x_k), 0)$ if $k \neq j$, and to $(\psi(x_j); 1)$ if $k = j$; here $1 = 1(e)$ is a generator of the cyclic $H$-module $R_{H,p} \cong \mathbb{Z}_p H$. Let $V$ be a simple $\mathbb{Z}_p H$-module and let $U = V(R_{H,p})$ be as in Definition 4.1. By Section 2.1 we have
\[ R_{H,p} = D_1^{r_1} \oplus \ldots \oplus D_t^{r_t}, \]
and there is a unique index $i$ such that
\[ D_i/\text{rad}(D_i) \cong V; \]
we fix $i$ and set $r = r_i$. Note that $R_{H,p}/U \cong V^r$ is the largest $V$-homogeneous quotient of $R_{H,p}$.

Composing $\psi_j$ with the projection $R_{H,p} \rightarrow V^r$, we get a homomorphism $\psi_{V,j} : F \rightarrow H \rtimes V^r$ that maps $x_k$ to $(\psi(x_k), 0)$ if $k \neq j$, and to $(\psi(x_j); 1 + U)$ if $k = j$; here $1 + U$ is a generator of the cyclic module $V^r = R_{H,p}/U$. We use these maps to define
\[ \Psi_{V,e} = \psi_{V,1} \times \ldots \times \psi_{V,e} : F \rightarrow (H \rtimes V^r)^e. \]
We now prove that the image $\Psi_{V,e}(F)$ exposes the split part of $\hat{H}_{V,e}$. For this, recall from Theorem 2.4 that $M/M_p \cong \mathcal{M} = \mathcal{A}_{H,p,e} \oplus \mathcal{B}_{H,p,e} \leq R_{H,p}^e \leq (H \rtimes R_{H,p})^e$ with
\[ \mathcal{A}_{H,p,e} = D_1^{e-s_1} \oplus D_2^{(e-1)r_2-s_2} \oplus \ldots \oplus D_t^{(e-1)r_t-s_t}. \]

Proposition 4.4. The group $\Psi_{V,e}(F)$ is a quotient of $\hat{H}$ that maps onto $H$ with $V$-homogeneous kernel $\Psi_{V,e}(M)$. If $E$ is any quotient of $\hat{H}$ with these properties such that $E$ is a split extension of $H$ with this kernel, then the projection $\hat{H} \rightarrow E$ factors through $\Psi_{V,e}(F)$. 

PROOF. We abbreviate $T = \Psi_{V,e}(F)$ and let $\pi: T \to H$ be the natural epimorphism. Write $W = H \rtimes R_{H,p}$ so that $\Psi_p: F \to W^e$ and we can identify $\hat{H} = \Psi_p(F)$ as a subgroup of $W^e$, see Theorem [3.4]. Recall that $U = V(R_{H,p})$, so $U^e \leq (R_{H,p})^e \leq W^e$, where all inclusions are the natural ones. Since $U \leq W$, we have $U^e \leq W^e$, and so the natural projection induces a homomorphism $\nu: \hat{H} \to W^e/U^e$. It follows that $\Psi_{V,e} = \nu \circ \Psi_p$ and the natural projection $\hat{H} \to H$ is $\nu \circ \pi$. Note that $\psi = \pi \circ \nu \circ \Psi_p$ has kernel $M$, which shows that

$$\ker \pi = \nu(\Psi_p(M)) = \Psi_{V,e}(M);$$

by construction, $\Psi_{V,e}(M) \leq V^{re}$, so $\ker \pi$ is $V$-homogeneous.

By Section [2.1] the group $K = \hat{H}/B_{H,p,e}$ is the largest finite $e$-generated split extension of $H$. It follows that the largest finite $e$-generated split extension of $H$ with a $V$-homogeneous module is $K/R$ where $R = V(M/B_{H,p,e})$. Note that $R = W/B_{H,p,e}$ with $W = B_{H,p,e} \oplus V(A_{H,p,e})$ and the epimorphism $K/R \to H$ has kernel isomorphic to $V^f$ where $f$ the multiplicity of $D_i$ in $A_{H,p,e}$, see Theorem [2.4]; recall that $D_i/\ker(D_i) \cong V$. Since every finite $e$-generated split extension of $H$ with a $V$-homogeneous module is a quotient of $K/R$, it is therefore sufficient to show that $K/R$ is a quotient of $T$. To prove the latter, it is sufficient to show that $\nu(A_{H,p,e}) \cong V^f$.

Recall that we identify $A_{H,p,e} \leq M \leq \hat{H} = \Psi_p(F)$ and $A \leq A_{H,p,e}$ be the direct summand of $A_{H,p,e}$ of the form $D_i^f$ and recall that $A \leq (R_{H,p})^e \leq W^e$. Since $D_i$ is projective, $A \cong D_i^f$ is projective as well, cf. [13] Definition 1.6.15]. Now [13] Example 1.1.46 and Theorem 1.6.27(d) show that $A$ is injective and a direct summand of $(R_{H,p})^e$. Without loss of generality, we can therefore assume that $A$ is part of the direct sum decomposition of $(R_{H,p})^e$. This implies that $\nu(A_{H,p,e}) = \nu(A) = V^f$, as claimed. \qed

4.2. A practical construction of $\Psi_{V,e}(F)$. Here we describe how to construct $\Psi_{V,e}(F)$ immediately from $H$ and a simple $\mathbb{Z}_pH$-module $V$, without going via the large module $M$. We denote the dimension of $V$ by $s$ and the multiplicity of $V$ in the radical factor of $R_{H,p}$ by $r$. By Theorem [1.3], this multiplicity is the dimension of an absolutely simple constituent $W$ of $V$ and a divisor of $s$.

