FINDING DIRECT PRODUCT DECOMPOSITIONS IN POLYNOMIAL TIME

JAMES B. WILSON

Abstract. A polynomial-time algorithm is produced which, given generators for a group of permutations on a finite set, returns a direct product decomposition of the group into directly indecomposable subgroups. The process uses bilinear maps and commutative rings to characterize direct products of p-groups of class 2 and reduces general groups to p-groups using group varieties. The methods apply to quotients of permutation groups and operator groups as well.

Contents

Date: October 27, 2018.
Key words and phrases. direct product, polynomial time, group variety, p-group, bilinear map.
This research was supported in part by NSF Grant DMS 0242983.

1. Introduction

Forming direct products of groups is an old and elementary way to construct new groups from old ones. This paper concerns reversing that process by efficiently decomposing a group into a direct product of nontrivial subgroups in a maximal way, i.e. constructing a *Remak decomposition* of the group. We measure efficiency by describing the time (number of operations) used by an algorithm, as a function of the input size. Notice that a small set of generating permutations or matrices can specify a group of exponentially larger size; hence, there is some work just to find the order of a group in polynomial time. In the last 40 years, problems of this sort have been attacked with ever increasing dependence on properties of simple groups, and primitive and irreducible actions, cf. [32]. A polynomial-time algorithm to construct a Remak decomposition is an obvious addition to those algorithms and, as might be expected, our solution depends on many of those earlier works. Surprisingly, the main steps involve tools (bilinear maps, commutative rings, and group varieties) that are not standard in Computational Group Theory.

We solve the Remak decomposition problem for permutation groups and describe the method in a framework suitable for other computational settings, such as matrix groups. We prove:

Theorem 1.1. *There is a deterministic polynomial-time algorithm which, given a permutation group, returns a Remak decomposition of the group.*

It seems natural to solve the Remak decomposition problem by first locating a direct factor of the group, constructing a direct complement, and then recursing on the two factors. Indeed, Luks [18] and Wright [37] (cf. Theorem 4.2) gave polynomial-time algorithms to test if a subgroup is a direct factor and if so to construct a direct complement. But how do we find a proper nontrivial direct factor to start with? A critical case for that problem is p-groups. A p-group generally has an exponential number of normal subgroups so that searching for direct factors of a p-group appears impossible.

The algorithm for Theorem 1.1 does not proceed in the natural fashion just described, and it is more of a construction than a search. In fact, the algorithm does not produce a single direct factor of the original group until the final step, at which point it has produced an entire Remak decomposition.

It was the study of central products of p-groups which inspired the approach we use for Theorem 1.1. In [35, 36], central products of a p-group P of class 2 were linked, via a bilinear map $\mathsf{Bi}(P)$, to idempotents in a Jordan algebra in a way that explained their size, their $(\mathrm{Aut}\, P)$-orbits, and demonstrated how to use the polynomial-time algorithms for rings (Ronyai [29]) to construct fully refined central decompositions all at once (rather than incrementally refining a decomposition). This approach is repeated here, only we replace Jordan algebras with a canonical commutative ring $C(P) := C(\mathsf{Bi}(P))$ (cf. (5.10) and Definition 5.16). Thus, we characterize directly indecomposable p-groups of class 2 as follows:

Theorem 1.2. *If P and Q are finite p-groups of nilpotence class 2 then $C(P\times Q) \cong C(P) \oplus C(Q)$. Hence, if $C(P)$ is a local ring and $\zeta_1(P) \leq \Phi(P)$, then P is directly indecomposable. Furthermore, if $P^p = 1$ then the converse also holds.*

The algorithm applies the implications of Theorem 1.2 and begins with the *unique* Remak decomposition of a commutative ring. This process is repeated across several sections of the group. Using group varieties we organize the various sections. Group varieties behave well regarding direct products and come with natural and computable normal subgroups used to create the sections. To work within these sections of a permutation group we have had to prove Theorem 1.1 in the generality of quotients of permutation groups and thus we have used the Kantor-Luks polynomial-time quotient group algorithms [12]. Those methods depend on the Classification of Finite Simple Groups and, in this way, so does Theorem 1.1. A final generalization of the main result is the need to allow groups with operators Ω and consider Remak Ω-decompositions. The most general version of our main result is summarized in Theorem 6.4 followed by a variant for matrix groups in Corollary 6.6.

Theorem 1.1 was proved in 2008 [34]. That same year, with entirely different methods, Kayal-Nezhmetdinov [14] proved there is a deterministic polynomial-time algorithm which, given a group G specified by its multiplication table (i.e. the size of input is $|G|^2$), returns a Remak decomposition of G. The same result follows as a corollary to Theorem 1.1 by means of the regular permutation representation of G. Theorem 8.1 states that in that special situation there is a nearly-linear-time algorithm for the task.

1.1. **Outline.**

We organize the paper as follows.

In Section 2 we introduce the notation and definitions we use throughout. This includes the relevant group theory background, discussion of group varieties, rings and modules, and a complete listing of the prerequisite tools for Theorem 1.1.

In Section 3 we show when and how a direct decomposition of a subgroup or quotient group can be extended or lifted to a direct decomposition of the whole group (Sections 3.1–3.4). That task centers around the selection of good classes of groups as well as appropriate normal subgroups. The results in that section are largely non-algorithmic though they lay foundations for the correctness proofs and suggest how the data will be processed by the algorithm for Theorem 1.1.

Section 4 applies the results of the earlier section to produce a polynomial-time algorithm which can effect the lifting/extending of direct decompositions of subgroups and quotient groups. First we show how to construct direct Ω-complements of a direct Ω-factor of a group (Section 4.1) by modifying some earlier unpublished work of Luks [18] and Wright [37]. Those algorithms answer Problem 2, and (subject to some constraints) also Problem 4 of [14, p. 13]. The rest of the work concerns the algorithm Merge described in Section 4.2 which does the 'glueing' together of direct factors from a normal subgroup and its quotient.

In Section 5 we characterize direct decompositions of p-groups of class 2 by means of an associated commutative ring and prove Theorem 1.2. We close that section with some likely well-known results on groups with trivial centers.

In Section 6 we prove Theorem 1.1 and its generalization Theorem 6.4. This is a specific application which demonstrates the general framework setup in Sections 3 and 4. Theorem 6.4 answers Problem 3 of [14, p. 13] and Corollary 6.6 essentially answers Problem 5 of [14, p. 13].

Section 7 is an example of how the algorithm's main components operate on a specific group. The execution is explained with an effort to indicate where some of the subtle points in the process arise.

Section 8 wraps up loose ends and poses some questions.

2. Background

We begin with a survey of the notation, definitions, and algorithms we use throughout the paper. Much of the preliminaries can be found in standard texts on Group Theory, consider [16, Vol. I §§15–18; Vol. II §§45–47].

Typewriter fonts $\mathtt{X}, \mathtt{R}$, etc. denote sets without implied properties; Roman fonts G, H, etc., denote groups; Calligraphic fonts $\mathcal{H}, \mathcal{X}$, etc. denote sets and multisets of groups; and the Fraktur fonts $\mathfrak{X}$, $\mathfrak{N}$, etc. denote classes of groups.

With few exceptions we consider only finite groups. Functions are evaluated on the right and group actions are denoted exponentially. We write $\operatorname{End} G$ for the set of endomorphisms of G and $\operatorname{Aut} G$ for the group of automorphisms. The *centralizer* of a subgroup $H \leq G$ is $C_G(H) = \{g \in G : H^g = H\}$. The *upper central series* is $\{\zeta_i(G) : i \in \mathbb{N}\}$ where $\zeta_0(G) = 1$, $\zeta_i(G) \lhd \zeta_{i+1}(G)$ and $\zeta_{i+1}(G)/\zeta_i(G) = C_{G/\zeta_i(G)}(G/\zeta_i(G))$, for all $i \in \mathbb{N}$. The commutator of subgroups H and K of G is $[H, K] = \langle [h, k] : h \in H, k \in K\rangle$. The *lower central series* is $\{\gamma_i(G) : i \in \mathbb{Z}^+\}$ where $\gamma_1(G) = G$ and $\gamma_{i+1}(G) = [G, \gamma_i(G)]$ for all $i \in \mathbb{Z}^+$. The *Frattini* subgroup $\Phi(G)$ is the intersection of all maximal subgroups.

2.1. Operator groups.

An Ω-group G is a group, a possibly empty set Ω, and a function $\theta : \Omega \to \operatorname{End} G$. Throughout the paper we write g^ω for $g(\omega\theta)$, for all $g \in G$ and all $\omega \in \Omega$.

With the exception of Section 6.3, we insist that $\Omega\theta \subseteq \operatorname{Aut} G$.

In a natural way, Ω-groups have all the usual definitions of Ω-subgroups, quotient Ω-groups, and Ω-homomorphisms. Call H is *fully invariant*, resp. *characteristic* if it is an $(\operatorname{End} G)-$, resp. $(\operatorname{Aut} G)-$, subgroup. As we insist that $\Omega\theta \subseteq \operatorname{Aut} G$, in this work every characteristic subgroup of G is automatically an Ω-subgroup. Let $\operatorname{Aut}_\Omega G$ denote the Ω-automorphisms of G. We describe normal Ω-subgroups M of G simply as $(\Omega \cup G)$-subgroup of G.

The following characterization is critical to our proofs.

$$\operatorname{Aut}_{\Omega\cup G} G = \{\varphi \in \operatorname{Aut}_\Omega G : \forall g \in G, g\varphi \equiv g \pmod{\zeta_1(G)}\}. \tag{2.1}$$

It is also evident that $\operatorname{Aut}_{\Omega\cup G} G$ acts as the identity on $\gamma_2(G)$. Such automorphisms are called *central* but for uniformity we described them as $(\Omega \cup G)$-automorphisms.

We repeatedly use the following property of the $(\Omega \cup G)$-subgroup lattice.

Lemma 2.2 (Modular law)**.** [16, Vol. II §44: pp. 91-92] *If M, H, and R are $(\Omega \cup G)$-subgroups of an Ω-group G and $M \leq H$, then $H \cap RM = (H \cap R)M$.*

2.2. Decompositions, factors, and refinement.

Let G be an Ω-group. An Ω-*decomposition* of G is a set $\mathcal{H}$ of $(\Omega \cup G)$-subgroups of G which generates G but no proper subset of $\mathcal{H}$ does. A *direct* Ω-*decomposition* is an Ω-decomposition $\mathcal{H}$ where $H \cap \langle \mathcal{H} - \{H\}\rangle = 1$, for all $H \in \mathcal{H}$. In that case, elements H of $\mathcal{H}$

are direct Ω-factors of G and $\langle \mathcal{H} - \{H\}\rangle$ is a *direct Ω-complement* to H. Call G *directly Ω-indecomposable* if $\{G\}$ is the only direct Ω-decomposition of G. Finally, a *Remak Ω-decomposition* means a direct Ω-decomposition consisting of directly Ω-indecomposable groups.

Our definitions imply that the trivial subgroup 1 is not a direct Ω-factor. Furthermore, the only direct decomposition of 1 is $\emptyset$ and so 1 is not directly Ω-indecomposable.

We repeatedly use for the following notation. Fix an Ω-decomposition $\mathcal{H}$ of an Ω-group G, and an $(\Omega \cup G)$-subgroup M of G. Define the sets

$$\mathcal{H} \cap M = \{H \cap M : H \in \mathcal{H}\} - \{1\}, \tag{2.3}$$

$$\mathcal{H}M = \{HM : H \in \mathcal{H}\} - \{M\}, \text{ and} \tag{2.4}$$

$$\mathcal{H}M/M = \{HM/M : H \in \mathcal{H}\} - \{M/M\}. \tag{2.5}$$

If $f : G \to H$ is an Ω-homomorphism then define

$$\mathcal{H}f = \{Hf : H \in \mathcal{H}\} - \{1\}. \tag{2.6}$$

Each of these sets consists of Ω-subgroups of $G \cap M$, M, G/M, and $\operatorname{im} f$ respectively. It is not generally true that these sets are Ω-decompositions. In particular, for arbitrary M, we should not expect a relationship between the direct Ω-decompositions of G/M and those of G.

If $\mathfrak{X}$ is a class of groups then set

$$\mathcal{H} \cap \mathfrak{X} = \{H \in \mathcal{H} : H \in \mathfrak{X}\}, \text{ and} \tag{2.7}$$

$$\mathcal{H} - \mathfrak{X} = \mathcal{H} - (\mathcal{H} \cap \mathfrak{X}). \tag{2.8}$$

An Ω-decomposition $\mathcal{H}$ of G *refines* an Ω-decomposition $\mathcal{K}$ of G if for each $H \in \mathcal{H}$, there a unique $K \in \mathcal{K}$ such that $H \leq K$ and furthermore,

$$\forall K \in \mathcal{K}, \quad K = \langle H \in \mathcal{H} : H \leq K\rangle. \tag{2.9}$$

When $\mathcal{K}$ is a direct Ω-decomposition, (2.9) implies the uniqueness preceding the equation. If $\mathcal{H}$ is a direct Ω-decomposition then $\mathcal{K}$ is a direct Ω-decomposition.

An essential tool for us is the so called "Krull-Schmidt" theorem for finite groups.

Theorem 2.10 ("Krull-Schmidt"). [16, Vol. II, p. 120] *If G is an Ω-group and $\mathcal{R}$ and $\mathcal{T}$ are Remak Ω-decompositions of G, then for every $\mathcal{X} \subseteq \mathcal{R}$, there is a $\varphi \in \operatorname{Aut}_{\Omega \cup G} G$ such that $\mathcal{X}\varphi \subseteq \mathcal{T}$ and φ is the identity on $\mathcal{R} - \mathcal{X}$. In particular, $\mathcal{R}\varphi = \mathcal{X}\varphi \sqcup (\mathcal{R} - \mathcal{X})$ is a Remak Ω-decomposition of G.*

Remark 2.11. The "Krull-Schmidt" theorem combines two distinct properties. First, it is a theorem about exchange (as compared to a basis exchange). That property was proved by Wedderburn [19] in 1909. Secondly, it is a theorem about the transitivity of a group action. That property was the contribution of Remak [27] in 1911. Remak was made aware of Wedderburn's work in the course of publishing his paper and added to his closing remarks [27, p. 308] that Wedderburn's proof contained an unsupported leap (specifically at [19, p.175, l.-4]). This leap is not so great by contemporary standards, for example it occurs in [30, p.81, l.-12]. Few references seem to be made to Wedderburn's work following Remak's publication.

In 1913, Schmidt [31] simplified and extended the work of Remak and in 1925 Krull [15] considered direct products of finite and infinite abelian Ω-groups. Fitting [5] invented the standard proof using idempotents, Ore [26] grounded the concepts in Lattice theory, and in several works Kurosh [16, §17, §§42–47] and others unified and expanded these results. By the 1930's direct decompositions of maximum length appear as "Remak decompositions" while at the same time the theorem is referenced as "Krull-Schmidt".

2.3. Free groups, presentations, and constructive presentations.

In various places we use free groups. Fix a set $\mathtt{X} \neq \emptyset$ and a group G. Let $G^{\mathtt{X}}$ denote the set of functions from $\mathtt{X}$ to G, equivalently, the set of all $\mathtt{X}$-tuples of G.

Every $f \in G^{\mathtt{X}}$ is the restriction of a unique homomorphism $\hat{f}$ from the free group $F(\mathtt{X})$ into G, that is:

$$\forall x \in \mathtt{X}, \quad x\hat{f} = xf. \tag{2.12}$$

We use $\hat{f}$ exclusively in that manner. As usual we call $\langle \mathtt{X}|\mathtt{R}\rangle$ a *presentation* for a group G with respect to $f : \mathtt{X} \to G$ if $\mathtt{X}f$ generates G and $\ker \hat{f}$ is the smallest normal subgroup of $F(\mathtt{X})$ containing $\mathtt{R}$.

Following [13, Section 3.1], $\{\langle \mathtt{X}|\mathtt{R}\rangle, f : \mathtt{X} \to G, \ell : G \to F(\mathtt{X})\}$ is a *constructive presentation* for G, if $\langle \mathtt{X}|\mathtt{R}\rangle$ is a presentation for G with respect to f and $\ell\hat{f}$ is the identity on G. More generally, if M is a normal subgroup of G then call $\{\langle \mathtt{X}|\mathtt{R}\rangle, f : \mathtt{X} \to G, \ell : G \to F(\mathtt{X})\}$ a *constructive presentation for G mod M* if $\langle \mathtt{X}|\mathtt{R}\rangle$ is a presentation of G/M with respect to the induced function $\mathtt{X} \xrightarrow{f} G \to G/M$, also $\ell\hat{f}$ is the identity on G, and $M\ell \leq \langle \mathtt{R}^{F(\mathtt{X})}\rangle$.

2.4. Group classes, varieties, and verbal and marginal subgroups.

In this section we continue the notation given in Section 2.3 and introduce the vocabulary and elementary properties of group varieties studies at length in [24].

By a *class of Ω-groups* we shall mean a class which contains the trivial group and is closed to Ω-isomorphic images. If $\mathfrak{X}$ is a class of ordinary groups, then $\mathfrak{X}^{\Omega}$ denotes the subclass of Ω-groups in $\mathfrak{X}$.

A *variety* $\mathfrak{V} = \mathfrak{V}(\mathtt{W})$ is a class of groups defined by a set $\mathtt{W}$ of words, known as *laws*. Explicitly, $G \in \mathfrak{X}$ if, and only if, every $f \in G^{\mathtt{X}}$ has $\mathtt{W} \subseteq \ker \hat{f}$. We say that $w \in F(\mathtt{X})$ is a *consequence* of the laws $\mathtt{W}$ if for every $G \in \mathfrak{V}$ and every $f \in G^{\mathtt{X}}$, $w \in \ker \hat{f}$.

The relevance of these classes to direct products is captured in the following:

Theorem 2.13 (Birkhoff-Kogalovski)**.** [24, 15.53] *A class of groups is a variety if, and only if, it is nonempty and is closed to homomorphic images, subgroups, and direct products (including infinite products).*

Fix a word $w \in F(\mathtt{X})$. We regard w as a function $G^{\mathtt{X}} \to G$, denoted w, where

$$\forall f \in G^{\mathtt{X}}, \quad w(f) = w\hat{f}. \tag{2.14}$$

On occasion we write $w(f)$ as $w(g_1, g_2, \dots)$, where $f \in G^{\mathtt{X}}$ is understood as the tuple $(g_1, g_2, \dots)$. For example, if $w = [x_1, x_2]$, then $w : G^2 \to G$ can be defined as $w(g_1, g_2) = [g_1, g_2]$, for all $g_1, g_2 \in G$.