As shown above, 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 $H \rtimes V^r$ and homomorphisms

$$\psi_j^e: F \to H \rtimes V^r$$

that map $x_j$ to $(\psi(x_j), z)$ and $x_k \neq x_j$ to $(\psi(x_k), 0)$. Setting $\Psi_p^e = \psi_1^e \times \ldots \times \psi_r^e: F \to (H \rtimes V^r)^e$, it is obvious that its image satisfies

$$\Psi_p^e(F) \cong \Psi_{V,e}(F).$$

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

Recall that here we have $K = \mathbb{Z}_p$. As in Theorem [1.3], let $\mathbf{K}$ be a splitting field for $KH$ and let $W$ be an absolute simple $\mathbf{K}H$-module that is a direct summand of $\mathbf{K}V$; let $\nu: \mathbf{K}V \to W$ 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 a $\mathbf{K}$-basis of $W$. Since the images of the standard $\mathbf{K}$-basis of $V$ span $W$ as a $\mathbf{K}$-vector space, we can take $w_1, \ldots, w_r$ as a subset of such a standard basis. Since $W$ is absolutely simple, it follows from [13] Corollary 1.3.7 that $\mathbf{K}H$ acts as full matrix algebra on $W$. That means that we can find elements $a_i \in \mathbf{K}H$, such that $\nu(w_i)a_j = \delta_{i,j}\nu(w_i)$, where $\delta_{i,j}$
is the Kronecker-delta. We now consider $W^r$ as a quotient of $(KV)^r$ and let $KH$ act diagonally. For $w \in W$, denote by $[w]_i$ this vector in the $i$-th component of $W^r$, and define

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

By the definition of $a_i$, we have $z^{a_i} = [\nu(w_i)]$. Since $W$ is simple, each $\nu(w_i)$ generates $W$ as $KH$-module; this shows that $z$ generates $W^r$ as $KH$ module. Since $V$ is a simple $KH$-module, this implies that the pre-image $[w_1]_1 + \cdots + [w_r]_r \in V^r$ of $z$ generates $V^r$ as $KH$-module.

5. Construction of the cover $\hat{H}_{V,e}$

We use the previous notation, that is, $H = F/M$ is finite and $e$-generated, and $V$ is a simple $\mathbb{Z}_pH$ module. As before, let $\hat{H} = \hat{H}_{p,e}$ be the covering group, let $M = M_{H,p,e} = M/M_p$ be the representation module, and let $\hat{H}_{V,e} = \hat{H}/V(M)$ the largest $e$-generated group that maps onto $H$ with $V$-homogeneous kernel. Because that kernel is $V$-homogeneous, $\hat{H}_{V,e}$ will be a subdirect product of individual extensions of $H$ with $V$. Furthermore, as seen in Section 4, we know that $\Psi_{V,e}(F)$ is a quotient of $\hat{H}_{V,e}$ through which all finite $e$-generated split extensions factor. Thus, $\hat{H}_{V,e}$ can be constructed as subdirect product of $\Psi_{V,e}(F)$ with nonsplit extensions. Such extensions only exist if $p \mid |H|$, which we shall assume from now on.

To fix notation, we recall the basic setup of extension theory [17, Section 11]. Every extension of $H$ with an $H$-module $V$ is isomorphic to a group $E_\gamma$ with underlying set $H \times V$ and multiplication

$$ (g, v) \cdot (h, w) = (gh, v^h w^\gamma(g, h)) \tag{5.1}$$

for a 2-cocycle $\gamma \in Z^2(H, V)$. We call $E_\gamma$ the extension corresponding to $\gamma$ and call the map

$$\varepsilon_\gamma : E_\gamma \rightarrow H, \quad (h, v) \mapsto h,$$

its natural epimorphism. Nonsplit extensions correspond to cocycles in $Z^2(H, V)$ that lie outside the subgroup of 2-coboundaries $B^2(H, V)$. We first show that it is sufficient to only take extensions corresponding to representatives of a basis for the second cohomology group $H^2(H, V) = Z^2(H, V)/B^2(H, V)$. For this we need a technical lemma; note that here we write $V$ multiplicatively, but we consider $Z^2(H, V)$ and $H^2(H, V)$ as additive groups.

**Lemma 5.1.** Let $H$ be a finite group and let $V$ be a simple $\mathbb{Z}_pH$-module. Consider extensions $E_\beta$ and $E_\gamma$ with $\beta, \gamma \in Z^2(H, V)$, and natural epimorphisms $\varepsilon_\beta$ and $\varepsilon_\gamma$, respectively.

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

b) The same statement as in a) holds for $\zeta = \beta + r\gamma$ for any $r \in \mathbb{Z}_p$.

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

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

$$(a, v, w) \cdot (b, x, y) = (ab, v^h x^\beta(a, b), w^h y^\gamma(a, b))$$
and natural projections \( \tau : S \to E_\beta, (a, v, w) \mapsto (a, v) \), and \( \sigma : S \to E_\gamma, (a, v, w) \mapsto (a, w) \). Let
\[
K = (\ker \tau)(\ker \sigma) = 1 \times V \times V \quad \text{and} \quad N = \{(1, v, v^{-1}) : v \in V\} \leq K;
\]
note that \( N, K \leq S \) and \( K/N \cong V \) as \( H \)-modules. Now consider the natural homomorphism \( \nu : S \to S/N \); note that every element in \( S/N \) has the form \((a, v, 1)N\), and \( \nu \) maps \((a, v, w)\) to \((a, vw, 1)N\). In particular, the multiplication in \( S/N \) 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 \( S/N \cong E_\zeta \) where \( \zeta = \beta + \gamma \). By abuse of notation, we consider the epimorphism \( \nu : S \to E_\zeta, (a, v, w) \mapsto (a, vw) \). Since the homomorphism \( \tau \times \nu : S \to E_\beta \times E_\zeta \) is injective, the claim follows.

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

c) Write \( A = \ker \pi \) and let \( A \leq B \leq D \) such that \( D/A \cong E_\beta \) and \( D/B \cong H \). As done in a), we identify \( S \) with the Cartesian product \( H \times B \times V \) and note that
\[
\hat{D} = \{(h, b, 1) : h \in H, b \in B\} \cong D \quad \text{and} \quad \hat{E}_\gamma = \{(h, 1, v) : h \in H, v \in V\} \cong E_\gamma,
\]
with corresponding natural projections \( \pi_{\hat{D}} : S \to \hat{D}, (h, b, v) \mapsto (h, b, 1) \), and \( \pi_{\hat{E}_\gamma} : S \to \hat{E}_\gamma, (h, b, v) \mapsto (h, 1, v) \). Note that \( L = \{(1, a, 1) : a \in A\} \) is normal in \( \hat{D} \) and \( \hat{D}/L \cong E_\beta \). In particular, \( L \leq S \), and \( S/L \) is isomorphic to the subdirect product of \( E_\beta \) and \( E_\gamma \) defined by identifying the common quotient \( H \). By b), there exists a normal subgroup \( N/L \leq S/L \) such that \((S/L)/(N/L) \cong S/N \cong E_\zeta \) and such that \( S/L \) is isomorphic to the subdirect product of \( E_\zeta \) and \( E_\beta \) defined by identifying the common quotient \( H \). Let \( \pi_N : S \to S/N \) be the natural projection. It also follows from b) that \( \ker \pi_N = N \) and \( \ker \pi_{\hat{D}} = \{(1, 1, v) : v \in V \} \) intersect trivially, so \( \pi_N \times \pi_{\hat{D}} : S \to S/N \times \hat{D} \) is injective. Since \( S/N \cong E_\zeta \) and \( \hat{D} \cong D \), the claim follows. \( \square \)