Levi and Hall separately introduced two natural subgroups to associate with the function $w : G^{\mathtt{X}} \to G$. First, to approximate the image of w with a group, we have the *verbal* subgroup

$$w(G) = \langle w(f) : f \in G^{\mathtt{X}}\rangle. \tag{2.15}$$

Secondly, to mimic the radical of a multilinear map, we use the *marginal* subgroup

$$w^*(G) = \{g \in G \ : \ \forall f' \in \langle g\rangle^{\mathtt{X}}, \forall f \in G^{\mathtt{X}}, \ w(ff') = w(f)\}. \tag{2.16}$$

(To be clear, $ff' \in G^{\mathtt{X}}$ is the pointwise product: $x(ff') = (xf)(xf')$ for all $x \in \mathtt{X}$.) Thus, $w : G^{\mathtt{X}} \to G$ factors through $w : (G/w^*(G))^{\mathtt{X}} \to w(G)$. For a set $\mathtt{W}$ of words, the $\mathtt{W}$-verbal subgroup is $\langle w(G) : w \in \mathtt{W}\rangle$ and the $\mathtt{W}$-marginal subgroup is $\bigcap\{w^*(G) : w \in \mathtt{W}\}$. Observe that for finite sets $\mathtt{W}$ a single word may be used instead, e.g. replace $\mathtt{W} = \{[x_1, x_2], x_1^2\} \subseteq F(\{x_1, x_2\})$ with $w = [x_1, x_2]x_3^2 \in F(\{x_1, x_2, x_3\})$. If we have a variety $\mathfrak{V}$ defined by two sets $\mathtt{W}$ and $\mathtt{U}$ of laws, then every $u \in \mathtt{U}$ is a consequence of the laws $\mathtt{W}$. From the definitions above it follows that $u(G) \leq \mathtt{W}(G)$ and $\mathtt{W}^*(G) \leq u^*(G)$. Reversing the roles of $\mathtt{W}$ and $\mathtt{U}$, it follows that $\mathtt{W}(G) = \mathtt{U}(G)$ and $\mathtt{W}^*(G) = \mathtt{U}^*(G)$. This justifies the notation

$$\mathfrak{V}(G) = \mathfrak{V}(\mathtt{W})(G) = \mathtt{W}(G),$$
$$\mathfrak{V}^*(G) = \mathfrak{V}(\mathtt{W})^*(G) = \mathtt{W}^*(G).$$

The verbal and marginal groups are dual in the following sense [6]: for a group G,

$$\mathfrak{V}(G) = 1 \quad \Leftrightarrow \quad G \in \mathfrak{V} \quad \Leftrightarrow \quad \mathfrak{V}^*(G) = G. \tag{2.17}$$

Also, verbal subgroups are radical, $\mathfrak{V}(G/\mathfrak{V}(G)) = 1$, and marginal subgroups are idempotent, $\mathfrak{V}^*(\mathfrak{V}^*(G)) = \mathfrak{V}^*(G)$, but verbal subgroups are not generally idempotent and marginal subgroups are not generally radical.

Example 2.18. (i) The class $\mathfrak{A}$ of abelian groups is a group variety defined by $[x_1, x_2]$. The $\mathfrak{A}$-verbal subgroup of a group is the commutator subgroup and the $\mathfrak{A}$-marginal subgroup is the center.

(ii) The class $\mathfrak{N}_c$ of nilpotent groups of class at most c is a group variety defined by $[x_1, \dots, x_{c+1}]$ (i.e. $[x_1] = x_1$ and $[x_1, \dots, x_{i+1}] = [[x_1, \dots, x_i], x_{i+1}]$, for all $i \in \mathbb{N}$). Also, $\mathfrak{N}_c(G) = \gamma_{c+1}(G)$ and $\mathfrak{N}_c^*(G) = \zeta_c(G)$ [28, 2.3].

(iii) The class $\mathfrak{S}_d$ of solvable groups of derived length at most d is a group variety defined by $\delta_d(x_1, \dots, x_{2^d})$ where $\delta_1(x_1) = x_1$ and for all $i \in \mathbb{N}$,

$$\delta_{i+1}(x_1, \dots, x_{2^{i+1}}) = [\delta_i(x_1, \dots, x_{2^i}), \delta_i(x_{2^i+1}, \dots, x_{2^{i+1}})].$$

Predictably, $\mathfrak{S}_d(G) = G^{(d)}$ is the d-th derived group of G. It appears that $\mathfrak{S}_d^*(G)$ is not often used and has no name. (This may be good precedent for $\mathfrak{S}_d^*(G)$ can be trivial while G is solvable; thus, the series $\mathfrak{S}_1^*(G) \leq \mathfrak{S}_2^*(G) \leq \cdots$ need not be strictly increasing.)

Verbal and marginal subgroups are characteristic in G and verbal subgroups are also fully invariant [6]. So if G is an Ω-group then so is $\mathfrak{V}(G)$. Moreover,

$$G \in \mathfrak{V}^{\Omega} \text{ if, and only if, } G \text{ is an } \Omega\text{-group and } \mathfrak{V}(G) = 1. \tag{2.19}$$

Unfortunately, marginal subgroups need not be fully invariant (e.g. the center of a group). In their place, we use the Ω-invariant marginal subgroup $(\mathfrak{V}^{\Omega})^*(G)$, i.e. the largest normal Ω-subgroup of $\mathfrak{V}^*(G)$. Since $\mathfrak{V}$ is closed to subgroups it follows that $(\mathfrak{V}^{\Omega})^*(G) \in \mathfrak{V}$. Furthermore, if G is an Ω-group and $G \in \mathfrak{V}$ then $\mathfrak{V}^*(G) = G$ and so the Ω-invariant marginal subgroup is G. Thus,

$$G \in \mathfrak{V}^{\Omega} \text{ if, and only if, } G \text{ is an } \Omega\text{-group and } \mathfrak{V}^*(G) = G. \tag{2.20}$$

In our special setting all operators act as automorphisms and so the invariant marginal subgroup is indeed the marginal subgroup. Nevertheless, to avoid confusion insist that the marginal subgroup of a variety of Ω-groups refers to the Ω-invariant marginal subgroup.

2.5. **Rings, frames, and modules.** We involve some standard theorems for associative unital finite rings and modules. Standard references for our uses include [7, Chapters 1–3] and [11, Chapters I–II, V.3]. Throughout this section R denotes a finite associative unital ring.

A $e \in R - \{0\}$ is *idempotent* if $e^2 = e$. An idempotent is *proper* if it is not 1 (as we have excluded 0 as an idempotent). Two idempotents $e, f \in R$ are *orthogonal* if $ef = 0 = fe$. An idempotent is *primitive* if it is not the sum of two orthogonal idempotents. Finally, a *frame* $\mathcal{E} \subseteq R$ is a set of pairwise orthogonal primitive idempotents of R which sum to 1. We use the following properties.

Lemma 2.21 (Lifting idempotents). *Let R be a finite ring.*

(i) If $e \in R$ such that $e^2 - e \in J(R)$ (the Jacobson radical) then for some $n \leq \log_2 |J(R)|$, $(e^2 - e)^n = 0$ and

$$\hat{e} = \sum_{i=0}^{n-1} \binom{2n-1}{i} e^{2n-1-i}(1-e)^i$$

is an idempotent in R. Furthermore, $\widehat{1-e} = 1 - \hat{e}$.

(ii) $\mathcal{E}$ is a frame of $R/J(R)$ then $\hat{\mathcal{E}} = \{\hat{e} : e \in \mathcal{E}\}$ is a frame of R.

(iii) Frames in R are conjugate by a unit in R; in particular, if R is commutative then R has a unique frame.

Proof. Part (i) is verified directly, compare [3, (6.7)]. Part (ii) follows from induction on (i). For (iii) see [3, p. 141]. □

If M is an R-module and e is an idempotent of $\operatorname{End}_R M$ then $M = Me \oplus M(1-e)$. Furthermore, if $M = E \oplus F$ as an R-module, then the projection $e_E : M \to M$ with kernel F and image E is an idempotent endomorphism of M. Thus, every direct R-decomposition $\mathcal{M}$ of M is parameterized by a set $\mathcal{E}(\mathcal{M}) = \{e_E : E \in \mathcal{M}\}$ of pairwise orthogonal idempotents of $\operatorname{End}_R M$ which sum to 1. Remak R-decompositions of M correspond to frames of $\operatorname{End}_R M$.

2.6. **Polynomial-time toolkit.** We use this section to specify how we intend to compute with groups of permutations. We operate in the context of quotients of permutation groups and borrow from the large library of polynomial-time algorithms for this class of groups. We detail the problems we use in our proof of Theorem 1.1 so that in principle any computational domain with polynomial-time algorithms for these problems will admit a theorem similar to Theorem 1.1. The majority of algorithms which we cite do not provide specific estimates on the polynomial timing. Therefore, our own main theorems will not have specific estimates.

The group S_n denotes the permutations on $\{1, \ldots, n\}$. Given $\mathtt{X} \subseteq S_n$, a *straight-line program* over $\mathtt{X}$ is a recursively defined function on $\mathtt{X}$ which evaluates to a word over $\mathtt{X}$, but can be stored and evaluated in an efficient manner; see [32, p. 10]. To simplify notation we treat these as elements in S_n.

Write $\mathbb{G}_n$ for the class of groups G encoded by $(\mathtt{X} : \mathtt{R})$ where $\mathtt{X} \subseteq S_n$ and $\mathtt{R}$ is a set of straight-line programs such that

$$G = \langle \mathtt{X} \rangle / N, \qquad N := \left\langle \mathtt{R}^{\langle \mathtt{X} \rangle} \right\rangle \leq \langle \mathtt{X} \rangle \leq S_n. \tag{2.22}$$

The notation $\mathbb{G}_n$ intentionally avoids reference to the permutation domain as the algorithms we consider can be adapted to other computational domains. Also, observe that a group $G \in \mathbb{G}_n$ may have no small degree permutation representation.

For example, the extraspecial group 2_+^{1+2n} is a quotient of $D_8^n \leq S_{4n}$; yet, the smallest faithful permutation representation of 2_+^{1+2n} has degree 2^n [25, Introduction]. It is misleading to think of $\mathtt{R}$ in (2.22) as relations for the generators $\mathtt{X}$; indeed, elements in $\mathtt{X}$ are also permutations and so there are relations implied on $\mathtt{X}$ which may not be implied by $\mathtt{R}$. We write $\ell(\mathtt{R})$ for the sum of the lengths of straight-line programs in $\mathtt{R}$.

A homomorphism $f : G \to H$ of groups $G = (\mathtt{X} : \mathtt{R}), H = (\mathtt{Y} : \mathtt{S}) \in \mathbb{G}_n$ is encoded by storing $\mathtt{X}f$ as straight-line programs in $\mathtt{Y}$. An Ω-group G is encoded by $G = (\mathtt{X} : \mathtt{R}) \in \mathbb{G}_n$ along with a function $\theta : \Omega \to \operatorname{End} G$. We write $\mathbb{G}_n^{\Omega}$ for the set of Ω-groups encoded in that fashion.

A *polynomial-time* algorithm with input $G = (\mathtt{X} : \mathtt{R}) \in \mathbb{G}_n^{\Omega}$ returns an output using a polynomial in $|\mathtt{X}|n + \ell(\mathtt{R}) + \ell(\Omega)$ number of steps. In some cases $|\mathtt{X}|n + \ell(\mathtt{R}) \in O(\log |G|)$; so, $|G|$ can be exponentially larger than the input size. When we say "given an Ω-group G" we shall mean $G \in \mathbb{G}_n^{\Omega}$.

Our objective in this paper is to solve the following problem.

P. 2.23. Remak-Ω-Decomposition

Given: *an Ω-group G,*
Return: *a Remak Ω-decomposition for G.*

The problems P. 2.24–P. 2.37 have polynomial-time solutions for groups in $\mathbb{G}_n^{\Omega}$.

P. 2.24. Order[12, P1]

Given: *a group G,*
Return: $|G|$.

P. 2.25. Member[12, 3.1]

Given: *a group G, a subgroup $H = (\mathtt{X}' : \mathtt{R}')$ of G, and $g \in G$,*
Return: *false if $g \notin H$; else, a straight-line program in $\mathtt{X}'$ reaching $g \in H$.*

We require the means to solve systems of linear equations, or determine that no solution exists, in the following generalized setting.

P. 2.26. Solve[13, Proposition 3.7]

Given: *a group G, an abelian normal subgroup M, a function $f \in G^{\mathtt{X}}$ of constants in G, and a set $\mathtt{W} \subseteq F(\mathtt{X})$ of words encoded via straight-line programs;*
Return: *false if $w(f\mu) \neq 1$ for all $\mu \in M^{\mathtt{X}}$; else, generators for the solution space $\{\mu \in M^{\mathtt{X}} : w(f\mu) = 1\}$.*

P. 2.27. Presentation[12, P2]

Given: *given a group G and a normal subgroup M,*
Return: *a constructive presentation $\{\langle \mathtt{X} | \mathtt{R} \rangle, f, \ell\}$ for G mod M.*

P. 2.28. Minimal-Normal[12, P11]

Given: *a group G,*
Return: *a minimal normal subgroup of G.*

P. 2.29. Normal-Centralizer[12, P6]

Given: *a group G and a normal subgroup H,*
Return: $C_G(H)$.

P. 2.30. Primary-Decomposition

Given: *an abelian group $A \in \mathbb{G}_n$,*
Return: *a primary decomposition for $A = \bigoplus_{v\in \mathtt{B}} \mathbb{Z}_{p^e} v$, where for each $v \in \mathtt{B}$, $|v| = p^e$ for some prime $p = p(v)$.*

We call $\mathcal{X}$, as in Primary-Decomposition, a *basis* for A. The polynomial-time solution of Primary-Decomposition is routine. Let $A = (\mathtt{X} : \mathtt{R}) \in \mathbb{G}_n$. Use Order to compute $|A|$. As A is a quotient of a permutation group, the primes dividing $|A|$ are less than n. Thus, pick a prime $p \mid |A|$ and write $|A| = p^e m$ where $(p, m) = 1$. Set $A_p = A^m$. Using Member build a basis $\mathtt{B}_p$ for A_p by unimodular linear algebra. (Compare [36, Section 2.3].) The return is $\bigsqcup_{p||A|} \mathtt{B}_p$.

We involve some problems for associative rings. For ease we assume that all rings R are finite of characteristic p^e and specified with a basis $\mathtt{B}$ over $\mathbb{Z}_{p^e}$. To encode the multiplication in R we store structure constants $\{\lambda^z_{xy} \in \mathbb{Z}_{p^e} : x, y, z \in \mathtt{B}\}$ which are defined so that:

$$\left(\sum_{x\in\mathcal{X}} r_x x\right)\left(\sum_{y\in\mathcal{X}} s_y y\right) = \sum_{z\in\mathtt{B}}\left(\sum_{x,y\in\mathcal{X}} r_x \lambda^z_{xy} s_y\right) z$$

where, for all x and all y in $\mathtt{B}$, $r_x, s_y \in \mathbb{Z}_{p^e}$.

P. 2.31. Frame
Given: *an associative unital ring R,*
Return: *a frame of R.*

Frame has various nondeterministic solutions [4, 9] with astonishing speed. However, we need a deterministic solution such as in the work of Ronyai.

Theorem 2.32 (Ronyai [29])**.** *For rings R specified as an additive group in $\mathbb{G}_n$ with a basis and with structure constants with respect to the basis,* Frame *is solvable in polynomial-time in $p + n$ where $|R| = p^n$.*

Proof. First pass to $\mathbf{R} = R/pR$ and so create an algebra over the field $\mathbb{Z}_p$. Now [29, Theorem 2.7] gives a deterministic polynomial-time algorithm which finds a basis for the Jacobson radical of $\mathbf{R}$. This allows us to pass to $\mathbf{S} = \mathbf{R}/J(\mathbf{R})$, which is isomorphic to a direct product of matrix rings over finite fields. Finding the frame for $\mathbf{S}$ can be done by finding the minimal ideals $\mathcal{M}$ of $\mathbf{S}$ [29, Corollary 3.2]. Next, for each $M \in \mathcal{M}$, build an isomorphism $M \to M_n(\mathbb{F}_q)$ [29, Corollary 5.3] and choose a frame of idempotents from $M_n(\mathbb{F}_q)$ and let $\mathcal{E}_M$ be the pullback to M. Set $\mathcal{E} = \bigsqcup_{M\in\mathcal{M}} \mathcal{E}_M$ noting that $\mathcal{E}$ is a frame for S. Hence, use the power series of Lemma 2.21 to lift the frame $\mathcal{E}$ to a frame $\hat{\mathcal{E}}$ for R. □

With Theorem 2.32 we setup and solve a special instance of Theorem 1.1.

P. 2.33. Abelian.Remak-Ω-Decomposition
Given: *an abelian Ω-group A,*
Return: *a Remak Ω-decomposition for A.*

Corollary 2.34. Abelian.Remak-Ω-Decomposition *has a polynomial-time solution.*

Proof. Let $A \in \mathbb{G}^{\Omega}_n$ be abelian.

Algorithm. Use Primary-Decomposition to write A in a primary decomposition. For each prime p dividing $|A|$, let A_p be the p-primary component. Write a basis for $\operatorname{End} A_p$ (noting that $\operatorname{End} A_p$ is a checkered matrix ring determined completely by the Remak decomposition of A_p as a $\mathbb{Z}$-module [20, p. 196]) and use SOLVE to find a basis for $\operatorname{End}_\Omega A$. Finally, use FRAME to find a frame $\mathcal{E}_p$ for $\operatorname{End}_\Omega A_p$. Set $\mathcal{A}_p = \{Ae : e \in \mathcal{E}\}$. Return $\bigsqcup_{p||A|} \mathcal{A}_p$.

Correctness. Every direct Ω-decomposition of A corresponds to a set of pairwise orthogonal idempotents in $\operatorname{End}_\Omega A$ which sum to 1. Furthermore, Remak Ω-decomposition correspond to frames.

Timing. The polynomial-timing follows from Theorem 2.32 together with the observation that $p \leq n$ whenever $A \in \mathbb{G}_n$. □

Remark 2.35. In the context of groups of matrices our solution to ABELIAN.REMAK-Ω-DECOMPOSITION is impossible as it invokes integer factorization and MEMBER is a version of a discrete log problem in that case. The primes involved in the orders of matrix groups can be exponential in the input length and so these two routines are infeasible. For solvable matrix groups whose primes are bound and so called Γ_d-matrix groups the required problems in this section have polynomial-time solutions, cf. [17, 22].

P. 2.36. IRREDUCIBLE[29, Corollary 5.4]

Given: *an associative unital ring R, an abelian group V, and a homomorphism $\varphi : R \to \operatorname{End} V$,*
Return: *an irreducible R-submodule of V.*

As with the algorithm FRAME, there are nearly optimal nondeterministic methods for IRREDUCIBLE, for example, the MeatAxe [8, 10]; however, we are concerned here with a deterministic method solely.

P. 2.37. MINIMAL-Ω-NORMAL

Given: *an Ω-group G where Ω acts on G as automorphisms,*
Return: *a minimal $(\Omega \cup G)$-subgroup of G.*

Proposition 2.38. MINIMAL-Ω-NORMAL *has a polynomial-time solution.*

Proof. Let $G = (\mathtt{X} : \mathtt{R}) \in \mathbb{G}_n^\Omega$.

Algorithm. Use MINIMAL-NORMAL to compute a minimal normal subgroup N of G. Using MEMBER, run the following transitive closure: set $M := N$, then while there exists $w \in \Omega \cup \mathtt{X}$ such that $M^w \neq M$, set $N = \langle M, M^w \rangle$. Now $M = \langle N^{\Omega \cup G} \rangle$. If N is non-abelian then return M; otherwise, treat M as an $(\Omega \cup G)$-module and use IRREDUCIBLE to find an irreducible $(\Omega \cup G)$-submodule K of M. Return K.

Correctness. Note that $M = \langle N^{\Omega \cup G} \rangle = N N^{w_1} N^{w_2} \cdots N^{w_t}$ for some $w_1, \dots, w_t \in \langle \Omega\theta \rangle \ltimes G \leq \operatorname{Aut} G \ltimes G$. As N is minimal normal, so is each N^{w_i} and therefore M is a direct product of isomorphic simple groups. If N is non-abelian then the normal subgroups of M are its direct factors and furthermore, every direct factor F of M satisfies $M = \langle F^{\Omega \cup G} \rangle$. If N is abelian then $N \cong \mathbb{Z}_p^d$ for some prime p. A minimal $(\Omega \cup G)$-subgroup of N is therefore an irreducible $(\Omega \cup G)$-submodule of V.

Timing. First the algorithm executes a normal closure using the polynomial-time algorithm MEMBER. We test if N is abelian by computing the commutators of the generators. The final step is the polynomial-time algorithm IRREDUCIBLE. □

3. LIFTING, EXTENDING, AND MATCHING DIRECT DECOMPOSITIONS

We dedicate this section to understanding when a direct decomposition of a quotient or subgroup lifts or extends to a direct decomposition of the whole group.

Ultimately we plan these ideas for use in the algorithm for Theorem 1.1, but the questions have taken on independent intrigue. The highlights of this section are Theorems 3.6 and 3.28 and Corollaries 3.14 and 3.21.

Fix a short exact sequence of Ω-groups:

$$(3.1) \qquad \begin{tikzcd} 1 \arrow[r] & K \arrow[r, "i"] & G \arrow[r, "q"] & Q \arrow[r] & 1. \end{tikzcd}$$

With respect to (3.1) we study instances of the following problems.

Extend: for which direct $(\Omega \cup G)$-decomposition $\mathcal{K}$ of K, is there a Remak Ω-decomposition $\mathcal{R}$ of G such that $\mathcal{K}i = \mathcal{R} \cap (Ki)$.

Lift: for which direct $(\Omega \cup G)$-decomposition $\mathcal{Q}$ of Q, is there a Remak Ω-decomposition $\mathcal{R}$ of G such that $\mathcal{Q} = \mathcal{R}q$.

Match: for which pairs $(\mathcal{K}, \mathcal{Q})$ of direct $(\Omega \cup G)$-decompositions of K and Q respectively, is there a Remak Ω-decomposition of G which is an extension of $\mathcal{K}$ and a lift of $\mathcal{Q}$, i.e. $\mathcal{K}i = \mathcal{R} \cap (Ki)$ and $\mathcal{Q} = \mathcal{R}q$.

Finding direct decompositions which extend or lift is surprisingly easy (Theorem 3.6), but we have had only narrow success in finding matches. Crucial exceptions are p-groups of class 2 (Theorem 5.21) where the problem reduces to commutative ring theory.

3.1. Graded extensions.

In this section we place some reasonable parameters on the short exact sequences which we consider in the role of (3.1). This section depends mostly on the material of Sections 2.1–2.2.

Lemma 3.2. *Let G be a group with a direct Ω-decomposition $\mathcal{H}$. If X is an $(\Omega \cup G)$-subgroup of G and $X = \langle \mathcal{H} \cap X \rangle$, then*

(i) $\mathcal{H} \cap X$ is a direct Ω-decomposition of X,
(ii) $\mathcal{H}X/X$ is a direct Ω-decomposition of G/X,
(iii) $\mathcal{H} - \{H \in \mathcal{H} : H \leq X\}$, $\mathcal{H}X$, and $\mathcal{H}X/X$ are in a natural bijection, and
(iv) if Y is an $(\Omega \cup G)$-subgroup of G with $Y = \langle \mathcal{H} \cap Y \rangle$ then $\mathcal{H} \cap (X \cap Y) = \langle \mathcal{H} \cap (X \cap Y) \rangle$ and $\mathcal{H} \cap XY = \langle \mathcal{H} \cap XY \rangle$.

Proof. For (i), $(H \cap X) \cap \langle \mathcal{H} \cap X - \{H \cap X\} \rangle = 1$ for all $H \cap X \in \mathcal{H} \cap X$. For (ii), let $|\mathcal{H}| > 1$, take $H \in \mathcal{H}$, and set $J = \langle \mathcal{H} - \{H\} \rangle$. From (i): $HX \cap JX = (H \times (J \cap X)) \cap ((H \cap X) \times J) = (H \cap X) \times (J \cap X) = X$. For (iii), the functions $H \mapsto HX \mapsto HX/X$, for each $H \in \mathcal{H} - \{H \in \mathcal{H} : H \leq X\}$, suffice. Finally for (iv), let $g \in X \cap N$. So there are unique $h \in H$ and $k \in \langle \mathcal{H} - \{H\} \rangle$ with $g = hk$. By (i) and the uniqueness, we get that $h \in (H \cap X) \cap (H \cap Y)$ and $k \in \langle \mathcal{H} - \{H\} \rangle \cap (X \cap Y)$. So $g \in \langle \{H \cap (X \cap N), \langle \mathcal{H} - \{H\} \rangle \cap (X \cap Y)\} \rangle$. By induction on $|\mathcal{H}|$, $X \cap Y \leq \langle \mathcal{H} \cap (X \cap Y) \rangle \leq X \cap N$. The last argument is similar. □

We now specify which short exact sequence we consider.

Definition 3.3. A short exact sequence $1 \to K \overset{i}{\to} G \overset{q}{\to} Q \to 1$ of Ω-groups is Ω-*graded* if for all (finite) direct Ω-decomposition $\mathcal{H}$ of G, it follows that $Ki = \langle \mathcal{H} \cap (Ki) \rangle$. Also, if M is an $(\Omega \cup G)$-subgroup of G such that the canonical short exact sequence $1 \to M \to G \to G/M \to 1$ is Ω-graded then we say that M is Ω-graded.

Lemma 3.2 parts (i) and (ii) imply that every direct Ω-decomposition of G induces direct Ω-decompositions of K and Q whenever $1 \to K \overset{i}{\to} G \overset{q}{\to} Q \to 1$

$$\begin{tikzcd}
 & & 1 & 1 & \\
1 \arrow[r] & K \arrow[r, "i"] & G \arrow[r, "q"] \arrow[u] & Q \arrow[r] \arrow[u] & 1 \\
1 \arrow[r] & \hat{K} \arrow[r, "\hat{\imath}"] \arrow[u, "j"] & G \arrow[r, "\hat{q}"] \arrow[u, equal] & \hat{Q} \arrow[r] \arrow[u, "r"'] & 1 \\
 & 1 \arrow[u] & 1 \arrow[u] & &
\end{tikzcd}$$

Figure 1. A commutative diagram of Ω-groups which is exact and Ω-graded in all rows and all columns.

is Ω-graded. The universal quantifier in the definition of graded exact sequences may seem difficult to satisfy; nevertheless, in Section 3.3 we show many well-known subgroups are graded, for example the commutator subgroup.

Proposition 3.4. *(i) If M is an Ω-graded subgroup of G and N an $(\Omega \cup G)$-graded subgroup of M, then N is an Ω-graded subgroup of G.*

(ii) The set of Ω-graded subgroups of G is a modular sublattice of the lattice of $(\Omega \cup G)$-subgroups of G.

Proof. For (i), if $\mathcal{H}$ is a direct Ω-decomposition of G then by Lemma 3.2(i), $\mathcal{H} \cap M$ is direct Ω-decomposition of M and so $\mathcal{H} \cap N = (\mathcal{H} \cap M) \cap N$ is a direct Ω-decomposition of N. Also (ii) follows from Lemma 3.2(iv). □

Lemma 3.5. *For all Remak Ω-decomposition $\mathcal{H}$ and all direct Ω-decomposition $\mathcal{K}$ of G,*

(i) $\mathcal{H}M$ refines $\mathcal{K}M$ for all $(\Omega \cup G)$-subgroups $M \geq \zeta_1(G)$,

(ii) $\mathcal{H} \cap M$ refines $\mathcal{K} \cap M$ for all $(\Omega \cup G)$-subgroups $M \leq \gamma_2(G)$.

Proof. Let $\mathcal{T}$ be a Remak Ω-decomposition of G which refines $\mathcal{H}$. By Theorem 2.10, there is a $\varphi \in \mathrm{Aut}_{\Omega\cup G}\, G$ such that $\mathcal{R}\varphi = \mathcal{T}$. Form (2.1) it follows that $\mathcal{R}\zeta_1(G) = \mathcal{R}\zeta_1(G)\varphi = \mathcal{T}\zeta_1(G)$ and $\mathcal{R} \cap \gamma_2(G) = (\mathcal{R} \cap \gamma_2(G))\varphi = \mathcal{T} \cap \gamma_2(G)$. □

Theorem 3.6. *Given the commutative diagram in Figure 1 which is exact and Ω-graded in all rows and all columns, the following hold.*

(i) If $\zeta_1(\hat{Q})r = 1$ then for every Remak Ω-decomposition $\hat{\mathcal{Q}}$ of $\hat{Q}$ and every Remak Ω-decomposition $\mathcal{H}$ of G, $\mathcal{Q} := \hat{\mathcal{Q}}r$ refines $\mathcal{H}q$. In particular, $\mathcal{H}$ lifts a partition of $\mathcal{Q}$ which is unique to (G, i, q).

(ii) If $\gamma_2(K) \leq \hat{K}j$ then for every Remak $(\Omega \cup G)$-decomposition $\mathcal{K}$ of K and every Remak Ω-decomposition $\mathcal{H}$ of G, $\mathcal{K}i \cap \hat{K}\hat{\imath}$ refines $\mathcal{H} \cap \left(\hat{K}\hat{\imath}\right)$. In particular, $\mathcal{H}$ extends a partition of $\hat{\mathcal{K}} := (\mathcal{K} \cap \hat{K}j)j^{-1}$ which is unique to $(G, \hat{\imath}, \hat{q})$.

Proof. Fix a Remak Ω-decomposition $\mathcal{H}$ of G.

As $\hat{K}$ and K are Ω-graded, it follows that $\mathcal{H}\hat{q}$ is a direct Ω-decompositions of $\hat{Q}$ (Lemma 3.2(ii)). Let $\mathcal{T}$ be a Remak Ω-decomposition of $\hat{Q}$ which refines $\mathcal{H}\hat{q}$.

By Lemma 3.5(i), $\hat{\mathcal{Q}}\zeta_1(\hat{Q}) = \mathcal{T}\zeta_1(\hat{Q})$ and so $\hat{\mathcal{Q}}r = \mathcal{T}r$. Therefore, $\mathcal{Q} := \hat{\mathcal{Q}}r$ refines $\mathcal{H}\hat{q}r = \mathcal{H}q$. That proves (i).

To prove (ii), by Lemma 3.2(i) we have that $\mathcal{H} \cap (Ki)$ is a direct $(\Omega \cup G)$-decompositions of Ki. Let $\mathcal{T}$ be a Remak $(\Omega \cup G)$-decomposition of Ki which refines $\mathcal{H} \cap (Ki)$. By Lemma 3.5(ii), $\hat{\mathcal{K}} = \mathcal{K}i \cap (\hat{K}\hat{i}) = \mathcal{T} \cap \left(\hat{K}\hat{i}\right)$. Therefore, $\mathcal{K}i \cap \left(\hat{K}\hat{i}\right)$ refines $\mathcal{H} \cap \left(\hat{K}\hat{i}\right)$. □

Theorem 3.6 implies the following special setting where the match problem can be answered. This is the only instance we know where the matching problem can be solved without considering the cohomology of the extension.

Corollary 3.7. *If $1 \to K \to G \to Q \to 1$ is a Ω-graded short exact sequence where $K = \gamma_2(K)$ and $\zeta_1(Q) = 1$; then for every Remak $(\Omega \cup G)$-decomposition $\mathcal{K}$ of K and $\mathcal{Q}$ of Q, there are partitions $[\mathcal{K}]$ and $[\mathcal{Q}]$ unique to the short exact sequence such that every Remak Ω-decomposition $\mathcal{H}$ of G matches $([\mathcal{K}], [\mathcal{Q}])$.*

3.2. **Direct classes, and separated and refined decompositions.** In this section we begin our work to consider the extension, lifting, and matching problems in a constructive fashion. We introduce classes of groups which are closed to direct products and direct decompositions and show how to use these classes to control the exchange of direct factors.

Definition 3.8. A class $\mathfrak{X}$ (or $\mathfrak{X}^{\Omega}$ if context demands) of Ω-groups is *direct* if $1 \in \mathfrak{X}$, and $\mathfrak{X}$ is closed to Ω-isomorphisms, as well as the following:

(i) if $G \in \mathfrak{X}$ and H is a direct Ω-factor of G, then $H \in \mathfrak{X}$, and
(ii) if $H, K \in \mathfrak{X}$ then $H \times K \in \mathfrak{X}$.

Every variety of Ω-groups is a direct class by Theorem 2.13 and to specify the finite groups in a direct class it is sufficient to specify the directly Ω-indecomposable group it contains. However, in practical terms there are few settings where the directly Ω-indecomposable groups are known.

Definition 3.9. A direct Ω-decomposition $\mathcal{H}$ is $\mathfrak{X}$*-separated* if for each $H \in \mathcal{H} - \mathfrak{X}$, if H has a direct Ω-factor K, then $K \notin \mathfrak{X}$. If additionally every member of $\mathcal{H} \cap \mathfrak{X}$ is directly Ω-indecomposable, then $\mathcal{H}$ is $\mathfrak{X}$*-refined.*

Proposition 3.10. *Suppose that $\mathfrak{X}$ is a direct class of Ω-groups, G an Ω-group, and $\mathcal{H}$ a direct Ω-decomposition of G. The following hold.*

(i) $\langle \mathcal{H} \cap \mathfrak{X} \rangle \in \mathfrak{X}$.
(ii) If $\mathcal{H}$ is $\mathfrak{X}$-separated and $\mathcal{K}$ is a direct Ω-decomposition of G which refines $\mathcal{H}$, then $\mathcal{K}$ is $\mathfrak{X}$-separated.
(iii) $\mathcal{H}$ is a $\mathfrak{X}$-separated if, and only if, $\{\langle \mathcal{H} - \mathfrak{X} \rangle, \langle \mathcal{H} \cap \mathfrak{X} \rangle\}$ is $\mathfrak{X}$-separated.
(iv) Every Remak Ω-decomposition is $\mathfrak{X}$-refined.
(v) If $\mathcal{H}$ and $\mathcal{K}$ are $\mathfrak{X}$-separated direct Ω-decompositions of G then $(\mathcal{H} - \mathfrak{X}) \sqcup (\mathcal{K} \cap \mathfrak{X})$ is an $\mathfrak{X}$-separated direct Ω-decomposition of G.

Proof. First, (i) follows as $\mathfrak{X}$ is closed to direct Ω-products.

For (ii), notice that a direct Ω-factor of a $K \in \mathcal{K}$ is also a direct Ω-factor of the unique $H \in \mathcal{H}$ where $K \leq H$.

For (iii), the reverse direction follows from (ii). For the forward direction, let K be a direct Ω-factor of $\langle \mathcal{H} - \mathfrak{X} \rangle$. Because $\mathfrak{X}$ is closed to direct Ω-factors, if $K \in \mathfrak{X}$

then so is every directly Ω-indecomposable direct Ω-factor of K, and so we insist that K is directly Ω-indecomposable. Therefore K lies in a Remak Ω-decomposition of $\langle \mathcal{H} - \mathfrak{X} \rangle$. Let $\mathcal{R}$ be a Remak Ω-decomposition of $\langle \mathcal{H} - \mathfrak{X} \rangle$ which refines $\mathcal{H} - \mathfrak{X}$. By Theorem 2.10 there is a $\varphi \in \mathrm{Aut}_{\Omega \cup G}\langle \mathcal{H} - \mathfrak{X} \rangle$ such that $K\varphi \in \mathcal{R}$ and so $K\varphi$ is a direct Ω-factor of the unique $H \in \mathcal{H}$ where $K\varphi \leq H$. As $\mathcal{H}$ is $\mathfrak{X}$-separated and $K\varphi$ is a direct Ω-factor of $H \in \mathcal{H}$, it follows that $K\varphi \notin \mathfrak{X}$. Thus, $K \notin \mathfrak{X}$ and $\{\langle \mathcal{H} - \mathfrak{X} \rangle, \langle \mathcal{H} \cap \mathfrak{X} \rangle\}$ is $\mathfrak{X}$-separated.