**Theorem 5.2.** Let \( H \) be a finite \( e \)-generated finite group, let \( F \) be the free group on \( \{x_1, \ldots, x_e\} \), and let \( \psi : F \to H \) be the epimorphism with kernel \( M \). Let \( V \) be a simple \( \mathbb{Z}_p \)-module and let \( \gamma_1, \ldots, \gamma_d \in \text{Z}^2(H, V) \) be representatives for a basis of \( H^2(H, V) \). For each \( i \), let the homomorphism \( \phi_i : F \to E_{\gamma_i} \) be defined by \( x_j \mapsto (\psi(x_j), 1) \). Using \( \Psi_{V, e}(F) \) from Section 4, we define
\[
D = E_{\gamma_1} \times \cdots \times E_{\gamma_d}
\]
and \( \rho : F \to D, f \mapsto (\Psi_{V, e}(f), \phi_1(f), \phi_2(f), \ldots, \phi_e(f)) \). Then \( \rho(F) = \hat{H}_{V, e} \) is the largest quotient of \( \hat{H} \) that maps onto \( H \) with \( V \)-homogeneous kernel.

**Proof.** In this proof, write \( E_i = E_{\gamma_i} \) and \( h_i = \psi(x_i) \) for each \( i \). Since \( \gamma_i \notin B^2(H, V) \), each extension \( E_i \) is nonsplit; since \( V \) is a simple \( \mathbb{Z}_p \)-module, it follows that each \( \phi_i \) is surjective. By construction, \( \rho(F) \) is \( e \)-generated and an extension of \( H \) with a \( V \)-homogeneous module \( \rho(M) \leq \Psi_{V, e}(M) \times V^d \), see Proposition 4.4. This implies that \( \rho \) factors through \( \hat{H}_{V, e} \); let \( \nu : \hat{H}_{V, e} \to \rho(F) \) the corresponding epimorphism. To prove the theorem, it is sufficient to show that \( \nu \) is injective.

Suppose, for a contradiction, that \( \nu \) is not injective. In this case \( \hat{H}_{V, e} \neq \rho(F) \), so there is a finite \( e \)-generated extension \( E \) of \( H \) with a \( V \)-homogeneous module \( W \) such that the map \( F \to E \) factors through \( \hat{H}_{V, e} \), but \( E \) is not an image of \( \rho(F) \). Since \( \Psi_{V, e}(F) \) is a quotient of \( \rho(F) \), it follows from Proposition 4.4 that \( \hat{E} \) is a nonsplit extension.
Suppose that $G$ and we want to find certain larger quotients $H$ of $G$ that map onto $H$ with elementary abelian kernel. We assume that $G$ is a finitely presented group and that $H$ is finite; moreover $G$ and $H$ are both $e$-generated. The following simplification is useful: Since $G$ is finitely presented, we can suppose that $G = F/N$ for some free group $F$ of rank $e$. If $M$ is the normal subgroup of $F$ with $M/N = \ker \varphi$, then there is an isomorphism $\beta: F/M \to H$, $fM \mapsto \varphi(fN)$. Replacing $H$ by its isomorphic copy $F/M$, we can assume that $H = F/M$ and $\varphi: G \to H$, $fN \mapsto fM$, is the natural projection. Maps onto the original group can then be obtained via the isomorphism $\beta$.

We first show that the extensions $\hat{H}$ can also be computed via a suitable covering group.
Proposition 6.1. Let $G$ be an $e$-generated group with epimorphism $\varphi: G \to H$ onto a finite group. There is a unique largest quotient $H_{\varphi,p,e}$ of $G$ with the properties that $\varphi$ factors through $H_{\varphi,p,e}$ and that $H_{\varphi,p,e}$ maps onto $H$ with $p$-elementary abelian kernel. If $G = F/N$ and $H = F/M$ with $\ker \varphi = M/N$, then $H_{\varphi,p,e} = F/NM_p$. In particular, the isomorphism type of $H_{\varphi,p,e}$ is independent of the choice of epimorphism $\varphi$.

Proof. As explained above, we can assume that $G = F/N$ and $H = F/M$ such that $\varphi: G \to H$ is the natural projection. Let $H_{\varphi,p,e} = F/NM_p$. Clearly, this group is a quotient of $G$ that maps onto $H$ with $p$-elementary abelian kernel $MN/NM_p \cong M/M_p(N \cap M_p)$; we also have that $\varphi$ factors through $H_{\varphi,p,e}$. Now consider a group $K$ that also satisfies these properties; we show that $K$ is a quotient of $H_{\varphi,p,e}$, which proves the proposition. By assumption, we have projections

$$F \xrightarrow{\pi} G \xrightarrow{\varphi} H$$

such that $\alpha \circ \pi = \varphi$ with $\ker \tau = N$ and $\ker \varphi = M/N = \tau(M)$. This shows that $\tau(M) = \pi^{-1}(\ker \alpha)$, where $\pi^{-1}$ means taking full preimages under $\pi$. Writing $D = \tau^{-1}(\ker \pi)$, the isomorphism theorem implies that

$$\ker \alpha \cong \pi^{-1}(\ker \alpha)/\ker \pi \cong \tau(M)/\tau(D) \cong (M/\ker \tau)/(D/\ker \tau) \cong M/D.$$  

Since $\ker \alpha$ is $p$-elementary abelian, it follows that $M_p \leq D$. By construction, $N = \ker \tau \leq D$, so $NM_p \leq D$. Finally, observe that $F/D \cong K$: this follows since $K \cong F/\ker(\pi \circ \tau)$ and $\ker(\pi \circ \tau) = \tau^{-1}(\ker \pi) = D$. This proves that $K$ is a quotient of $H_{\varphi,p,e}$, as required. \hfill \square

Definition 6.2. Given $\varphi: G \to H$ as in Proposition 6.1, we call $H_{\varphi,p,e}$ the $(G,p)$-cover of $H$ of rank $e$; this group exists and is uniquely defined whenever $H$ is a finite $e$-generated group.

With the notation of Proposition 6.1, the group $U = M/NM_p$ is the largest $\mathbb{Z}_pG$-module by which $H = F/M$ can be extended such that the resulting group is a quotient of $G = F/N$.

We now discuss a reduction to $V$-homogeneous modules. One way to obtain the set of simple modules for a finite group $H$ is to start with the constituents of some faithful representation (for example, a permutation representation) and to form tensor products of the constituents, adding new (not isomorphic) simple constituents to the pool for forming tensor products; by the Burnside-Brauer theorem, this will produce representatives of all classes of irreducible representations; we refer to [11] Section 7.5.5 for more details and references.

Lemma 6.3. Let $G = F/N$ and $H = F/M$ as above. Let $V$ be a simple $\mathbb{Z}_pH$-module, and let $U \leq F$ such that $U/M_p = V(M/M_p)$ as in Definition 4.7. Then $\tilde{H} = F/NU$ is the largest quotient of $G$ such that the kernel of the epimorphism from $\tilde{H} \to H$ is $V$-homogeneous.

Proof. Clearly, $\tilde{H}$ is a quotient of $G$, and the epimorphism from $\tilde{H} \to H$ has kernel $K = M/UN$. Note that $K$ is $p$-elementary abelian since $M_p \leq U$. By Proposition 6.1, the group $M/NM_p$ is the largest quotient of $M/M_p$ by which $H$ can be extended such that the resulting group is a quotient of $G$. Moreover, $M/U$ is the largest $V$-homogeneous quotient of $M/M_p$. It follows that $M/NU$ is the largest $\mathbb{Z}_pH$-module by which $H$ can be extended such that the extension is a quotient of $G$. \hfill \square
7. Computing Cohomology via Rewriting Systems

To make the construction of $\hat{H}_{V,e}$ as in Theorem 5.2 concrete and effective, we need to be able to calculate 2-cohomology groups and extensions for the finite group $H$. The purpose of this section is to describe a way of doing so.

In this section, as before, let $H$ be a finite group with $e$ generators $\{h_1, \ldots, h_e\}$, and let $V$ be a $d$-dimensional $\mathbb{Z}_p H$-module with $\mathbb{Z}_p$-basis $\{v_1, \ldots, v_d\}$. If $H$ is given by a polycyclic presentation, then the group of 2-cocycles $Z^2(H, V)$ can be computed by using tails and consistency checks, see [11] Section 8.7.2 for details: first, one adds the generators of $V$ and the $H$-module relations to the presentation of $H$; then one appends to each polycyclic relation of $H$ an indeterminate (tail) in $V$; finally, one performs consistency checks which yield sufficient and necessary conditions on the tails for the new group to be an extension of $H$ with $V$. The set of all those tails that yield an extension is then a homomorphic image $Z$ of $Z^2(H, V)$. Similarly, an image $B$ of the 2-coboundaries $B^2(H, V)$ can be constructed, and eventually the quotient $Z/B$ turns out to be isomorphic to the cohomology group $H^2(H, V)$. The key tool that makes this computation feasible is the fact that one can usually compute efficiently with polycyclic groups, in particular, since every element in a polycyclic group has a normal form with respect to the given polycyclic generating set.

We now discuss a similar approach for a group $H$ that is non necessarily polycyclic, but for which we are given a confluent rewriting system, see [11] Chapter 12 and [20] Section 2 for details on rewriting systems; such a rewriting system allows us to compute normal forms of elements in $H$, so that a similar approach can be used to compute $H^2(H, V)$. The method described here is a natural generalisation of the polycyclic case and already arises implicitly in Holt & Plesken [10] and in Groves [7], as well as in the work of of Schmidt [18], yet we were not able to find a complete description in the literature.

7.1. Extending the rewriting system. By introducing formal inverses, we interpret the group $H$ as a monoid with $2e$ monoid generators $\{h_1^{\pm 1}, \ldots, h_e^{\pm 1}\}$. We consider this monoid as a quotient of a free monoid $A$ on $a = \{a_1^{\pm 1}, \ldots, a_e^{\pm 1}\}$, with $\alpha: A \to H, a_i^{\pm 1} \mapsto h_i^{\pm 1}$, being the natural epimorphism. Note that $a_i^{-1}$ is a formal symbol, while $h_i^{-1}$ is the inverse of the element $h_i$. Using a Knuth-Bendix procedure [20], Section 2.5], we assume that we have a confluent rewriting system (with respect to a reduction order $<_a$) for the monoid $H$ on this generating set; we assume that the system is reduced, that is, no left hand side of a rule is a subset of any other (left or right) hand side. We refer to [20, pp. 51,52,59] for the precise definitions; here we only recall that this rewriting system essentially consists of rules $R_q$ which have the form $l \to r$ for certain words $l$ and $r$ in the generators of $A$.

Since we introduced extra generators to represent inverses, we assume that $R_q$ 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 $R_q \subset R_q$; here $\emptyset$ denotes the empty word. We note that this assumption holds automatically if $<_a$ is based on length. If the order of one group generator $h_i$ is 2, these rules will change shape: without loss of generality, after possibly switching the $a_i$ and $a_i^{-1}$, there will be a

---

2Proving that computing with polycyclic groups has a favourable complexity is difficult because of the challenges involving collection, see Newman & Niemeyer, “On complexity of multiplication in finite solvable groups” (2015). However, the situation for polycyclic groups is much better than for general finitely presented groups where many problems are proven to be undecidable.
rule $a_i^2 \to \emptyset$ (since otherwise $a_i^2$ cannot be reduced), so that the inversion rule becomes $a_i^{-1} \to a_i$. In this case we also add this last rule to $\bar{\mathcal{R}}_q$. We now define $\widehat{\mathcal{R}}_q = \mathcal{R}_q - \bar{\mathcal{R}}_q$, so that our rules are partitioned as

$$\mathcal{R} = \bar{\mathcal{R}}_q \cup \widehat{\mathcal{R}}_q.$$ 

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

$$\mathcal{R}_b = \{b_i^0 \to \emptyset,\ b_j b_j \to b_j b_j : i \in \{1, \ldots, d\}, j > i\}.$$ 