For (iv), note that elements of a Remak Ω-decomposition have no proper direct Ω-factors.

Finally for (v), let $\mathcal{R}$ and $\mathcal{T}$ be a Remak Ω-decompositions of G which refine $\mathcal{H}$ and $\mathcal{K}$ respectively. Set $\mathcal{U} = \{R \in \mathcal{R} : R \leq \langle \mathcal{H} \cap \mathfrak{X} \rangle\}$. By Theorem 2.10 there is a $\varphi \in \mathrm{Aut}_{\Omega \cup G} G$ such that $\mathcal{U}\varphi \subseteq \mathcal{T}$ and $\mathcal{R}\varphi = (\mathcal{R} - \mathcal{U}) \sqcup \mathcal{U}\varphi$. As $\mathfrak{X}$ is closed to isomorphisms, it follows that $\mathcal{U}\varphi \subseteq \mathcal{T} \cap \mathfrak{X}$. As $\mathcal{H}$ is $\mathfrak{X}$-separated, $\mathcal{U} = \mathcal{R} \cap \mathfrak{X}$. As $\mathrm{Aut}_{\Omega \cup G} G$ is transitive on the set of all Remak Ω-decompositions of G (Theorem 2.10), we have that $|\mathcal{T} \cap \mathfrak{X}| = |\mathcal{R} \cap \mathfrak{X}| = |\mathcal{U}\varphi|$. In particular, $\mathcal{U}\varphi = \mathcal{T} \cap \mathfrak{X} = \{T \in \mathcal{T} : T \leq \langle \mathcal{K} \cap \mathfrak{X} \rangle\}$. Hence, $\mathcal{R}\varphi$ refines $(\mathcal{H} - \mathfrak{X}) \sqcup (\mathcal{K} \cap \mathfrak{X})$ and so the latter is a direct Ω-decomposition. □

3.3. **Up grades and down grades.**

Here we introduce a companion subgroup to a direct class $\mathfrak{X}$ of Ω-groups. These groups specify the kernels we consider in the problems of extending and lifting in concrete settings.

Definition 3.11. An *up Ω-grader* (resp. *down Ω-grader*) for a direct class $\mathfrak{X}$ of Ω-groups is a function $G \mapsto \mathfrak{X}(G)$ of finite Ω-groups G where $\mathfrak{X}(G) \in \mathfrak{X}$ (resp. $G/\mathfrak{X}(G) \in \mathfrak{X}$) and such that the following hold.

(i) If $G \in \mathfrak{X}$ then $\mathfrak{X}(G) = G$ (resp. $\mathfrak{X}(G) = 1$).
(ii) $\mathfrak{X}(G)$ is an Ω-graded subgroup of G.
(iii) For direct Ω-factor H of G, $\mathfrak{X}(H) = H \cap \mathfrak{X}(G)$.

The pair $(\mathfrak{X}, G \mapsto \mathfrak{X}(G))$ is an up/down *Ω-grading pair.*

If $(\mathfrak{X}, G \mapsto \mathfrak{X}(G))$ is an Ω-grading pair then we have $\mathfrak{X}(H \times K) = \mathfrak{X}(H) \times \mathfrak{X}(K)$. First we concentrate on general and useful instances of grading pairs.

Proposition 3.12. *The marginal subgroup of a variety of Ω-groups is an up Ω-grader and the verbal subgroup is a down Ω-grader for the variety.*

Proof. Let $\mathfrak{V} = \mathfrak{V}^{\Omega}$ be a variety of Ω-groups with defining laws $\mathtt{W}$ and fix an Ω-group G. As the marginal function is idempotent, (2.20) implies that $\mathfrak{V}^*(G) \in \mathfrak{V}$ and that if $G \in \mathfrak{V}$ then $G = \mathfrak{V}^*(G)$. Similarly, verbal subgroups are radical so that by (2.19) we have $G/\mathfrak{V}(G) \in \mathfrak{V}$ and when $G \in \mathfrak{V}$ then $\mathfrak{V}(G) = 1$. It remains to show properties (ii) and (iii) of Definition 3.11.

Fix a direct Ω-decomposition $\mathcal{H}$ of G, fix an $H \in \mathcal{H}$, and set $K = \langle \mathcal{H} - \{H\} \rangle$. For each $f \in G^{\mathtt{X}} = (H \times K)^{\mathtt{X}}$ there are unique $f_H \in H^{\mathtt{X}}$ and $f_K \in K^{\mathtt{X}}$ such that $f = f_H f_K$. Thus, for all $w \in \mathtt{W}$, $w(f) = w(f_H)w(f_K)$ and so $w(H \times K) = w(H) \times w(K)$. Hence, $\mathfrak{V}(H \times K) = \mathfrak{V}(H) \times \mathfrak{V}(K)$. By induction on $|\mathcal{H}|$, $\mathcal{H} \cap \mathfrak{V}(G) = \{\mathfrak{V}(H) : H \in \mathcal{H}\}$ is a direct Ω-decomposition of $\mathfrak{V}(G)$. So $\mathfrak{V}(G)$ is a down Ω-grader.

For the marginal case, for all $f' \in \langle (h,k) \rangle^{\mathtt{X}} \leq (H \times K)^{\mathtt{X}} = G^{\mathtt{X}}$ and all $f \in G^{\mathtt{X}}$, again there exist unique $f_H, f'_H \in H^{\mathtt{X}}$ and $f_K, f'_K \in K^{\mathtt{X}}$ such that $f = f_H f_K$ and $f' = f'_H f'_K$. Also, $w(ff') = w(f)$ if, and only if, $w(f_H f'_H) = w(f_H)$ and $w(f_K f'_K) = w(f_K)$. Thus, $w^*(H \times K) = w^*(H) \times w^*(K)$. Hence, $\mathfrak{V}^*(H \times K) =$

$\mathfrak{V}^*(H)\times\mathfrak{V}^*(K)$ and by induction $\mathcal{H}\cap\mathfrak{V}^*(G)$ is a direct Ω-decomposition of $\mathfrak{V}^*(G)$. Thus, $\mathfrak{V}^*(G)$ is an up Ω-grader. □

Remark 3.13. There are examples of infinite direct decompositions $\mathcal{H}$ of infinite groups G and varieties $\mathfrak{V}$, where $\mathfrak{V}(G)\neq\langle\mathcal{H}\cap\mathfrak{V}(G)\rangle$ [1]. However, our definition of grading purposefully avoids infinite direct decompositions.

With Proposition 3.12 we get a simultaneous proof of some individually evident examples of direct ascenders and descenders.

Corollary 3.14. *Following the notation of Example 2.18 we have the following.*

(i) The class $\mathfrak{N}_c$ of nilpotent groups of class at most c is a direct class with up grader $G\mapsto\zeta_c(G)$ and down grader $G\mapsto\gamma_c(G)$.

(ii) The class $\mathfrak{S}_d$ of solvable groups of derived length at most d is a direct class with up grader $G\mapsto(\delta_d)^*(G)$ and down grader $G\mapsto G^{(d)}$.

(iii) For each prime p the class $\mathfrak{V}([x,y]z^p)$ of elementary abelian p-groups is a direct class with up grader $G\mapsto\Omega_1(\zeta_1(G))$ and down grader $G\mapsto[G,G]\mho_1(G)$.[1]

We also wish to include direct classes $\mathfrak{N}:=\bigcup_{c\in\mathbb{N}}\mathfrak{N}_c$ and $\mathfrak{S}:=\bigcup_{d\in\mathbb{N}}\mathfrak{S}_d$. These classes are not varieties (they are not closed to infinite direct products as required by Theorem 2.13). Therefore, we must consider alternatives to verbal and marginal groups for appropriate graders. Our approach mimics the definitions $G\mapsto O_p(G)$ and $G\mapsto O^p(G)$. We explain the up grader case solely.

Definition 3.15. For a class $\mathfrak{X}$, the $\mathfrak{X}$-core, $O_{\mathfrak{X}}(G)$, of a finite group G is the intersection of all maximal $(\Omega\cup G)$-subgroups contained in $\mathfrak{X}$.

If $\mathfrak{V}$ is a union of a chain $\mathfrak{V}_0\subseteq\mathfrak{V}_1\subseteq\cdots$ of varieties then $1\in\mathfrak{V}$, and so the maximal $(\Omega\cup G)$-subgroups of a group G contained in $\mathfrak{V}$ is nonempty. Also $\mathfrak{V}$ is closed to subgroups so that $O_{\mathfrak{V}}(G)\in\mathfrak{V}$.

Example 3.16. (i) $O_{\mathfrak{A}}(G)$ is the intersection of all maximal normal abelian subgroups of G. Generally there can be any number of maximal normal abelian subgroups of G so $O_{\mathfrak{A}}(G)$ is not a trivial intersection.

(ii) $O_{\mathfrak{N}_c}(G)$ is the intersection of all maximal normal nilpotent subgroups of G with class at most c. As in (i), this need not be a trivial intersection. However, if $c>\log|G|$ then all nilpotent subgroups of G have class at most c and therefore $O_{\mathfrak{N}}(G)=O_{\mathfrak{N}_c}(G)$ is the Fitting subgroup of G: the unique maximal normal nilpotent subgroup of G.

(iii) $O_{\mathfrak{S}_d}(G)$, $d>\log|G|$, is the unique maximal normal solvable subgroup of G, i.e.: the solvable radical $O_{\mathfrak{S}}(G)$ of G.

Lemma 3.17. *Let $\mathfrak{V}$ be a group variety of Ω-groups and G an Ω-group. If H is a $\mathfrak{V}$-subgroup of G then so is $\mathfrak{V}^*(G)H$, that is: $\mathfrak{V}^*(G)H\in\mathfrak{V}$.*

Proof. Let W be a set of defining laws for $\mathfrak{V}$. Let $f'\in G^{\mathtt{X}}$ with $\operatorname{im}f\subseteq\mathfrak{V}^*(G)H$. Thus, for all $w\in\mathtt{W}$, there is a decomposition $f=f'f''$ where $\operatorname{im}f'\subseteq w^*(G)$ and $\operatorname{im}f''\subseteq H$. As $w^*(G)$ is marginal to G it is marginal to H and so $w(f)=w(f'')$. As $H\in\mathfrak{V}$, $w(f'')=1$. Thus, $w(f)=1$ and so $w(w^*(G)H)=1$. It follows that $\mathfrak{V}^*(G)H\in\mathfrak{V}$. □

[1] Here $\Omega_1(X)=\langle x\in X : x^p=1\rangle$ and $\mho_1(X)=\langle x^p : x\in G\rangle$, which are traditional notations having nothing to do with our use of Ω for operators elsewhere.

Proposition 3.18. *If $\mathfrak{V}$ is a group variety of Ω-groups and G an Ω-group, then*

(i) $\mathfrak{V}^*(G) \leq O_{\mathfrak{V}}(G)$, *and*

(ii) if M is an $(\Omega \cup G)$-subgroup then $O_{\mathfrak{V}}(G)O_{\mathfrak{V}}(M)$ is an $(\Omega \cup G)$-subgroup contained in $\mathfrak{V}$.

Proof. (i). By Lemma 3.17, every maximal normal $\mathfrak{V}$-subgroup of G contains $\mathfrak{V}^*(G)$.

(ii). As $M \trianglelefteq G$ and $O_{\mathfrak{V}}(M)$ is characteristic in M, it follows that $O_{\mathfrak{V}}(M)$ is a normal $\mathfrak{V}$-subgroup of G. Thus, $O_{\mathfrak{V}}(M)$ lies in a maximal normal $\mathfrak{V}$-subgroup N of G. As $O_{\mathfrak{V}}(G) \leq N$ we have $O_{\mathfrak{V}}(G)O_{\mathfrak{V}}(M) \leq N \in \mathfrak{V}$. As $\mathfrak{V}$ is closed to subgroups, it follows that $O_{\mathfrak{V}}(G)O_{\mathfrak{V}}(M)$ is in $\mathfrak{V}$. □

Remark 3.19. It is possible to have $\mathfrak{V}^*(G) < O_{\mathfrak{V}}(G)$. For instance, with $G = S_3 \times C_2$ and the class $\mathfrak{A}$ of abelian groups, the $\mathfrak{A}$-marginal subgroup is the center $1 \times C_2$, whereas the $\mathfrak{A}$-core is $C_3 \times C_2$.

Proposition 3.20. *Let G be a finite group with a direct decomposition $\mathcal{H}$. If $\mathfrak{V}$ is a group variety then*

$$\mathcal{H} \cap O_{\mathfrak{V}}(G) = \{O_{\mathfrak{V}}(H) : H \in \mathcal{H}\}$$

and this is a direct decomposition of $O_{\mathfrak{V}}(G)$. In particular, $G \mapsto O_{\mathfrak{V}}(G)$ is an up Ω-grader. Furthermore, if $\mathfrak{V}$ is a union of a chain $\mathfrak{V}_0 \subseteq \mathfrak{V}_1 \subseteq \cdots$ of group varieties then $O_{\mathfrak{V}}(G)$ is an up Ω-grader.

Proof. Let $H \in \mathcal{H}$ and $K := \langle \mathcal{H} - \{H\} \rangle$. Let M be a maximal normal $\mathfrak{V}$-subgroup of $G = H \times K$. Let M_H be the projection of M to the H-component. As $\mathfrak{V}$ is closed to homomorphic images, $M_H \in \mathfrak{V}$. Furthermore, $M_H \trianglelefteq H$ so there is a maximal normal $\mathfrak{V}$-subgroup N of H such that $M_H \leq N$.

We claim that $MN \in \mathfrak{V}$.

As $G = H \times K$, every $g \in M$ has the unique form $g = hk$, $h \in H$, $k \in K$. As M_H is the projection of M to H, $h \in M_H \leq N$. Thus, $g, h \in MN$ so $k \in MN$. Thus, $MN = N \times M_K$, where M_K is the projection of M to K. Now let $\mathfrak{V} = \mathfrak{V}(w)$. For each $f : X \to MN$, write $f = f_N \times f_K$ where $f_N : X \to N$ and $f_K : X \to M_K$. Hence, $w(f) = w(f_N \times f_K) = w(f_N) \times w(f_K)$. However, $w(N) = 1$ and $w(M_K) = 1$ as $N, M_K \in \mathfrak{V}$. Thus, $w(f) = 1$, which proves that $w(MN) = 1$. So $MN \in \mathfrak{V}$ as claimed.

As M is a maximal normal $\mathfrak{V}$-subgroup of G, $M = MN$ and $N = M_H$. Hence, $H \cap M = N$ is a maximal normal $\mathfrak{V}$-subgroup of H. So we have characterized the maximal normal $\mathfrak{V}$-subgroups of G as the direct products of maximal normal $\mathfrak{V}$-subgroups of members $H \in \mathcal{H}$. Thus, $\mathcal{H} \cap O_{\mathfrak{V}}(G) = \{O_{\mathfrak{V}}(H) : H \in \mathcal{H}\}$ and this generates $O_{\mathfrak{V}}(G)$. By Lemma 3.2, $\mathcal{H} \cap O_{\mathfrak{V}}(G)$ is a direct decomposition of $O_{\mathfrak{V}}(G)$. □

Corollary 3.21. *(i) The class $\mathfrak{N}$ of nilpotent groups is a direct class and $G \mapsto O_{\mathfrak{N}}(G)$ (the Fitting subgroup) is up grader.*

(ii) The class $\mathfrak{S}$ of solvable groups is a direct class and $G \mapsto O_{\mathfrak{S}}(G)$ (the solvable radical) is an up grader.

Proof. For a finite group G, the Fitting subgroup is the $\mathfrak{N}_c$-core where $c > |G|$. Likewise, the solvable radical is the $\mathfrak{S}_c$-core for $d > |G|$. The rest follows from Proposition 3.20. □

We now turn our attention away from examples of grading pairs and focus on their uses. In particular it is for the following "local-global" property which clarifies, in the up grader case, when a direct factor of a subgroup is also a direct factor of the whole group.

Proposition 3.22. *Let $G \mapsto \mathfrak{X}(G)$ be an up Ω-grader for a direct class $\mathfrak{X}$ of Ω-groups and let G be an Ω-group. If H is an $(\Omega \cup G)$-subgroup of G and the following hold:*

(a) for some direct Ω-factor R of G, $H\mathfrak{X}(G) = R\mathfrak{X}(G) > \mathfrak{X}(G)$, and

(b) H lies in an $\mathfrak{X}$-separated direct $(\Omega \cup G)$-decomposition of $H\mathfrak{X}(G)$;

then H is a direct Ω-factor of G.

Proof. By (a) there is a direct $(\Omega \cup G)$-complement C in G to R. Also $\mathfrak{X}(G) = \mathfrak{X}(R) \times \mathfrak{X}(C)$, as $\mathfrak{X}(G)$ is Ω-graded. Hence, $R\mathfrak{X}(G) = R \times \mathfrak{X}(C)$. By (b), there is an $\mathfrak{X}$-separated direct Ω-decomposition $\mathcal{H}$ of $H\mathfrak{X}(G)$ such that $H \in \mathcal{H}$. As $H\mathfrak{X}(G) > \mathfrak{X}(G)$ it follows that $H \notin \mathfrak{X}$ and so by Lemma 3.2(iii), $\mathcal{H} - \mathfrak{X} = \{H\}$ and $X = \langle \mathcal{H} \cap \mathfrak{X} \rangle \in \mathfrak{X}$. So

$$R \times \mathfrak{X}(C) = R\mathfrak{X}(G) = H\mathfrak{X}(G) = H \times X.$$

Let $\mathcal{A}$ be Remak $(\Omega \cup G)$-decomposition of R. Since $\mathfrak{X}(C) \in \mathfrak{X}$, $\mathcal{A} \sqcup \{\mathfrak{X}(C)\}$ is an $\mathfrak{X}$-separated direct $(\Omega \cup G)$-decomposition of $R\mathfrak{X}(G)$. By Proposition 3.10(v),

$$\mathcal{C} = \{H\} \sqcup \{\mathfrak{X}(C)\} \sqcup (\mathcal{A} \cap \mathfrak{X})$$

is an $\mathfrak{X}$-separated direct $(\Omega \cup G)$-decomposition of $R\mathfrak{X}(G)$, and we note that $\{H\} = \mathcal{C} - \mathfrak{X}$. We claim that $\{H, C\} \sqcup (\mathcal{A} \cup \mathfrak{X})$ is a direct Ω-decomposition of G. Indeed, $H \cap \langle C, \mathcal{A} \cap \mathfrak{X} \rangle \leq R\mathfrak{X}(G) \cap C\mathfrak{X}(G) = \mathfrak{X}(G)$ and so $H \cap \langle C, \mathcal{A} \cap \mathfrak{X} \rangle = H \cap \langle \mathfrak{X}(C), \mathcal{A} \cap \mathfrak{X} \rangle = 1$. Also, $\mathfrak{X}(C) \leq \langle H, C, \mathcal{A} \cap \mathfrak{X} \rangle$ thus $\langle H, C, \mathcal{A} \cap \mathfrak{X} \rangle = G$. As the members of $\{H, C\} \sqcup (\mathcal{A} \cap \mathfrak{X})$ are $(\Omega \cup G)$-subgroups we have proved the claim. In particular, H is a direct Ω-factor of G. □

3.4. **Direct chains.** In Theorem 3.6 we specified conditions under which any direct decomposition of an appropriate subgroup, resp. quotient, led to a solution of the extension (resp. lifting) problem. However, within that theorem we see that it is not the direct decomposition of the subgroup (resp. quotient group) which can be extended (resp. lifted). Instead it a some unique partition of the direct decomposition. Finding the correct partition by trial and error is an exponentially sized problem. To avoid this we outline a data structure which enables a greedy algorithm to find this unique partition. The algorithm itself is given in Section 4.2. The key result of this section is Theorem 3.28.

Throughout this section we suppose that $G \to \mathfrak{X}(G)$ is an (up) Ω-grader for a direct class $\mathfrak{X}$.

Definition 3.23. A *direct chain* is a proper chain $\mathcal{L}$ of $(\Omega \cup G)$-subgroups starting at $\mathfrak{X}(G)$ and ending at G, and where there is a direct Ω-decomposition $\mathcal{R}$ of G with:

(i) for all $L \in \mathcal{L}$, $L = \langle \mathcal{R} \cap L \rangle$, and

(ii) for each $L \in \mathcal{L} - \{G\}$, there is a unique $R \in \mathcal{R}$ such that the successor $M \in \mathcal{L}$ to L satisfies: $R\mathfrak{X}(G) \cap L \neq R\mathfrak{X}(G) \cap M$. We call R the *direction of L*.

We call $\mathcal{R}$ a set of directions for $\mathcal{L}$.

If $\mathcal{L}$ is a direct chain with directions $\mathcal{R}$, then for all $L \in \mathcal{L}$, $\mathcal{R} \cap L$ is a direct Ω-decomposition of L (Lemma 3.2(i)). When working with direct chains it helps to remember that for all $(\Omega \cup G)$-subgroups L and R of G, if $\mathfrak{X}(G) \leq L$, then $(R \cap L)\mathfrak{X}(G) = R\mathfrak{X}(G) \cap L$. Also, if $\mathfrak{X}(G) \leq L < M \leq G$, $L = \langle \mathcal{R} \cap L \rangle$ and $M = \langle \mathcal{R} \cap M \rangle$, and

$$\forall R \in \mathcal{R} - \mathfrak{X}, \qquad R\mathfrak{X}(G) \cap L = R\mathfrak{X}(G) \cap M \tag{3.24}$$

then $L = \langle \mathcal{R} \cap L \rangle = \langle \mathcal{R} \cap L, \mathfrak{X}(G) \rangle = \langle \mathcal{R} \cap M, \mathfrak{X}(G) \rangle = \langle \mathcal{R} \cap M \rangle = M$. Therefore, it suffices to show there is at most one $R \in \mathcal{R} - \mathfrak{X}$ such that $R\mathfrak{X}(G) \cap L \neq R\mathfrak{X}(G) \cap M$.

Lemma 3.25. *Suppose that $\mathcal{H} = \mathcal{H}\mathfrak{X}(G)$ is an $(\Omega \cup G)$-decomposition of G such that $\mathcal{H}$ refines $\mathcal{R}\mathfrak{X}(G)$, for a direct Ω-decomposition $\mathcal{R}$. It follows that, if $L = \langle \mathcal{J}, \mathfrak{X}(G) \rangle$, for some $\mathcal{J} \subseteq \mathcal{H}$, then $L = \langle \mathcal{R} \cap L \rangle$.*

Proof. As $\mathfrak{X}(G) \leq L$, for each $R \in \mathcal{R}$, $R \cap \mathfrak{X}(G) \leq R \cap L$. As $\mathfrak{X}(G)$ is $(\Omega \cup G)$-graded, $\mathfrak{X}(G) = \langle \mathcal{R} \cap \mathfrak{X}(G) \rangle$. Thus, $\mathfrak{X}(G) \leq \langle \mathcal{R} \cap L \rangle$. Also, $\mathcal{H}$ refines $\mathcal{R}\mathfrak{X}(G)$. Thus, for each $J \in \mathcal{J} \subseteq \mathcal{H}$ there is a unique $R \in \mathcal{R} - \{R \in \mathcal{R} : R \leq \mathfrak{X}(G)\}$ such that $J \leq R\mathfrak{X}(G)$. As $L = \langle \mathcal{J}, \mathfrak{X}(G) \rangle$, $J \leq L$ and so $J \leq R\mathfrak{X}(G) \cap L = (R \cap L)\mathfrak{X}(G)$. Now $R \cap L, \mathfrak{X}(G) \leq \langle \mathcal{R} \cap L \rangle$ thus $J \leq \langle \mathcal{R} \cap L \rangle$. Hence $L = \langle \mathcal{J}, \mathfrak{X}(G) \rangle \leq \langle \mathcal{R} \cap L \rangle \leq L$. □

Lemma 3.26. *If $\mathcal{H}$ is an $(\Omega \cup G)$-decomposition of G and $\mathcal{R}$ a direct $(\Omega \cup G)$-decomposition of G such that $\mathcal{H} = \mathcal{H}\mathfrak{X}(G)$ refines $\mathcal{R}\mathfrak{X}(G)$, then for all $\mathcal{J} \subset \mathcal{H}$ and all $H \in \mathcal{H} - \mathcal{J}$, there is a unique $R \in \mathcal{R}$ such that $H \leq R\mathfrak{X}(G)$ and*

$$\langle \mathcal{R} - \{R\} \rangle \mathfrak{X}(G) \cap \langle H, \mathcal{J}, \mathfrak{X}(G) \rangle = \langle \mathcal{R} - \{R\} \rangle \mathfrak{X}(G) \cap \langle \mathcal{J}, \mathfrak{X}(G) \rangle.$$

Proof. Fix $\mathcal{J} \subseteq \mathcal{H}$ and $H \in \mathcal{H} - \mathcal{J}$. By the definition of refinement there is a unique $R \in \mathcal{R}$ such that $H \leq R\mathfrak{X}(G)$. Set $J = \langle \mathcal{J}, \mathfrak{X}(G) \rangle$ and $C = \langle \mathcal{R} - \{R\} \rangle$. By Lemma 3.25, $\mathcal{R} \cap HJ$ and $\mathcal{R} \cap J$ are direct $(\Omega \cup G)$-decompositions of HJ and J respectively. As $J = (R \cap J) \times (C \cap J)$ and $\mathfrak{X}(G) \leq J$, we get that $J = (R\mathfrak{X}(G) \cap J)(C\mathfrak{X}(G) \cap J)$. Also, $\mathfrak{X}(G)$ is $(\Omega \cup G)$-graded; hence, by Lemma 3.2(ii), $G/\mathfrak{X}(G) = R\mathfrak{X}(G)/\mathfrak{X}(G) \times C\mathfrak{X}(G)/\mathfrak{X}(G)$ and $C\mathfrak{X}(G) \cap R\mathfrak{X}(G) = \mathfrak{X}(G)$.

Combining the modular law with $\mathfrak{X}(G) \leq H \leq R\mathfrak{X}(G)$ and $R\mathfrak{X}(G) \cap C\mathfrak{X}(G) = \mathfrak{X}(G)$ we have that

$$\begin{aligned} C\mathfrak{X}(G) \cap HJ &= C\mathfrak{X}(G) \cap \Big(H(R\mathfrak{X}(G) \cap J) \cdot (C\mathfrak{X}(G) \cap J) \Big) \\ &= \Big(C\mathfrak{X}(G) \cap H(R\mathfrak{X}(G) \cap J) \Big) (C\mathfrak{X}(G) \cap J) \\ &= (C\mathfrak{X}(G) \cap R\mathfrak{X}(G) \cap HJ)(C\mathfrak{X}(G) \cap J) \\ &= \mathfrak{X}(G)(C\mathfrak{X}(G) \cap J) = C\mathfrak{X}(G) \cap J. \end{aligned}$$

Thus, $C\mathfrak{X}(G) \cap HJ = C\mathfrak{X}(G) \cap J$. □

Proposition 3.27. *If $\mathcal{H} = \mathcal{H}\mathfrak{X}(G)$ is an $(\Omega \cup G)$-decomposition of G and $\mathcal{R}$ is a direct Ω-decomposition of G such that $\mathcal{H}$ refines $\mathcal{R}\mathfrak{X}(G)$, then every maximal proper chain $\mathscr{C}$ of subsets of $\mathcal{H}$ induces a direct chain $\{\langle \mathcal{C}, \mathfrak{X}(G) \rangle : \mathcal{C} \in \mathscr{C}\}$.*

Proof. For each $\mathcal{C} \subseteq \mathcal{H}$, by Lemma 3.25, $\langle \mathcal{C} \rangle = \big\langle \mathcal{R} \cap \langle \mathcal{C} \rangle \big\rangle$. The rest follows from Lemma 3.26. □

The following Theorem 3.28 is a critical component of the proof of the algorithm for Theorem 1.1, specifically in proving Theorem 4.13. What it says is that we can proceed through any direct chain as the $\mathfrak{X}$-separated direct decompositions of lower terms in the chain induce direct factors of the next term in the chain, and in a predictable manner.

Theorem 3.28. *If $\mathcal{L}$ is a direct chain with directions $\mathcal{R}$, $L \in \mathcal{L} - \{G\}$, and $R \in \mathcal{R}$ is the direction of L, then for every $\mathfrak{X}$-separated direct $(\Omega \cup G)$-decomposition $\mathcal{K}$ of L such that $\mathcal{K}\mathfrak{X}(G)$ refines $\mathcal{R}\mathfrak{X}(G) \cap L$, it follows that*

$$\left\{K \in \mathcal{K} - \mathfrak{X} : K \leq \langle \mathcal{R} - \{R\}\rangle \mathfrak{X}(G)\right\}$$

lies in an $\mathfrak{X}$-separated direct $(\Omega \cup G)$-decomposition of the successor to L.

Proof. Let M be the successor to L in $\mathcal{L}$ and set $C = \langle \mathcal{R} - \{R\}\rangle$. As $\mathcal{K}\mathfrak{X}(G)$ refines $\mathcal{R}\mathfrak{X}(G) \cap L$, it also refines $\{R\mathfrak{X}(G) \cap L, C\mathfrak{X}(G) \cap L\}$ and so

$$C\mathfrak{X}(G) \cap L = \langle K \in \mathcal{K}, K \leq C\mathfrak{X}(G)\rangle = \langle K \in \mathcal{K} - \mathfrak{X}, K \leq C\mathfrak{X}(G)\rangle \mathfrak{X}(G).$$

Since $\mathcal{K}$ is $\mathfrak{X}$-separated $F = \langle K \in \mathcal{K} - \mathfrak{X}, K \leq C\mathfrak{X}(G)\rangle$ has no direct $(\Omega \cup G)$-factor in $\mathfrak{X}$. Also, as the direction of L is R, $C\mathfrak{X}(G) \cap M = C\mathfrak{X}(G) \cap L$ and so

$$\begin{aligned}(C \cap M)\mathfrak{X}(G) &= C\mathfrak{X}(G) \cap M \\ &= C\mathfrak{X}(G) \cap L \\ &= \langle K \in \mathcal{K} - \mathfrak{X}, K \leq C\mathfrak{X}(G)\rangle \mathfrak{X}(G) \\ &= F \times \langle \mathcal{K} \cap \mathfrak{X}\rangle.\end{aligned}$$

Using $(M, F, C \cap M)$ in the role of (G, H, R) in Proposition 3.22, it follows that F is a direct $(\Omega \cup G)$-factor of M. In particular, $\{K \in \mathcal{K} - \mathfrak{X}, K \leq C\mathfrak{X}(G)\}$ lies in a direct $(\Omega \cup G)$-decomposition of M. □

4. Algorithms to lift, extend, and match direct decompositions

Here we transition into algorithms beginning with a small modification of a technique introduced by Luks and Wright to find a direct complement to a direct factor (Theorem 4.8). We then produce an algorithm Merge (Theorem 4.13) to lift direct decompositions for appropriate quotients. That algorithm is the work-horse which glues together the unique constituents predicted by Theorem 3.6. That task asks us to locate a unique partition of a certain set, but in a manner that does not test each of the exponentially many partitions. The proof relies heavily on results such as Theorem 3.28 to prove that an essentially greedy algorithm will suffice.

For brevity we have opted to describe the algorithms only for the case of lifting decompositions. The natural duality of up and down graders makes it possible to modify the methods to prove similar results for extending decompositions.

This section assumes familiarity with Sections 2.6 and 3.

4.1. Constructing direct complements.

In this section we solve the following problem in polynomial-time.

P. 4.1. Direct-Ω-Complement

Given: *a Ω-group G and an Ω-subgroup H,*
Return: *an Ω-subgroup K of G such that $G = H \times K$, or certify that no such K exists.*

Luks and Wright gave independent solutions to Direct-$\emptyset$-Complement in back-to-back lectures at the University of Oregon [18, 37].

Theorem 4.2 (Luks [18],Wright [37]). *For groups of permutations,* Direct-$\emptyset$-Complement *has a polynomial-time solution*

Both [18] and [37] reduce Direct-$\emptyset$-Complement to the following problem (here generalized to Ω-groups):

P. 4.3. Ω-Complement-Abelian

Given: *an Ω-group G and an abelian $(\Omega \cup G)$-subgroup M,*
Return: *an Ω-subgroup K of G such that $G = M \rtimes K$, or certify that no such K exists.*

To deal with operator groups we use some modifications to the problems above. Many of the steps are conceived within the group $\langle \Omega\theta \rangle \ltimes G \leq \operatorname{Aut} G \ltimes G$. However, to execute these algorithms we cannot assume that $\langle \Omega\theta \rangle \ltimes G$ is a permutation group as it is possible that these groups have no small degree permutation representations (e.g. $G = \mathbb{Z}_p^d$ and $\langle \Omega\theta \rangle = \mathrm{GL}(d,p)$). Instead we operate within G and account for the action of Ω along the way.

Lemma 4.4. *Let G be an Ω-group where $\theta : \Omega \to \operatorname{Aut} G$. If $\{\langle \mathtt{X}|\mathtt{R}\rangle, f, \ell\}$ is a constructive presentation for G and $\langle \Omega | \mathtt{R}' \rangle$ a presentation for $A := \langle \Omega\theta \rangle \leq \operatorname{Aut} G$ with respect to θ, then $\langle \Omega \sqcup \mathtt{X} | \mathtt{R}' \ltimes \mathtt{R} \rangle$ is a presentation for $A \ltimes G$ with respect to $\theta \sqcup f$, where*

$$\mathtt{R}' \ltimes \mathtt{R} = \mathtt{R}' \sqcup \mathtt{R} \sqcup \{(xf)^s \ell \cdot (x^s)^{-1} : x \in \mathtt{X}, s \in \Omega\}, \text{ and}$$
$$\forall z \in \Omega \sqcup \mathtt{X}, \quad z(\theta \sqcup f) = \begin{cases} z\theta & z \in \Omega, \\ zf & z \in \mathtt{X}. \end{cases}$$

Proof. Without loss of generality we assume $F(\Omega), F(\mathtt{X}) \leq F(\Omega \sqcup \mathtt{X})$. Let K be the normal closure of $\mathtt{R}' \ltimes \mathtt{R}$ in $F(\Omega \sqcup \mathtt{X})$. For each $s \in \Omega$ and each $x \in \mathtt{X}$ it follows that $Kx^s = K(xf)^s\ell \leq N = \langle K, F(\mathtt{X}) \rangle$. In particular, N is normal in $F(\Omega \sqcup \mathtt{X})$. Set $C = \langle K, F(\Omega) \rangle$. It follows that $F(\Omega \sqcup \mathtt{X}) = \langle C, N \rangle = CN$. Thus, $H = F(\Omega \sqcup \mathtt{X})/K = CN/K = (C/K)(N/K)$ and N/K is normal in H. Since C/K and N/K satisfy the presentations for A and G respectively, it follows that H is a quotient of $A \ltimes G$. To show that $H \cong A \ltimes G$ it suffices to notice that $A \ltimes G$ satisfies the relations in $\mathtt{R}' \ltimes \mathtt{R}$, with respect to $\Omega \sqcup \mathtt{X}$ and $\theta \sqcup \ell$. Indeed, for all $s \in \Omega$ and all $x \in \mathtt{X}$ we see that

$$x^s(\widehat{\theta \sqcup f}) = (s\theta^{-1}, 1)(1, xf)(s\theta, 1) = (1, (xf)^s) = (1, (xf)^s\ell\hat{f}) = (xf)^s\ell(\widehat{\theta \sqcup f}),$$

which implies that $(xf)^s\ell(x^s)^{-1} \in \ker \widehat{\theta \sqcup f}$; so, $K \leq \ker \widehat{\theta \sqcup f}$. Hence, $\langle \Omega \sqcup \mathtt{X} | \mathtt{R}' \ltimes \mathtt{R} \rangle$ is a presentation for $A \ltimes G$. □

Proposition 4.5. Ω-Complement-Abelian *has a polynomial-time solution.*

Proof. Let $M, G \in \mathbb{G}_n$, and $\theta : \Omega \to \operatorname{Aut} G$ a function, where M is an abelian $(\Omega \cup G)$-subgroup of G.