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

We now take the combined alphabet $\mathcal{A} = \{a_1^{\pm 1}, \ldots, a_e^{\pm 1}\} \cup \{b_1, \ldots, b_d\}$ and denote by $<_b$ the wreath product ordering $<_b \triangleleft <_a$, see [20, p. 46]. We define $\mathcal{R}_c$ to be the set of all rules

$$\mathcal{R}_c = \{b_j a_i^\sigma \to a_i^\sigma b_j^{f_{i,j,\sigma,1} \cdots f_{i,j,\sigma,d}} : \sigma \in \{\pm 1\}, i \in \{1, \ldots, e\}, j \in \{1, \ldots, d\}\}$$

where the exponents $f_{i,j,\sigma,k}$ are defined by $v_j^{\sigma(a_i^k)} = v_j^{(f_{i,j,\sigma,1} \cdots f_{i,j,\sigma,d})}$. Correspondingly, we define

$$\mathcal{R}_a = \mathcal{R}_a(\mathbf{x}) = \{l_i \to r_i b^{(x_{i,1} \cdots x_{i,d})} : (l_i \to r_i) \in \widehat{\mathcal{R}}_q\},$$

where

$$\mathbf{x} = (x_{1,1}, \ldots, x_{1,d}, x_{2,1}, \ldots, x_{2,d}, x_{3,1}, \ldots, x_{r-1,d}, x_r, 1, \ldots, x_{r,d})$$

is a list of indeterminates in $\mathbb{Z}_p$, analogous to the aforementioned tails. Lastly, we set

$$\mathcal{R} = \mathcal{R}(\mathbf{x}) = \mathcal{R}_a(\mathbf{x}) \cup \mathcal{R}_b \cup \mathcal{R}_c \cup \bar{\mathcal{R}}_q.$$ 

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. Note that $\mathcal{R}$ is reduced if $\mathcal{R}_q$ and $\mathcal{R}_b$ are reduced. We wish to determine those values for $x_{i,j}$ that make $\mathcal{R}(\mathbf{x})$ a confluent rewriting system defining a group extension of $H$ with $V$; this is analogous to consistency checks for polycyclic groups. We start with the following observation.

**Lemma 7.1.** The monoid presentation $\langle \mathcal{A} | \mathcal{R}(\mathbf{x}) \rangle$ defines a group

**Proof.** Write $\mathcal{R} = \mathcal{R}(\mathbf{x})$. The rules $b_i^0 \to \emptyset$ in $\mathcal{R}_b \subset \mathcal{R}$ show that every generator $b_i$ has an inverse. As $H$ is a group, $\mathcal{R}_q$ 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 $\bar{\mathcal{R}}_q \subseteq \mathcal{R}$. If $h_i$ has order 2, then there will be a rule $a_i^{-1} \to a_i$ in $\bar{\mathcal{R}}_q$ (thus the generator $a_i^{-1}$ is a redundant duplicate generator) and a rule $a_i^2 \to \emptyset$ in $\bar{\mathcal{R}}_q$; this last rule implies the existence of a rule $a_i^2 \to w \in \mathcal{R}_a$, with $w$ a word in the generators $\{b_1, \ldots, b_d\}$ only. Thus $w$ represents an invertible element, and $a_i^{-1} w^{-1}$ will be an inverse for $a_i$. Since every generator has an inverse, the monoid is a group. \qed

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

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

note that some of the relations might become vacuously true in a group.
Lemma 7.2. If $R = R(\mathbf{x})$ is confluent, then $\langle A' \mid R \rangle$ 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 $R_b$ and $R_c$ show that the subgroup $S = \langle b_1, \ldots, b_d \rangle$ is abelian and normal. As the only relations in $R$ whose left side only involves the generators $b_1, \ldots, b_d$ are the relations in $R_b$, confluence of $R$ implies that $S$ is isomorphic to $V$. The factor group can be described by setting all $b_i$ to 1 in the relations; this produces the rules $R_q$, and those define $H$. The rules in $R_c$ prove the claim about the action. \hfill $\square$

7.2. Making the system confluent. We now consider how to determine for which $\mathbf{x}$ the system $R(\mathbf{x})$ is confluent. Using the method described in [20, Section 2.3], we need to consider overlaps (see [20, p. 59]) of left hand sides of rules in $R$. Let $\overline{R}_a = R_a \cup R_q$.

Overlaps of left hand sides of rules in $R_b$ reduce uniquely by the definition of $R_b$. The left hand sides of two rules in $R_c$ cannot overlap because of their specific form. Similarly, rules in $R_b$ and $\overline{R}_a$ cannot overlap as their left hand sides are on disjoint alphabets. The overlap of a left hand side in $R_b$ and in $R_c$ will have the form $w_b a_i$ (where $w_b$ is a word expression in $b$) and reduces uniquely as the action on $V$ is linear. A left hand side in $R_c$ and one in $\overline{R}_a$ will overlap in the form $w_b w_a^i$; such expressions reduce uniquely as the action on a module is a group action. In conclusion, only overlaps of left hand sides in $\overline{R}_a$ remain. These left hand sides are words in $a$ only, and confluence will be a condition on the tuples

$$\mathbf{x} = (x_{1,1}, \ldots, x_{1,d}, x_{2,1}, \ldots, x_{2,d}, x_{3,1}, \ldots, x_{r-1,d}, x_{r,1}, \ldots, x_{r,d})$$

whose entries specify $R_a$; recall that $r$ is the number of rules in $\overline{R}_q$.

To determine these conditions, we consider $R(\mathbf{x})$ as a set of rules on “words” in $A$ that may involve powers of generators $b_i$ whose exponents are linear expressions in the indeterminates $x_{i,j}$. We call such a word $w$ in $A$ clean if it is of the form $w = ab$, where $a$ is a word in the generators $\{a_1^{-1}, \ldots, a_e^{-1}\}$ and $b$ is a word of the form $b_1^{e_1} \cdots b_d^{e_d}$, where the $e_j$ are linear expressions in the $x_{i,k}$ considered modulo $p$. We say that $a$ and $b$ are the $a$-part and $b$-part of $w$. Note that, by repeated application of the rules in $R_a$ and $R_c$, any word can be transformed into a clean word. This implies that any word that cannot be reduced through $R(\mathbf{x})$ must be clean. Furthermore, if the initial word only involved $b_1, \ldots, b_d$, with exponents homogeneous in the $x_{j,k}$ (that is, no constant term), then also the resulting exponents $e_i$ in a reduced form will be homogeneous in the $x_{j,k}$.

Following [20 Proposition 3.1] and the test for confluence [20, p. 62], we now have to consider the overlap of two left hand sides of the rules in $\overline{R}_a$, say $l_i$ and $l_j$. By definition of an overlap, we can write $l_i = st$ and $l_j = tu$ for some words $s, t, u$ in the $a_i$, and the overlap to consider is the word $w = stu$. Applying rule $l_i$ first, we transform $w$ into $w_1 = r(l_b^{(x_{i,1}, \ldots, x_{i,d})} u)$; applying rule $l_j$ first, we obtain $w_2 = s r(l_b^{(x_{j,1}, \ldots, x_{j,d})})$. We apply rules, to $w_1$ and to $w_2$, until we arrive at words $\tilde{w}_1$ and $\tilde{w}_2$ that cannot be reduced any longer, and therefore are clean. Since the $a$-parts of the rules form a confluent rewriting system (and $R_b$ and $R_c$ do not change that part of words), the $a$-parts of the clean results $\tilde{w}_1$ and $\tilde{w}_2$ must be equal; this shows that the condition becomes an equality of $b$-parts with exponents that are homogeneous linear in the $x_{i,k}$. Confluence of $R(\mathbf{x})$ therefore is determined by a finite list of homogeneous linear equations over $\mathbb{Z}_p$, and the system of these equations can be obtained through a collection process applied to overlaps of left hand sides of

...
rules in $\mathcal{R}_A$. We denote the solution space by $X$, that is,

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

We now show that every extension $E$ of $H$ with $V$ is isomorphic to $\langle \mathcal{A}^t \mid \mathcal{R}(\mathbf{x}) \rangle$ for some $\mathbf{x} \in X$. For this recall (for example from [11, p. 53]) that $E$ is isomorphic to a group $E_\gamma$ with underlying set $H \times V$ and multiplication $(g, v)(h, w) = (gh, v^b g \gamma(g, h))$ for some 2-cocycle $\gamma \in Z^2(H, V)$, see also (5.1). We identify $E = E_\gamma$ in the following, and note that we write the normal subgroup $V \leq E$ multiplicatively. Our approach now is to use $E$ to calculate the values $x_{i,j}$ of a suitable $\mathbf{x}$. For this define $\mathbf{u} = (u_1, \ldots, u_e)$, where each $u_i = (h_i, 1) \in E$. For a word $w$ in $\{a_i^{\pm 1}, \ldots, a_e^{\pm 1}\}$ we denote by $\text{Eval}(w, \mathbf{u})$ the element in $E$ that is obtained by replacing each $a_i^{\pm 1}$ by $u_i^{\pm 1}$. Now, for each rule $l_i \rightarrow r_i$ in $\mathcal{R}_q$, calculate

$$t_i = \text{Eval}(r_i, \mathbf{u})^{-1} \text{Eval}(l_i, \mathbf{u}).$$

Since $\mathcal{R}_q$ is a confluent rewriting system of $H$, we must have $t_i \in V$, where we identify $V$ with the subgroup $\{(1, v) : v \in V\} \leq E$; now define $x_{i,1}, \ldots, x_{i,d} \in \mathbb{Z}_p$ such that $t_i = b_{i,1}^{x_{i,1}} \cdots b_{i,d}^{x_{i,d}}$. This defines a tuple $\mathbf{x}$. By the rules of arithmetic in $E$, each $x_{i,j}$ is a homogeneous linear combinations of values of the 2-cocycle $\gamma$, thus the map $\xi : \gamma \mapsto \mathbf{x}$ is linear. Since multiplication in $E$ is associative, the tuple $\mathbf{x}$ defines a confluent rewriting system $\mathcal{R}(\mathbf{x})$, and therefore this process defines a linear map

$$\xi : Z^2(H, V) \rightarrow X.$$

In particular, if $E$ is any group isomorphic to $E_\gamma$ for some $\gamma \in Z^2(H, V)$, then $E \cong \langle \mathcal{A}^t \mid \mathcal{R}(\mathbf{x}) \rangle$ for $\mathbf{x} = \xi(\gamma)$: by the construction of $\mathbf{x}$, the group $E$ satisfies the relations $\mathcal{R}(\mathbf{x})$ and therefore is a quotient of $\langle \mathcal{A}^t \mid \mathcal{R}(\mathbf{x}) \rangle$ by von Dyck’s Theorem [11, Theorem 2.53]; both groups have the same order, so isomorphism is established.

Since $\langle \mathcal{A}^t \mid \mathcal{R}(\mathbf{0}) \rangle$ is the semidirect product of $H$ with $V$, the kernel of $\xi$ lies in $B^2(H, V)$, thus we have determined the second cohomology group $H^2(H, V)$ as

$$H^2(H, V) \cong X/\xi(B^2(H, V)).$$

Note that we can calculate the image of $B^2(H, V)$ under $\xi$ by using a similar collection process: let $\mathbf{x} \in X$ and write $L = \langle \mathcal{A}^t \mid \mathcal{R}(\mathbf{x}) \rangle$ for the corresponding extension. Then $\mathbf{x}$ comes from a 2-coboundary if and only if $L$ is a split extension of $H$ with $V$, if and only if there exist $r_1, \ldots, r_e \in V$ such that the elements $a_1 r_1, \ldots, a_e r_e$ satisfy the relations of $H$; here we identify $V$ with the subgroup of $L$ generated by the $b_{1, \ldots, b_d}$. Thus, assuming that $\mathbf{x}$ defines an extension, we consider indeterminates $r_1, \ldots, r_e \in V$ and then collect and evaluate all rules $\mathcal{R}_q$ in $L$ with each $a_i$ replaced by $a_i r_i$; this gives linear equations relating the entries of the tuple $\mathbf{x}$ with the indeterminates $r_i$. The corresponding solution space characterises the image of $B^2(H, V)$ under $\xi$. In conclusion, we have proved the following result.

**Theorem 7.3.** The tuples $\mathbf{x}$ that make $\mathcal{R}$ confluent form a $\mathbb{Z}_q$-vector space $X$ that is the epimorphic image of $Z^2(H, V)$, the epimorphism $\xi$ preserving isomorphism of the respective extensions. The kernel of $\xi$ lies in the set of 2-coboundaries, thus $H^2(H, V) \cong X/\xi(B^2(H, V))$. 

### 8. Concluding remarks and examples

If the group $H$ we start with is solvable, then the approach outlined here is similar to Plesken’s version [16] of the solvable quotient algorithm in that it constructs simple modules, and forms
extensions with these through 2-cohomology (via tails and consistency checks), since one can use polycyclic presentations in place of rewriting systems), verifying for each extension whether this extensions can be a quotient.