Algorithm. Use Presentation to produce a constructive presentation $\{\langle \mathtt{X}|\mathtt{R}\rangle, f, \ell\}$ for G mod M. For each $s \in \Omega$ and each $x \in \mathtt{X}$, define

$$r_{s,x} = (xf^s)\ell \cdot (x^s)^{-1} \in F(\Omega \sqcup \mathtt{X}).$$

Use Solve to decide if there is a $\mu \in M^{\mathtt{X}}$ where

$$\forall r \in \mathtt{R}, \quad r(f\mu) = 1, \text{ and} \tag{4.6}$$
$$\forall s \in \Omega, \forall x \in \mathtt{X} \quad r_{s,x}(f\mu) = 1. \tag{4.7}$$

If no such μ exists, then assert that M has no Ω-complement in G; otherwise, return $K = \langle x(f\mu) = (xf)(x\mu) : x \in \mathtt{X} \rangle$.

Correctness. Let $A = \langle \Omega\theta \rangle \leq \operatorname{Aut} G$ and let $\langle \Omega | \mathtt{R}' \rangle$ be a presentation of A with respect to θ. The algorithm creates a constructive presentation $\{\langle \mathtt{X} | \mathtt{R} \rangle, f, \ell\}$ for G mod M and so by Lemma 4.4, $\langle \Omega \sqcup \mathtt{X} | \mathtt{R}' \ltimes \mathtt{R} \rangle$ is a presentation for $A \ltimes G$ mod M with respect to $\theta \sqcup f$.

First suppose that the algorithm returns $K = \langle x(f\mu) : x \in \mathtt{X} \rangle$. As $\mathtt{X}f \subseteq KM$ we get that $G = \langle \mathtt{X}f \rangle \leq KM \leq G$. By (4.6), $r(f\mu) = 1$ for all $r \in \mathtt{R}$. Therefore K satisfies the defining relations of $G/M \cong K/(K \cap M)$, which forces $K \cap M = 1$ and so $G = K \ltimes M$. By (4.6) and (4.7), the generator set $\Omega\theta \sqcup \{x\bar{\mu} : x \in \mathtt{X}\}f$ of $\langle A, K \rangle$ satisfies the defining relations $\mathtt{R}' \ltimes \mathtt{R}$ of $(A \ltimes G)/M$ and so $\langle A, K \rangle$ is isomorphic to a quotient of $(A \ltimes G)/M$ where K is the image of G/M. This shows K is normal in $\langle A, K \rangle$. In particular, $\langle K^{\Omega} \rangle \leq K$. Therefore if the algorithm returns a subgroup then the return is correct.

Now suppose that there is a $K \leq G$ such that $\langle K^{\Omega} \rangle \leq K$ and $G = K \ltimes M$. We must show that in this case the algorithm returns a subgroup. We have that $G = \langle \mathtt{X}f \rangle$ and the generators $\mathtt{X}f$ satisfy (mod M) the relations $\mathtt{R}$. Let $\varphi : G/M \to K$ be the isomorphism $kM\varphi = k$, for all $km \in KM = G$, where $k \in K$ and $m \in M$. Define $\tau : \mathtt{X} \to M$ by $x\tau = (xf)^{-1}(xfM)\varphi$, for all $x \in \mathtt{X}$. Notice $\langle x(x\tau) : x \in \mathtt{X} \rangle = K$. Furthermore, $\Phi : (a, hM) \mapsto (a, hM\varphi)$ is an isomorphism $A \ltimes (G/M) \to A \ltimes K$. As $\mathtt{R} \subseteq F(\mathtt{X})$ it follows that $r((\theta \sqcup f)\Phi) = r(f)\Phi = 1$, for all $r \in \mathtt{R}$. Also,

$$\forall z \in \Omega \sqcup \mathtt{X}, \quad z(\theta \sqcup f)\Phi = \begin{cases} (z\theta, 1), & z \in \Omega; \\ (1, (xfM)\varphi) = (1, x\bar{\tau}), & z \in \mathtt{X}. \end{cases}$$

Therefore, $r(f\tau) = r((\theta \sqcup f)\Phi) = 1$ for all $r \in \mathtt{R}$. Thus, an appropriate $\tau \in M^{\mathtt{X}}$ exists and the algorithm is guaranteed to find such an element and return an Ω-subgroup of G complementing M.

Timing. The algorithm applies two polynomial-time algorithms. □

Theorem 4.8. Direct-Ω-Complement *has a polynomial-time solution.*

Proof. Let $H, G \in \mathbb{G}_n$ and $\theta : \Omega \to \operatorname{Aut} G$, where $\langle H^{\Omega} \rangle \leq H \leq G$.

Algorithm. Use Member to determine if H is an $(\Omega \cup G)$-subgroup of G. If not, then this certifies that H is not a direct factor of G. Otherwise, use Normal-Centralizer to compute $C_G(H)$ and $\zeta_1(H)$. Using Member, test if $G = HC_G(H)$ and if $\langle C_G(H)^{\Omega} \rangle = C_G(H)$. If either fails, then certify that H is not a direct Ω-factor of G. Next, use Proposition 4.5 to find an Ω-subgroup $K \leq C_G(H)$ such that $C_G(H) = \zeta_1(H) \rtimes K$, or determine that no such K exists. If K exists, return K; otherwise, H is not a direct Ω-factor of G.

Correctness. Note that if $G = H \times J$ is a direct Ω-decomposition then H and J are $(\Omega \cup G)$-subgroups of G, $G = HC_G(H)$, and $C_G(H) = \zeta_1(H) \times J$. As $\Omega\theta \subseteq \operatorname{Aut} G$, $\zeta_1(H)$ is an Ω-subgroup and therefore $C_G(H)$ is an Ω-subgroup. Therefore the tests within the algorithm properly identify cases where H is not a direct Ω-factor of G. Finally, if the algorithm returns an Ω-subgroup K such that $C_G(H) = \zeta_1(H) \rtimes K = \zeta_1(G) \times K$, then $G = H \times K$ is a direct Ω-decomposition.

Timing. The algorithm makes a bounded number of calls to polynomial-time algorithms. □

4.2. **Merge.** In this section we provide an algorithm which given an appropriate direct decomposition of a quotient group produces a direct decomposition of original group.

Throughout this section we assume that $(\mathfrak{X}, G \mapsto \mathfrak{X}(G))$ is an up Ω-grading pair in which $\zeta_1(G) \leq \mathfrak{X}(G)$.

The constraints of exchange by $\mathrm{Aut}_{\Omega\cup G}\, G$ given in Lemma 3.5 can be sharpened to individual direct factors as follows. (Note that Proposition 4.9 is false when considering the action of $\mathrm{Aut}\, G$ on direct factors.)

Proposition 4.9. *Let X and Y be direct Ω-factors of G with no abelian direct Ω-factor. The following are equivalent.*

(i) $X\varphi = Y$ *for some* $\varphi \in \mathrm{Aut}_{\Omega\cup G}\, G$.

(ii) $X\zeta_1(G) = Y\zeta_1(G)$.

Proof. By (2.1), $\mathrm{Aut}_{\Omega\cup G}\, G$ is the identity on $G/\zeta_1(G)$; therefore (i) implies (ii).

Next we show (ii) implies (i). Recall that $\mathfrak{A}$ is the class of abelian groups. Let $\{X, A\}$ and $\{Y, B\}$ be direct Ω-decompositions of G. Choose Remak $(\Omega \cup G)$-decompositions $\mathcal{R}$ and $\mathcal{C}$ which refine $\{X, A\}$ and $\{Y, B\}$ respectively. Let $\mathcal{X} = \{R \in \mathcal{R} : R \leq X\}$. By Theorem 2.10 there is a $\varphi \in \mathrm{Aut}_{\Omega\cup G}\, G$ such that $\mathcal{X}\varphi \subseteq \mathcal{C}$. However, φ is the identity on $G/\zeta_1(G)$. Hence, $\langle\mathcal{X}\rangle\zeta_1(G) = X\zeta_1(G)\varphi = Y\zeta_1(G)$. Thus, $\mathcal{X}\varphi \subseteq \{C \in \mathcal{C} : C \leq Y\zeta_1(G)\} - \mathfrak{A}$. Yet, $\mathcal{C}$ refines $\{Y, B\}$ and Y has no direct Ω-factor in $\mathfrak{A}$. Thus,

$$\{C \in \mathcal{C} : C \leq Y\zeta_1(G) = Y \times \zeta_1(B)\} - \mathfrak{A} = \{C \in \mathcal{C} : C \leq Y\}.$$

Thus, $\mathcal{X}\varphi \subseteq \mathcal{Y}$. By reversing the roles of X and Y we see that $\mathcal{Y}\varphi' \subseteq \mathcal{X}$ for some φ'. Thus, $|\mathcal{X}| = |\mathcal{Y}|$. So we conclude that $\mathcal{X}\varphi = \mathcal{Y}$ and $X\varphi = Y$. □

Theorem 4.10. *There is a polynomial-time algorithm which, given an Ω-group G and a set $\mathcal{K}$ of $(\Omega \cup G)$-subgroups such that*

(a) $\mathfrak{X}(\langle\mathcal{K}\rangle) = \mathfrak{X}(G)$ *and*

(b) $\mathcal{K}$ *is a direct* $(\Omega \cup G)$*-decomposition of* $\langle\mathcal{K}\rangle$,

returns a direct Ω-decomposition $\mathcal{H}$ of G such that

(i) $|\mathcal{H} - \mathcal{K}| \leq 1$,

(ii) if $K \in \mathcal{K}$ *such that* $\langle\mathcal{H} \cap \mathcal{K}, K\rangle$ *has a direct* Ω*-complement in* G, *then* $K \in \mathcal{H}$; *and*

(iii) if $K \in \mathcal{K} - \mathfrak{X}$ *such that* K *is a direct* $(\Omega \cup G)$*-factor of* G, *then* $K \in \mathcal{H}$.

Proof. Algorithm.

```
Extend( $G$, $\mathcal{K}$ )
begin
    $\mathcal{L} = \emptyset$; $\lfloor G \rfloor = G$;
    /* Using the algorithm for Theorem 4.8 to determine the existence of $H$,
    execute the following. */
    while ( $\exists K \in \mathcal{K}, \exists H, \mathcal{L} \sqcup \{K, H\}$ is a direct $\Omega$-decomposition of $G$ )
        $\lfloor G \rfloor = H$;
        $\mathcal{L} = \mathcal{L} \sqcup \{K\}$;
        $\mathcal{K} = \mathcal{K} - \{K\}$;

    return $\mathcal{H} = \mathcal{L} \sqcup \{\lfloor G \rfloor\}$ ;
end.
```

Correctness. We maintain the following loop invariant (true at the start and end of each iteration of the loop): $\mathcal{L} \sqcup \{\lfloor G \rfloor\}$ is a direct $(\Omega \cup G)$-decomposition of G

and $\mathcal{L} \subseteq \mathcal{K}$. The loop exits once $\mathcal{L} \sqcup \{\lfloor G \rfloor\}$ satisfies (ii). Hence, $\mathcal{H} = \mathcal{L} \sqcup \{\lfloor G \rfloor\}$ satisfies (i) and (ii).

For (iii), suppose that $\mathcal{K}$ is $\mathfrak{X}$-separated and that $K \in (\mathcal{K} - \mathfrak{X}) - \mathcal{H}$ such that K is a direct $(\Omega \cup G)$-factor of G. Let $\langle F^{\Omega} \rangle \leq F \leq G$ such that $\{F, K\}$ is a direct $(\Omega \cup G)$-decomposition of G and $\mathcal{R}$ a Remak $(\Omega \cup G)$-decomposition of G which refines $\{F, K\}$. Also let $\mathcal{T}$ be a Remak $(\Omega \cup G)$-decomposition of G which refines $\mathcal{H}$. Set $\mathcal{X} = \{R \in \mathcal{R} : R \leq K\}$, and note that $\mathcal{X} \subseteq \mathcal{R} - \mathfrak{X}$ as K has no direct Ω-factor in $\mathfrak{X}$. By Theorem 2.10 we can exchange $\mathcal{X}$ with a $\mathcal{Y} \subseteq \mathcal{T} - \mathfrak{X}$ to create a Remak $(\Omega \cup G)$-decomposition $(\mathcal{T} - \mathcal{Y}) \sqcup \mathcal{X}$ of G. As $\zeta_1(G) \leq \mathfrak{X}(G)$ we get $\mathcal{R}\mathfrak{X}(G) = \mathcal{T}\mathfrak{X}(G)$ and $\mathcal{X}\mathfrak{X}(G) = \mathcal{Y}\mathfrak{X}(G)$ (Lemma 3.5, Proposition 4.9). Thus, by (a) and then (b),

$$\begin{aligned}
\langle \mathcal{Y} \rangle \cap \langle \mathcal{H} \cap \mathcal{K} \rangle &\equiv \langle \mathcal{X} \rangle \cap \langle \mathcal{H} \cap \mathcal{K} \rangle && \pmod{\mathfrak{X}(G)} \\
&\equiv K \cap \langle \mathcal{H} \cap \mathcal{K} \rangle && \pmod{\mathfrak{X}(\langle \mathcal{K} \rangle)} \\
&\leq K \cap \langle \mathcal{K} - \{K\} \rangle \\
&\equiv 1
\end{aligned}$$

Therefore $\langle \mathcal{Y} \rangle \leq \langle (\mathcal{T} - \mathfrak{X}) - \{T \in \mathcal{T} : T \leq \langle \mathcal{H} - \mathcal{K} \rangle\} \rangle$. Thus,

$$\mathcal{J} = (\mathcal{H} \cap \mathcal{K}) \sqcup \{K\} \sqcup \{\langle (\mathcal{T} - \mathcal{Y}) - \{T \in \mathcal{T} : T \leq \langle \mathcal{H} \cap \mathcal{K} \rangle\}$$

is a direct Ω-decomposition of G and $(\mathcal{H} \cap \mathcal{K}) \sqcup \{K\} \subseteq \mathcal{J} \cap \mathcal{K}$ which shows that $\mathcal{L}$ is not maximal. By the contrapositive we have (iii).

Timing. This loop makes $|\mathcal{K}| \leq \log_2 |G|$ calls to a polynomial-time algorithm for Direct-Ω-Complement. □

Under the hypothesis of Theorem 4.10 it is not possible to extend (iii) to say that if $K \in \mathcal{K}$ and K is a direct Ω-factor of G then $K \in \mathcal{H}$. Consider the following example (where $\Omega = \emptyset$).

Example 4.11. Let $G = D_8 \times \mathbb{Z}_2$, $D_8 = \langle a, b | a^4, b^2, (ab)^2 \rangle$. Use $\mathfrak{A}$ (the class of abelian groups) for $\mathfrak{X}$ and $\mathcal{K} = \{\langle (0,1) \rangle, \langle (a^2, 1) \rangle\}$. Each member of $\mathcal{K}$ is a direct factor of G, but $\mathcal{K}$ is not contained in any direct decomposition of G.

Lemma 4.12. *If $\mathcal{K}$ is a $\mathfrak{X}$-refined direct $(\Omega \cup G)$-decomposition of G such that $\mathcal{K}\mathfrak{X}(G)$ refines $\mathcal{R}\mathfrak{X}(G)$ for some Remak $(\Omega \cup G)$-decomposition of G, then $\mathcal{K}$ is a Remak $(\Omega \cup G)$-decomposition of G.*

Proof. As $\mathcal{R}$ is a Remak $(\Omega \cup G)$-decomposition of G, by Lemma 3.5, $\mathcal{R}\mathfrak{X}(G)$ refines $\mathcal{K}\mathfrak{X}(G)$ and so $\mathcal{K}\mathfrak{X}(G) = \mathcal{R}\mathfrak{X}(G)$. Hence, $|\mathcal{K} - \mathfrak{X}| = |\mathcal{R} - \mathfrak{X}|$ and because $\mathcal{K}$ is $\mathfrak{X}$-refined we also have: $|\mathcal{K} \cap \mathfrak{X}| = |\mathcal{R} \cap \mathfrak{X}|$. Therefore, $|\mathcal{K}| = |\mathcal{K} - \mathfrak{X}| + |\mathcal{K} \cap \mathfrak{X}| = |\mathcal{R} - \mathfrak{X}| + |\mathcal{R} \cap \mathfrak{X}| = |\mathcal{R}|$. As every Remak $(\Omega \cup G)$-decomposition of G has the same size, it follows that $\mathcal{K}$ cannot be refined by a larger direct $(\Omega \cup G)$-decomposition of G. Hence $\mathcal{K}$ is a Remak $(\Omega \cup G)$-decomposition of G. □

Theorem 4.13. *There is a polynomial-time algorithm which, given $G \in \mathbb{G}_n$, sets $\mathcal{A}, \mathcal{H} \subseteq \mathbb{G}_n$, and a function $\theta : \Omega \to \operatorname{Aut} G$, such that*

(a) $\mathcal{A}$ is a Remak $(\Omega \cup G)$-decomposition of $\mathfrak{X}(G)$,
(b) $\forall H \in \mathcal{H}$, $\mathfrak{X}(H) = \mathfrak{X}(G)$,
(c) $\mathcal{H}/\mathfrak{X}(G)$ is a direct Ω-decomposition of $G/\mathfrak{X}(G)$;

returns an $\mathfrak{X}$-refined direct Ω-decomposition $\mathcal{K}$ of G with the following property. If $\mathcal{R}$ is a direct Ω-decomposition of G where $\mathcal{H}$ refines $\mathcal{R}\mathfrak{X}(G)$ then $\mathcal{K}\mathfrak{X}(G)$ refines $\mathcal{R}\mathfrak{X}(G)$; in particular, if $\mathcal{R}$ is Remak then $\mathcal{K}$ is Remak.

Proof. Algorithm.

```
Merge( $\mathcal{A}$, $\mathcal{H}$ )
begin
    $\mathcal{K} = \mathcal{A}$;
    $\forall H \in \mathcal{H}$
        $\mathcal{K}$ =Extend( $\langle H, \mathcal{K}\rangle$, $\mathcal{K}$ );
    return $\mathcal{K}$ ;
end.
```

Correctness. Fix a direct Ω-decomposition $\mathcal{R}$ of G where $\mathcal{H}$ refines $\mathcal{R}\mathfrak{X}(G)$. We can assume $\mathcal{R}$ is $\mathfrak{X}$-refined.