Apart from not requiring solvability of the factor group $H$, our approach differs in that we construct only one (larger) cover for each module type and only need to consider extensions corresponding to a basis of the 2-cohomology group. This significantly reduces the cost of having to construct many extensions if the group of 2-cocycles is of larger dimension. This approach also mirrors the process of the $p$-quotient algorithm [14], which first computes the $p$-cover and then evaluates relators in this cover.

8.1. Explicit computations. As a proof of concept, we have implemented our approach in the computer algebra system GAP [4] and provide functions that compute the covers $\Psi_{V,e}$ and $\hat{H}_{V,e}$, and the lifting process of Section 6. This code is available at

https://www.math.colostate.edu/~hulpke/liftquot.gap;

it requires GAP 4.11, since this version provides our function TwoCohomologyGeneric to compute cohomology groups for non-polycyclic groups. The code represents quotients as permutation groups; to help calculating the orders for $\hat{H}_{V,e}$, a matrix representation of its module is used as well. We use the built-in MeatAxe functionality to determine the splitting field $K$ for a module $V$ and an (absolutely) simple factor module $W$ of $KV$, which gives us the vectors $w_i$ needed in the construction of Section 4.2.

Below we give three examples that illustrate the scope of our approach. The selection of examples has been restricted to groups whose nonabelian composition factors are alternating groups since we have not yet implemented other cases, following [19].

**Example 8.1.** Let $H = A_5$ be the alternating group of degree 5. Over $\mathbb{Z}_2$, it has simple modules of dimension 1, 4, and 4, of which the last one is not absolutely simple. Over $\mathbb{Z}_3$, the simple modules have dimension 1, 4, and 6, respectively. Table 8.1 lists the cohomology groups $H^2(H, V)$ and the sizes of the covers $\Psi_{V,e}(F)$ and $\hat{H}_{V,2}$ for those simple modules. We denote by $p^{a \cdot b}$ a $\mathbb{Z}_pH$-module that can be written as the direct sum of $b$ isomorphic copies of an irreducible module of dimension $a$, it thus is a module of dimension $a \cdot b$. The calculations used the following commands (given for characteristic 3); they completed all in less than a second:

\begin{verbatim}
gap> G:=AlternatingGroup(5);;
gap> irr:=IrreducibleModules(G,GF(3))[2];;
gap> List(irr,x->x.dimension);
[ 1, 4, 6 ]
gap> cov:=ModuleCover(G,irr[1]);;Size(cov);
540
\end{verbatim}

Extending this example, let $G$ be the Heineken group defined by

\[
G = \langle a, b, c \mid [a, [a, b]] = c, [b, [b, c]] = a, [c, [c, a]] = b \rangle;
\]

by eliminating the generator $c$, we consider it as a finitely presented group on two generators. By von Dyck’s Theorem [11, Theorem 2.53], there is a unique epimorphism $\varphi: G \to H$ with
\( \varphi(a) = (1, 2, 4, 5, 3) \) and \( \varphi(b) = (1, 2, 3, 4, 5) \). It was shown in [9, p. 725] that the largest finite nilpotent quotient of \( \ker \varphi \) has order \( 2^{24} \). Evaluating the relators in the covers for characteristic 2, we find that the cover of size \( 2^3 \cdot 60 \) yields a quotient of \( G \) of order \( 2 \cdot 60 \), the cover of size \( 2^{16} \cdot 60 \) yields a quotient of order \( 2^4 \cdot 60 \), and the cover of size \( 2^4 \cdot 60 \) yields no further quotient. We thus found a quotient \( \varphi_2: G \to (2 \times 2^4)A_5 \). We can make this quotient explicit, by forming factor groups of the respective covers \( \tilde{H}_{1,2} \). With our code, the corresponding calculation in GAP uses the following commands; our code uses GAP's functionality to represent quotients as permutation groups and forming their subdirect products:

\[
\text{gap> } \text{F:=FreeGroup("x","y","z");;}
\text{gap> } \text{r:=ParseRelators(F,\"[x,\{x,y\}\]=z,\{y,\{y,z\}\}=x,\{z,\{z,x\}\}=y\");}\n\text{gap> } \text{G:=SimplifiedFpGroup(F/r);;}
\text{gap> } \text{q:=GQuotients(G,AlternatingGroup(5))\[1\];}
\text{gap> } [ x, y ] -> [ (1,2,4,5,3), (1,2,3,4,5) ]
\text{gap> } \text{cov:=LiftQuotient(q,2);;}
\text{gap> } [ x, y ] -> [ (1,12,9,21,23,2,11,10,22,24)(3,7,17,14,5,4,8,18,13,6)(15,16)(25,33,31,27,29)(26,34,32,28,30),
(1,20,10,7,4,2,19,9,8,3)(5,24,21,17,15,6,23,22,18,16)(11,12)(13,14)(25,32,28,33,30)(26,31,27,34,29) ]
\text{gap> } \text{LogInt(Size(Image(cov))/60,2);5}
\]

This calculation took under a second on a 3.7 GHz 2013 Mac Pro. Iterating this construction to the newly found quotient, the following code

\[
\text{gap> } \text{cov:=LiftQuotient(cov,2);;}
\text{gap> } \text{LogInt(Size(Image(cov))/60,2);6}
\]

extends to an image group \( (2 \times 2^4)A_5 \) in about 3 seconds. Further iterations yield quotients

\[
2^4.2.(2 \times 2^4).A_5,
2^4.2^2.(2 \times 2^4).A_5,
(2 \times 2).2^4.2^2.(2 \times 2^4).A_5,
2^4.(2 \times 2).2^4.2^2.(2 \times 2^4).A_5,
2^4.2^4.(2 \times 2).2^4.2^2.(2 \times 2^4).A_5;
\]

the last of which exposes the full quotient \( 2^{24} \) of \( \ker \varphi \). The image group of the last quotient was represented as a permutation group of degree 15360.

All but the last calculation fit easily into 1GB of memory, the last calculation required about 7GB of memory. The timings for these calculations were 8, 80, 246, 795, and 41591 seconds, respectively, and are correlate well with the orders of the covers involved. The runtime is dominated by calculating orders of covers and subgroups therein, and by representing factors as permutation groups.

**Example 8.2.** Consider the group

\[
G = \langle a, b \mid a^3, b^4, (ab)^{15}, [a, b]^2 \rangle;
\]

this is an example of presentations \((m, n, p; q)\) going back to Coxeter, and it is known that \( G \) is infinite, see [21]. The derived subgroup of \( G \) has index 3 and is generated by \( b, x = b^a, \) and
A standard application of a low-index algorithm for subgroups of index up to 12 finds that

\[ y = b^{(a^{-1})} \text{ subject to the relations } b^4 = (xb^{-1})^2 = x^4 = (yx^{-1})^2 = y^4 = (yb^{-1})^2 = (yx)^5 = 1. \]

A low index computation finds an epimorphism \( G' \to A_6 \) that is defined by

\[ b \mapsto (1, 6, 5, 2)(3, 4), \quad x \mapsto (1, 2)(3, 5, 6, 4), \quad y \mapsto (1, 2, 3, 4)(5, 6). \]

Over \( \mathbb{Z}_3 \) the simple modules of \( A_6 \) are of dimensions 1, 4, 6, 9; the corresponding covers \( \hat{H}_{V,2} \) are

\[ 3^{1\cdot 4}.A_6, \quad 3^{4\cdot 6}.A_6, \quad 3^{6\cdot 7}.A_6, \quad \text{and} \quad 3^{9\cdot 9}.A_6, \]

respectively. As quotients of \( G' \), the second and third contribute, resulting in a larger quotient \((3^4 \times 3^6).A_6 \). An iteration to covers of this quotient produces \((3^{4\cdot 3} \times 3^{6\cdot 2}).(3^4 \times 3^6).A_6 \).

**Example 8.3.** Consider the perfect group

\[ G = \langle a, b \mid aba^{-2}bab^{-1} = a(b^{-1}a^3b^{-1}a^{-3})^2 = 1 \rangle \]

from [2]; this group has been a standard example for investigating groups with a low-index algorithm. A standard application of a low-index algorithm for subgroups of index up to 12 finds that \( G \) has a factor group \( \text{PSL}_2(11) \times M_{12}^3 \times A_{11}^8 \times A_{12}^3 \). Since \( 11!/2 = 19958400 \), the order of \( A_{11} \) is so large to make it infeasible to study the kernel of the epimorphism via standard methods.

To illustrate what can be done with our approach, we consider the homomorphism \( G \to A_{11} \) defined by

\[ a \mapsto (1, 2, 3, 5, 4, 6, 7, 9, 10, 8, 11) \quad \text{and} \quad b \mapsto (1, 3, 2, 4)(5, 7, 10, 9, 11)(6, 8). \]

Our calculation shows that for the trivial module 1 in characteristic 2, the cover \( \hat{H}_{1,2} \) has the form \( 2^3.A_{11} \), and this yields a quotient \( 2.A_{11} \) of \( G \). The 10-dimensional module \( V \) of \( A_{11} \) in the same characteristic gives a cover \( \hat{H}_{V,2} = 2^{10\cdot 10}.A_{11} \), and yields a quotient \( 2^{10\cdot 2}.A_{11} \) of \( G \). The 32-dimensional module \( U \) gives a cover \( \hat{H}_{U,2} = 2^{32\cdot 16}.A_{11} \), and yields a quotient \( 2^{32\cdot 3}.A_{11} \) of \( G \). We did not attempt to work with modules in larger dimensions.

**Acknowledgement:** 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.

\[ \text{See } \text{http://www.gap-system.org/Doc/Examples/cavicchioli.html} \text{ for a discussion in the GAP manual.} \]
CONSTRUCTING UNIVERSAL COVERS OF FINITE GROUPS

REFERENCES

[1] E. Artin, C. J. Nesbitt, and R. M. Thrall. Rings with minimum condition. University of Michigan Press, Ann Arbor, 1948.
[2] A. Cavicchioli. A countable class of non-homeomorphic homology spheres with Heegard genus 2. Geom. Dedicata 20 (1986) 345–348
[3] J. Cossey, O. H. Kegel, and L. G. Kovacs. Maximal Frattini Extensions. Arch. Math. 35 (1980) 210–217.
[4] The GAP Group. GAP – Groups, Algorithms, and Programming. gap-system.org
[5] W. Gaschütz. Über modulare Darstellungen endlicher Gruppen, die von freien Gruppen induziert werden. Math. Zeitschr. 60 (1954) 274–286.
[6] R. L. Griess and P. Schmid. The Frattini module. Arch. Math. (Basel) 30 (1978) 256–266.
[7] R. J. R. Groves. An Algorithm for Computing Homology Groups. J. Algebra 194 (1999) 714–728.
[8] K. W. Gruenberg. Relation modules of finite groups. Conference Board of the Mathematical Sciences Regional Conference Series in Mathematics, No. 25. American Mathematical Society, Providence, R.I., 1976.
[9] D. F. Holt, and S. Rees. Computing with Abelian Sections of Finitely Presented Groups. J. Algebra 214 (1999) 714–728.
[10] D. F. Holt and W. Plesken. Perfect groups. Oxford University Press, New York, 1989
[11] D. F. Holt, B. Eick, and E. A. O’Brien. Handbook of computational group theory. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2005.
[12] D. L. Johnson. Presentations of Groups. Cambridge University Press, 1997.
[13] K. Lux and H. Pahlings. Representations of groups. A computational approach. Cambridge Studies in Advanced Mathematics, 124. Cambridge University Press, Cambridge, 2010.
[14] M. F. Newman and E. A. O’Brien. Application of computers to questions like those of Burnside. II. Internat. J. Algebra Comput 6 (1996) 593–605.
[15] A. Niemeyer. A finite soluble quotient algorithm. J. Symbolic Comput. 18 (1994) 541–561.
[16] W. Plesken. Towards a soluble quotient algorithm. J. Symbolic Comput. 4 (1987) 111–122.
[17] D. J. S. Robinson. A Course in the Theory of Groups. Springer-Verlag, 1982.
[18] J. Schmidt. Rewriting systems for finite groups. Thesis (Ph.D.)–University of Kentucky (ISBN: 978-1124-75160-3), 2008.
[19] J. Schmidt. Finite groups have short rewriting systems. Computational group theory and the theory of groups, II, 185-200, Contemp. Math., 511, Amer. Math. Soc., Providence, RI, 2010.
[20] C. C. Sims. Computation with finitely presented groups. Cambridge University Press, 1994.
[21] R. M. Thomas. Group presentations where the relators are proper powers. Groups ’93 Galway/St. Andrews, Vol. 2, 549-560, London Math. Soc. Lecture Note Ser., 212, Cambridge Univ. Press, Cambridge, 1995
[22] J. Thévenaz. Maximal subgroups of direct products. J. Algebra 198 (1997) 352–361.