The loop runs through a maximal chain $\mathscr{C}$ of subsets of $\mathcal{H}$ and so we track the iterations by considering the members of $\mathscr{C}$. By Proposition 3.27, $\mathcal{L} = \{L = L_{\mathcal{C}} = \langle \mathcal{C}, \mathfrak{X}(G)\rangle : \mathcal{C} \in \mathscr{C}\}$ is a direct chain. We claim the following properties as loop invariants. At the iteration $\mathcal{C} \in \mathscr{C}$, we claim that $(\mathcal{C}, L, \mathcal{K})$ satisfies:

(P.1) $\mathfrak{X}(L) = \mathfrak{X}(G)$,
(P.2) $\mathcal{K}\mathfrak{X}(G)$ refines $\mathcal{R}\mathfrak{X}(G) \cap L$, and
(P.3) $\mathcal{K}$ is an $\mathfrak{X}$-refined direct $(\Omega \cup G)$-decomposition of L.

Thus, when the loop completes, $L = \langle \mathcal{H}\rangle = G$. By (P.2) $\mathcal{K}\mathfrak{X}(G)$ refines $\mathcal{R}\mathfrak{X}(G)$. By (P.3), $\mathcal{K}$ is an $\mathfrak{X}$-refined direct Ω-decomposition of G. Following Lemma 4.12, if $\mathcal{R}$ is a Remak $(\Omega \cup G)$-decomposition of G then $\mathcal{K}$ is a Remak $(\Omega \cup G)$-decomposition. We prove (P.1)–(P.3) by induction.

As we begin with $\mathcal{K} = \mathcal{A}$, in the base case $\mathcal{C} = \emptyset$, $L = \mathfrak{X}(G)$, and so (P.1) holds. As $\mathcal{K}\mathfrak{X}(G) = \emptyset$ and $\mathcal{R}\mathfrak{X}(G) \cap \mathfrak{X}(G) = \emptyset$ we have (P.2). Also (P.3) holds because of (a).

Now suppose for induction that for some $\mathcal{C} \in \mathscr{C}$, $(\mathcal{C}, L, \mathcal{K})$ satisfies (P.1)–(P.3). Let $\mathcal{D} = \mathcal{C} \sqcup \{H\} \in \mathscr{C}$ be the successor to $\mathcal{C}$, for the appropriate $H \in \mathcal{H} - \mathcal{C}$. Set $M = \langle H, L\rangle$, and $\mathcal{M} = \texttt{Extend}(M, \mathcal{K})$. Since $H \leq M$ it follows from (b) that $\mathfrak{X}(G) \leq \mathfrak{X}(M) \leq \mathfrak{X}(H) = \mathfrak{X}(G)$ so that $\mathfrak{X}(M) = \mathfrak{X}(G)$; hence, (P.1) holds for $(\mathcal{D}, M, \mathcal{M})$.

Next we prove (P.2) holds for $(\mathcal{D}, M, \mathcal{M})$. As $L, M \in \mathcal{L}$ and $\mathcal{L}$ is a direct chain with directions $\mathcal{R}$, $\mathcal{R} \cap L$ and $\mathcal{R} \cap M$ are direct $(\Omega \cup G)$-decomposition of L and M, respectively. Following Theorem 4.10(i), $|\mathcal{M} - \mathcal{K}| \leq 1$. As $H \not\leq L$, $\mathcal{M} \neq \mathcal{K}$, and there is a group $\lfloor H \rfloor$ in $\mathcal{M} - \mathcal{K}$ with $H \leq \lfloor H \rfloor \mathfrak{X}(G)$. By assumption, $\mathcal{H}$ refines $\mathcal{R}\mathfrak{X}(G)$. Hence, there is a unique $R \in \mathcal{R} - \mathfrak{X}$ such that $\mathfrak{X}(G) < H \leq R\mathfrak{X}(G)$. Indeed, R is the direction of L. Let $C = \langle (\mathcal{R} - \{R\}) - \mathfrak{X}\rangle$ and define

$$\mathcal{J} = \{K \in \mathcal{K} - \mathfrak{X} : K \leq C\mathfrak{X}(G)\}.$$

As the direction of L is R, $C\mathfrak{X}(G) \cap M = C\mathfrak{X}(G) \cap L = \langle \mathcal{J}\rangle \mathfrak{X}(G)$ and by Theorem 3.28, $\mathcal{J}$ lies in a $\mathfrak{X}$-separated direct $(\Omega \cup G)$-decomposition of M. Thus, by Theorem 4.10(ii), $\mathcal{J} \subseteq \mathcal{M} \cap \mathcal{K}$. Also, $M = \langle \mathcal{M} - \mathcal{J}\rangle \times \langle \mathcal{J}\rangle$ and $\mathfrak{X}(M) = \mathfrak{X}(G)$, so

$$\begin{aligned} M/\mathfrak{X}(G) &= \langle \mathcal{M} - \mathcal{J}\rangle \mathfrak{X}(G)/\mathfrak{X}(G) \times \langle \mathcal{J}\rangle \mathfrak{X}(G)/\mathfrak{X}(G) \\ &= \langle \mathcal{M} - \mathcal{J}\rangle \mathfrak{X}(G)/\mathfrak{X}(G) \times (C\mathfrak{X}(G) \cap M)/\mathfrak{X}(G). \end{aligned}$$

Thus, $\langle \mathcal{M} - \mathcal{J}\rangle \mathfrak{X}(G) \cap C\mathfrak{X}(G) = \mathfrak{X}(G)$. Suppose that X is a directly $(\Omega \cup G)$-indecomposable direct $(\Omega \cup G)$-factor of $\langle \mathcal{M} - \mathcal{J}\rangle \mathfrak{X}(G)$ which does not lie in $\mathfrak{X}$. As $\mathcal{R} \cap M$ is a direct $(\Omega \cup M)$-decomposition of M and X lies in a Remak $(\Omega \cup G)$-decomposition of M, then by Lemma 3.5, $X \leq R\mathfrak{X}(M) = R\mathfrak{X}(G)$ or $X \leq C\mathfrak{X}(M) =$

$C\mathfrak{X}(G)$. Yet, $X \notin \mathfrak{X}$ so that $X \nleq \mathfrak{X}(G)$ and

$$X \cap C\mathfrak{X}(G) \leq \langle \mathcal{M} - \mathcal{J} \rangle \mathfrak{X}(G) \cap C\mathfrak{X}(G) = \mathfrak{X}(G);$$

hence, $X \nleq C\mathfrak{X}(G)$. Thus, $X \leq R\mathfrak{X}(G)$ and as X is arbitrary, we get

$$\langle \mathcal{M} - \mathcal{J} \rangle \mathfrak{X}(G) \leq R\mathfrak{X}(G).$$

As $M/\mathfrak{X}(G) = (R\mathfrak{X}(G) \cap M)/\mathfrak{X}(G) \times (C\mathfrak{X}(G) \cap M)/\mathfrak{X}(G)$ we indeed have

$$\langle \mathcal{M} - \mathcal{J} \rangle \mathfrak{X}(G) = R\mathfrak{X}(G) \cap M.$$

In particular, $\mathcal{M}\mathfrak{X}(G)$ refines $\mathcal{R}\mathfrak{X}(G) \cap M$ and so (P.2) holds.

Finally to prove (P.3) it suffices to show that $\lfloor H \rfloor$ has no direct $(\Omega \cup G)$-factor in $\mathfrak{X}$. Suppose otherwise: so $\lfloor H \rfloor$ has a direct $(\Omega \cup G)$-decomposition $\{H_0, A\}$ where $A \in \mathfrak{X}$ and A is directly $(\Omega \cup G)$-indecomposable. Swap out $\lfloor H \rfloor$ in $\mathcal{M}$ for $\{H_0, A\}$ creating

$$\mathcal{M}' = (\mathcal{M} - \{\lfloor H \rfloor\}) \sqcup \{H_0, A\} = (\mathcal{M} \cap \mathcal{K}) \sqcup \{H_0, A\}.$$

As $A \in \mathfrak{X}$ it follows that $A \leq \mathfrak{X}(M) = \mathfrak{X}(G) = \mathfrak{X}(L)$. In particular, $A \leq L \leq M$. As A is a direct $(\Omega \cup G)$-factor of M, A is also a direct $(\Omega \cup G)$-factor of L. Since $\langle A, \mathcal{M} \cap \mathcal{K} \rangle \leq L$ it follows that

$$\mathcal{M}' \cap L = \{H_0 \cap L, A\} \sqcup (\mathcal{M} \cap \mathcal{K})$$

is a direct $(\Omega \cup G)$-decomposition of L. Furthermore, A is directly $(\Omega \cup G)$-indecomposable, $A \in \mathfrak{X}$, and A lies in a Remak $(\Omega \cup G)$-decomposition of L. Also $\mathcal{K} \cap \mathfrak{X}$ lies in a Remak $(\Omega \cup G)$-decomposition $\mathcal{T}$ of L in which $\mathcal{K} \cap \mathfrak{X} = \mathcal{T} \cap \mathfrak{X}$ (Proposition 3.10(iv) and (v)); thus, by Theorem 2.10 there is a $B \in \mathcal{K} \cap \mathfrak{X}$ such that

$$(\mathcal{M}' \cap L - \{A\}) \sqcup \{B\}$$

is a direct $(\Omega \cup G)$-decomposition of L. Hence, $\mathcal{M}'' = (\mathcal{M}' - \{A\}) \sqcup \{B\}$ is a direct $(\Omega \cup G)$-decomposition of M. However, $\mathcal{M}'' \cap \mathcal{K} = (\mathcal{M} \cap \mathcal{K}) \cup \{B\}$. By Theorem 4.10(i), $\mathcal{M} \cap \mathcal{K}$ is maximal with respect to inclusion in $\mathcal{K}$, such that $\mathcal{M} \cap \mathcal{K}$ is contained in a direct $(\Omega \cup G)$-decomposition of M. Thus, $B \in \mathcal{M} \cap \mathcal{K}$. That is, impossible since it would imply that $\mathcal{M}' \cap L$ and $(\mathcal{M}' - \{A\}) \cap L$ are both direct $(\Omega \cup G)$-decompositions of L, i.e. that $A \cap L = 1$, But $1 < A \leq L$. This contradiction demonstrates that $\lfloor H \rfloor$ has no direct $(\Omega \cup G)$-factor in $\mathfrak{X}$. Therefore, $\mathcal{M}$ is $\mathfrak{X}$-refined.

Having shown that M and $\mathcal{M}$ satisfy (P.1)–(P.3), at the end of the loop $\mathcal{K}$ and L are reassigned to $\mathcal{M}$ and M respectively and so maintain the loop invariants.

Timing. The algorithm loops over every element of $\mathcal{H}$ applying the polynomial-time algorithm of Theorem 4.10 once in each loop. Thus, `Merge` is a polynomial-time algorithm. □

5. Bilinear maps and p-groups of class 2

In this section we introduce bilinear maps and a certain commutative ring as a means to access direct decompositions of a p-group of class 2. In our minds, those groups represent the most difficult case of the direct product problem. This is because p-groups of class 2 have so many normal subgroups, and many of those pairwise intersect trivially making them appear to be direct factors when they are not. Thus, a greedy search is almost certain to fail. Instead, we have had to consider a certain commutative ring that can be derived from a p-group. As commutative rings have unique Remak decomposition, and a decomposable p-group will have many Remak decompositions, we might expect such a method to have lost vital information. However, in view of results such as Theorem 3.6 we recognize that in fact what we will have constructed leads us to a matching for the extension $1 \to \zeta_1(G) \to G \to G/\zeta_1(G) \to 1$.

Unless specified otherwise, in this section G is a p-group of class 2.

5.1. **Bilinear maps.** Here we introduce Ω-bilinear maps and direct Ω-decompositions of Ω-bilinear maps. This allows us to solve the match problem for p-groups of class 2.

Let V and W denote abelian Ω-groups. A map $b : V \times V \to W$ is Ω-*bilinear* if

$$b(u+u', v+v') = b(u,v) + b(u',v) + b(u,v') + b(u',v'), \text{ and} \tag{5.1}$$

$$b(ur, v) = b(u,v)r = b(u, vr), \tag{5.2}$$

for all $u, u'v, v' \in V$ and all $r \in \Omega$. Every Ω-bilinear map is also $\mathbb{Z}$-bilinear. Define

$$b(X,Y) = \langle b(x,y) : x \in X, y \in Y \rangle \tag{5.3}$$

for $X, Y \subseteq V$. If $X \leq V$ then define the *submap*

$$b_X : X \times X \to b(X,X) \tag{5.4}$$

as the restriction of b to inputs from X. The *radical* of b is

$$\operatorname{rad} b = \{v \in V : b(v,V) = 0 = b(V,v)\}. \tag{5.5}$$

We say that b is *nondegenerate* if $\operatorname{rad} b = 0$. Finally, call b *faithful* Ω-bilinear when $(0 :_\Omega V) \cap (0 :_\Omega W) = 0$, where $(0 :_\Omega X) = \{r \in \Omega : Xr = 0\}$, $X \in \{V, W\}$.

Definition 5.6. Let $\mathcal{B}$ be a family of Ω-bilinear maps $b : V_b \times V_b \to W_b$, $b \in \mathcal{B}$. Define $\oplus\mathcal{B} = \bigoplus_{b\in\mathcal{B}} b$ as the Ω-bilinear map $\bigoplus_{b\in\mathcal{B}} V_b \times \bigoplus_{b\in\mathcal{B}} V_b \to \bigoplus_{b\in\mathcal{B}} W_b$ where:

$$(\oplus\mathcal{B})\left((u_b)_{b\in\mathcal{B}}, (v_b)_{b\in\mathcal{B}}\right) = (b(u_b, v_b))_{b\in\mathcal{B}}, \qquad \forall (u_b)_{b\in\mathcal{B}}, (v_b)_{b\in\mathcal{B}} \in \bigoplus_{b\in\mathcal{B}} V_b. \tag{5.7}$$

Lemma 5.8. *If $b : V \times V \to W$ is an Ω-bilinear map, $\mathcal{C}$ a finite set of submaps of b such that*

(i) $\{X_c : c : X_c \times X_c \to Z_c \in \mathcal{C}\}$ is a direct Ω-decomposition of V,
(ii) $\{Z_c : c : X_c \times X_c \to Z_c \in \mathcal{C}\}$ is a direct Ω-decomposition of W, and
(iii) $b(X_c, X_d) = 0$ for distinct $c, d \in \mathcal{C}$;

then $b = \bigoplus \mathcal{C}$.

Proof. By (i), we may write each $u \in V$ as $u = (u_c)_{c\in\mathcal{C}}$ with $u_c \in X_c$, for all $c : X_c \times X_c \to Z_c \in \mathcal{C}$. By (iii) followed by (ii) we have that $b(u,v) = \sum_{c,d\in\mathcal{C}} b(u_c, v_d) = \sum_{c\in\mathcal{C}} c(u_c, v_c) = (\oplus\mathcal{C})(u,v)$. □

Definition 5.9. A *direct* Ω-*decomposition* of an Ω-bilinear map $b : V \times V \to W$ is a set $\mathcal{B}$ of submaps of b satisfying the hypothesis of Lemma 5.8. Call b directly Ω-indecomposable if its only direct Ω-decomposition is $\{b\}$. A Remak Ω-decomposition of b is an Ω-decompositions whose members or directly Ω-indecomposable.

The bilinear maps we consider were created by Baer [2] and are the foundation for the many Lie methods that have been associated to p-groups. Further details of our account can be found in [33, Section 5].

The principle example of such maps is the commutation of an Ω-group G where $\gamma_2(G) \leq \zeta_1(G)$. There we define $V = G/\zeta_1(G)$, $W = \gamma_2(G)$, and $b = \mathsf{Bi}(G) : V \times V \to W$ where

$$b(\zeta_1(G)x, \zeta_1(G)y) = b(x,y), \qquad \forall x, \forall y, x, y \in G. \tag{5.10}$$

It is directly verified that b is $\mathbb{Z}_{p^e}[\Omega]$-bilinear where $G^{p^e} = 1$, and furthermore, nondegenerate. When working in V and W we use additive notation.

Given $H \leq G$ we define $U = H\zeta_1(G)/\zeta_1(G) \leq V$, $Z = H \cap \gamma_2(G) \leq W$, and $c := \mathsf{Bi}(H;G) : U \times U \to Z$ where

$$c(u,v) = b(u,v), \qquad \forall u \forall v, u, v \in U. \tag{5.11}$$

Proposition 5.12. *If G is a Ω-group and $\gamma_2(G) \leq \zeta_1(G)$, then every direct Ω-decomposition $\mathcal{H}$ of G induces a direct Ω-decomposition*

$$\mathsf{Bi}(\mathcal{H}) = \{\mathsf{Bi}(H;G) : H \in \mathcal{H}\}. \tag{5.13}$$

If $\mathsf{Bi}(P)$ is directly Ω-indecomposable and $\zeta_1(G) \leq \Phi(G)$, then G is directly Ω-indecomposable.

Proof. Set $b := \mathsf{Bi}(G)$. By Lemma 3.2 and Proposition 3.12, $\mathcal{H}\zeta_1(G)/\zeta_1(G)$ is a direct Ω-decomposition of $V = G/\zeta_1(G)$ and $\mathcal{H} \cap \gamma_2(G)$ is a direct Ω-decomposition of $W = \gamma_2(G)$. Furthermore, for each $H \in \mathcal{H}$,

$$b(H\zeta_1(G)/\zeta_1(G), \langle \mathcal{H} - \{H\}\rangle \zeta_1(G)/\zeta_1(G)) = [H, \langle \mathcal{H} - \{H\}\rangle] = 0 \in W.$$

In particular, $\mathsf{Bi}(\mathcal{H})$ is a direct Ω-decomposition of b.

Finally, if $\mathsf{Bi}(P)$ is directly indecomposable then $|\mathsf{Bi}(\mathcal{H})| = 1$. Thus, $\mathcal{H}\zeta_1(G) = \{G\}$. Therefore $\mathcal{H}$ has exactly one non-abelian member. Take $Z \in \mathcal{H} \cap \mathfrak{A}$. As Z is abelian, $Z \leq \zeta_1(G)$. If $\zeta_1(G) \leq \Phi(G)$ then the elements of G are non-generators. In particular, $G = \langle \mathcal{H} \rangle = \langle \mathcal{H} - \{Z\}\rangle$. But by definition no proper subset of decomposition generates the group. So $\mathcal{H} \cap \mathfrak{A} = \emptyset$. Thus, $\mathcal{H} = \{G\}$ and G is directly Ω-indecomposable. □

Baer and later others observed a partial reversal of the map $G \mapsto \mathsf{Bi}(G)$. Our account follows [33]. In particular, if $b : V \times V \to W$ is a $\mathbb{Z}_{p^e}$-bilinear map then we may define a group $\mathsf{Grp}(b)$ on the set $V \times W$ where the product is given by:

$$(u,w) * (u',w') = (u + u', w + b(u,u') + w'), \tag{5.14}$$

for all (u,w) and all (u',w') in $V \times W$. The following are immediate from the definition.

(i) $(0,0)$ is the identity and for all $(u,w) \in V \times W$, $(u,w)^{-1} = (-u, -w + b(u,u))$.
(ii) For all (u,w) and all (v,w) in $V \times W$, $[(u,w),(v,w')] = (0, b(u,v) - b(v,u))$.

If b is Ω-bilinear then $\mathsf{Grp}(b)$ is an Ω-group where

$$\forall s \in \Omega, \forall (u,w) \in V \times W, \qquad (u,w)^s = (u^s, w^s).$$

In light of (ii), if $p > 2$ and b is alternating, i.e. for all u and all v in V, $b(u,v) = -b(v,u)$, then $[(u,w),(v,w')] = (0, 2b(u,v))$. For that reason it is typical to consider $\mathsf{Grp}(\frac{1}{2}b)$ in those settings so that $[(u,w),(v,w')] = (0, b(u,v))$. We shall not require this approach. If $G^p = 1$ then $G \cong \mathsf{Grp}(\mathsf{Bi}(G))$ [35, Proposition 3.10(ii)].

Corollary 5.15. *If G is a p-group with $G^p = 1$ and $\gamma_2(G) \leq \zeta_1(G)$ then G is directly Ω-indecomposable if, and only if, $\mathsf{Bi}(G)$ is directly Ω-indecomposable and $\zeta_1(G) \leq \Phi(G)$.*

Proof. The reverse directions is Proposition 5.12. We focus on the forward direction. As $G^p = 1$ it follows that $G \cong \mathsf{Grp}(\mathsf{Bi}(G)) =: \hat{G}$. Set $b := \mathsf{Bi}(G)$. Let $\mathcal{B}$ be a direct Ω-decomposition of b, and therefore also of $\mathsf{Bi}(G)$. For each $c : X_c \times X_c \to Z_c \in \mathcal{B}$, define $\mathsf{Grp}(c, b) = X_c \times Z_c \leq V \times W$. We claim that $\mathsf{Grp}(c; b)$ is an Ω-subgroup of $\mathsf{Grp}(b)$. In particular, $(0, 0) \in \mathsf{Grp}(c; b)$ and for all $(x, w), (y, w') \in \mathsf{Grp}(c; b)$, $(x, w) * (-y, -w' + b(y, y)) = (x - y, w - b(x, y) - w' + b(y, y)) \in X_c \times Z_c = \mathsf{Grp}(c; b)$. Furthermore,

$$\left[\mathsf{Grp}(c; b), \mathsf{Grp}\left(\sum_{d\in\mathcal{C}-\{c\}} d; b\right)\right] = \left(0, 2b\left(X_c, \sum_{d\in\mathcal{C}-\{c\}} X_d\right)\right) = (0, 0).$$

Combined with $\mathsf{Grp}(b) = \langle \mathsf{Grp}(c; b) : c \in \mathcal{C}\rangle$ it follows that $\mathsf{Grp}(c; b)$ is normal in $\mathsf{Grp}(b)$. Finally,

$$\mathsf{Grp}(c; b) \cap \mathsf{Grp}\left(\sum_{d\in\mathcal{C}-\{c\}} d; b\right) = (X_c \times Z_c) \cap \sum_{d\in\mathcal{C}-\{c\}} (X_d \times Z_d) = 0 \times 0.$$

Thus, $\mathcal{H} = \{\mathsf{Grp}(c; b) : c \in \mathcal{C}\}$ is a direct Ω-decomposition of $\mathsf{Grp}(b)$. As G is directly Ω-indecomposable it follows that $\mathcal{H} = \{G\}$ and so $\mathcal{C} = \{b\}$. Thus, b is directly Ω-indecomposable. □

5.2. **Centroids of bilinear maps.**

In this section we replicate the classic interplay of idempotents of a ring and direct decompositions of an algebraic object, but now for context of bilinear maps. The relevant ring is the centroid, defined similar to centroid of a nonassociative ring [11, Section X.1]. As with nonassociative rings, the idempotents of the centroid of a bilinear map correspond to direct decompositions. Myasnikov [23] may have been the first to generalize such methods to bilinear maps.

Definition 5.16. The *centroid* of an Ω-bilinear $b : V \times V \to W$ is

$$C_\Omega(b) = \{(f, g) \in \operatorname{End}_\Omega V \oplus \operatorname{End}_\Omega W : b(uf, v) = b(u, v)g = b(u, vf), \forall u, v \in V\}.$$

If $\Omega = \emptyset$ then write $C(b)$.

Lemma 5.17. *Let $b : V \times V \to W$ be an Ω-bilinear map. Then the following hold.*

(i) $C_\Omega(b)$ is a subring of $\operatorname{End}_\Omega V \oplus \operatorname{End}_\Omega W$, and V and W are $C_\Omega(b)$-modules.

(ii) If b is K-bilinear for a ring K, then $K/(0 :_K V) \cap (0 :_K W)$ embeds in $C(b)$. In particular, $C(b)$ is the largest ring over which b is faithful bilinear.

(iii) If b is nondegenerate and $W = b(V, V)$ then $C_\Omega(b) = C(b)$ and $C(b)$ is commutative.

Proof. Parts (i) and (ii) are immediate from the definitions. For part (iii), if $s \in \Omega$ and $(f, g) \in C(b)$, then $b((su)f, v) = b(su, vf) = sb(u, vf) = b(s(uf), v)$ for all u and all $v \in V$. As b is nondegenerate and $b((su)f - s(uf), V) = 0$, it follows that $(su)f = s(uf)$. In a similar fashion, $g \in \operatorname{End}_\Omega W$ so that $(f, g) \in C_\Omega(b)$. For part (iii) we repeat the same shuffling game above: if $(f, g), (f', g') \in C(b)$ then $b(u(ff'), v) = b(u, vf)f' = b(u(f'f), v)$. By the nondegenerate assumption we get that $ff' = f'f$ and also $gg' = g'g$. □

Remark 5.18. If $\operatorname{rad} b = 0$ and $(f, g), (f', g) \in C(b)$ then $f = f'$. If $W = b(V, V)$ and $(f, g), (f, g') \in C(b)$ then $g = g'$. So if $\operatorname{rad} b = 0$ and $W = b(V, V)$ then the first variable determines the second and vice-versa.

5.3. **Idempotents, frames, and direct Ω-decompositions.** In this section we extend the usual interplay of idempotents and direct decompositions to the context of bilinear maps and them p-groups of class 2. This allows us to prove Theorem 1.2. This section follows the notation described in Subsection 2.5.

Lemma 5.19. *Let $b : V \times V \to W$ be an Ω-bilinear map.*

(i) A set $\mathcal{B}$ of Ω-submaps of b is a direct Ω-decomposition of b if, and only if,

$$\mathcal{E}(\mathcal{B}) = \{(e(V_c), e(W_c)) : c : V_c \times V_c \to W_c \in \mathcal{B}\}. \tag{5.20}$$

is a set of pairwise orthogonal idempotents of $C_\Omega(b)$ which sum to 1.

(ii) $\mathcal{B}$ is a Remak Ω-decomposition of b if, and only if, $\mathcal{E}(\mathcal{B})$ is a frame.

(iii) If b is nondegenerate and $W = b(V, V)$, then b has a unique Remak Ω-decomposition of b.

Proof. For (i), by Definition 5.9, $\{V_b : b \in \mathcal{B}\}$ is a direct decomposition of V and $\{W_b : b \in \mathcal{B}\}$ is a direct decomposition of W. Thus, $\mathcal{E}(\mathcal{B})$ is a set of pairwise orthogonal idempotents which sum to 1.

Let $(e, f) \in \mathcal{E}(\mathcal{X})$. As $1 - e = \sum_{(e',f')\in\mathcal{E}(\mathcal{B})-\{(e,f)\}} e'$ it follows that for all $u, v \in V$ we have $b(ue, v(1-e)) \in b(Ve, V(1-e)) = 0$ by the assumptions on $\mathcal{B}$. Also, $b(ue, ve) \in Wf$. Together we have:

$$\begin{aligned}
b(ue, v) &= b(ue, ve) + b(ue, v(1-e)) = b(ue, ve),\\
b(u, ve) &= b(u(1-e), ve) + b(ue, ve) = b(ue, ve), \text{ and}\\
b(u, v)f &= \left(\sum_{(e',f')\in\mathcal{E}(\mathcal{B})} b(ue', ve')f'\right) f = b(ue, ve)f = b(ue, ve).
\end{aligned}$$

Thus $b(ue, v) = b(u, v)f = b(u, ve)$ which proves $(e, f) \in C_\Omega(b)$; hence, $\mathcal{E}(\mathcal{B}) \subseteq C_\Omega(b)$.

Now suppose that $\mathcal{E}$ is a set of pairwise orthogonal idempotents of $C_\Omega(b)$ which sum to 1. It follows that $\{Ve : (e, f) \in \mathcal{E}\}$ is a direct Ω-decomposition of V and $\{Wf : (e, f) \in \mathcal{E}\}$ is a direct Ω-decomposition of W. Finally, $b(ue, ve') = b(uee', v) = 0$. Thus, $\{b|_{(e,f)} : V_e \times V_e \to W_f : (e, f) \in \mathcal{E}\}$ is a direct Ω-decomposition of $C(b)$.

Now (ii) follows. For (iii), we now by Lemma 5.17(ii) that $C(b) = C_\Omega(b)$ is commutative Artinian. The rest follows from Lemma 2.21(iv). □

Theorem 5.21. *If G is a p-group and $\gamma_2(G) \leq \zeta_1(G)$, then there is a unique frame $\mathcal{E}$ in $C(\mathsf{Bi}(G))$. Furthermore, if $\gamma_2(G) = \zeta_1(G)$ then every Remak Ω-decomposition $\mathcal{H}$ of G matches a unique partition of $(\mathcal{K}, \mathcal{Q})$ where*

$$\begin{aligned}
\mathcal{K} &:= \{W\hat{e} : (e, \hat{e}) \in \mathcal{E}\},\\
\mathcal{Q} &:= \{Ve : (e, \hat{e}) \in \mathcal{E}\}.
\end{aligned}$$

If $G^p = 1$ then every Remak Ω-decomposition of G matches $(\mathcal{K}, \mathcal{Q})$.

Proof. This follows from Proposition 5.12, Lemma 5.19, and Corollary 5.15. □

5.4. **Proof of Theorem 1.2.** This follows from Theorem 5.21. □

5.5. **Centerless groups.** We close this section with a brief consideration of groups with a trivial center.

Lemma 5.22. *Let G be an Ω-group with $\zeta_1(G) = 1$ and N a minimal $(\Omega \cup G)$-subgroup of G. Then the following hold.*

(i) G has a unique Remak Ω-decomposition $\mathcal{R}$.
(ii) There is a unique $R \in \mathcal{R}$ such that $N \leq R$.
(iii) $\{C_R(N), \langle \mathcal{R} - \{R\}\rangle\}$ is a direct $(\Omega \cup G)$-decomposition of $C_G(N)$.
(iv) Every Remak $(\Omega \cup G)$-decomposition $\mathcal{H}$ of $C_G(N)$ refines $\{C_R(N), \langle \mathcal{R} - \{R\}\rangle\}$.

Proof. Given Remak Ω-decompositions $\mathcal{R}$ and $\mathcal{S}$ of G, by Lemma 3.5 and the assumption that $\zeta_1(G) = 1$, it follows that $\mathcal{R} = \mathcal{R}\zeta_1(G) = \mathcal{S}\zeta_1(G) = \mathcal{S}$. This proves (i).

For (ii), if N is a minimal $(\Omega \cup G)$-subgroup of G then $[R, N] \leq R \cap N \in \{1, N\}$, for all $R \in \mathcal{R}$. If $[R, N] = 1$ for all $R \in \mathcal{R}$ then $N \leq \zeta_1(G) = 1$ which contradicts the assumption that N is minimal. Thus, for some $R \in \mathcal{R}$, $N \leq R$. The uniqueness follows as $R \cap \langle \mathcal{R} - \{R\}\rangle = 1$.

By (ii), $[N, \langle R - \{R\}\rangle] = [R, \langle \mathcal{R} - \{R\}\rangle] = 1$ which shows $\langle \mathcal{R} - \{R\}\rangle \leq C_G(N)$. Hence, $C_G(N) = C_R(N) \times \langle \mathcal{R} - \{R\}\rangle$. This proves (iii).

Finally we prove (iv). Let $\mathcal{K}$ be a Remak $(\Omega \cup G)$-decomposition of $C_G(N)$. Let $\mathcal{S}$ be a Remak $(\Omega \cup G)$-decomposition of $C_G(N)$ which refines the direct $(\Omega \cup G)$-decomposition $C_G(N) = C_R(N) \times \langle \mathcal{R} - \{R\}\rangle$ given by (iii). Note that $\mathcal{R} - \{R\} \subseteq \mathcal{S}$ as members of $\mathcal{R}$ cannot be refined further. By Theorem 2.10, there is a $\mathcal{J} \subseteq \mathcal{K}$ such that we may exchange $\mathcal{R} - \{R\} \subseteq \mathcal{S}$ with $\mathcal{J}$; hence, $\{C_R(N)\} \sqcup \mathcal{J}$ is a direct $(\Omega \cup G)$-decomposition of $C_G(N)$. Now $R \cap \langle \mathcal{J}\rangle \leq C_R(N) \cap \langle \mathcal{J}\rangle = 1$. Also

$$\langle R, \mathcal{J}\rangle = \langle R, C_R(N), \mathcal{J}\rangle = \langle R, \mathcal{R} - \{R\}\rangle = G. \tag{5.23}$$

As every member of $\mathcal{J}$ is an $(\Omega \cup G)$-subgroup of G, it follows that the are normal in G and so $\{R\} \sqcup \mathcal{J}$ is a direct Ω-decomposition of G. As the members of $\mathcal{J}$ are Ω-indecomposable it follows that $\{R\} \sqcup \mathcal{J}$ is a Remak Ω-decomposition of G. However, G has a unique Remak Ω-decomposition so $\mathcal{J} = \mathcal{R} - \{R\}$. As $\mathcal{J}$ was a subset of an arbitrary Remak $(\Omega \cup G)$-decomposition of $C_G(N)$ it follows that every Remak $(\Omega \cup G)$-decomposition of $C_G(N)$ contains $\mathcal{R} - \{R\}$. □

Proposition 5.24. *For groups G with $\zeta_1(G) = 1$, the set $\mathcal{M}$ of minimal $(\Omega \cup G)$-subgroups is a direct $(\Omega \cup G)$-decomposition of the socle of G and furthermore there is a unique partition of $\mathcal{M}$ which extends to the Remak Ω-decomposition of G.*

The following consequence shows how the global Remak decomposition of a group with trivial solvable radical is determined precisely from a unique partition of the Remak decomposition of it socle.

Corollary 5.25. *If G has trivial solvable radical and $\mathcal{R}$ is its Remak decomposition then $\mathcal{R} = \{C_G(C_G(\mathrm{soc}(R))) : R \in \mathcal{R}\}$.*

6. The Remak Decomposition Algorithm

In this section we prove Theorem 1.1. The approach is to break up a given group into sections for which a Remak $(\Omega \cup G)$-decomposition can be computed directly. The base cases include Ω-modules (Corollary 2.34), p-groups of class 2 (which follows from Theorem 5.21), and groups with a trivial center. We use Theorem 3.6 as justification that we can interlace these base cases to sequentially lift direct decomposition via the algorithm `Merge` of Theorem 4.13.

6.1. **Finding Remak Ω-decompositions for nilpotent groups of class 2.** In this section we prove Theorem 1.1 for the case of nilpotent groups G of class 2. The algorithm depends on Theorem 5.21 and Theorem 4.13.

To specify a $\mathbb{Z}$-bilinear map $b : V \times V \to W$ for computation we need only provide the *structure constants* with respect to fixed bases of V and W. Specifically let $\mathcal{X}$ be a basis of V and $\mathcal{Y}$ a basis of W. Define $B_{xy}^{(z)} \in \mathbb{Z}$ so that the following equation is satisfied:

$$b\left(\sum_{x\in\mathcal{X}} \alpha_x x, \sum_{y\in\mathcal{X}} \beta_y y\right) = \sum_{z\in\mathcal{Z}} \left(\sum_{x,y\in\mathcal{X}} \alpha_x B_{xy}^{(z)} \beta_y\right) z \qquad (\forall x \in \mathcal{X}, \forall \alpha_x, \beta_x \in \mathbb{Z}).$$

Lemma 6.1. *There is a deterministic polynomial-time algorithm, which given Ω-modules V and W and a nondegenerate Ω-bilinear map $b : V \times V \to W$ with $W = b(V, V)$, returns a Remak Ω-decomposition of b.*

Proof. Algorithm. Solve a system of linear equations in the (additive) abelian group $\mathrm{End}_\Omega V \times \mathrm{End}_\Omega W$ to find generators for $C_\Omega(b)$. Use Frame to find a frame $\mathcal{E}$ of $C_\Omega(b)$. Return $\{b|_{(e,f)} : Ve \times Ve \to Wf : (e, f) \in \mathcal{E}\}$.

Correctness. This is supported by Lemma 5.19 and Theorem 2.32.

Timing. This follows from the timing of Solve and Frame. □

Theorem 6.2. *There is a polynomial-time algorithm which, given a nilpotent Ω-group of class 2, returns a Remak Ω-decomposition of the group.*

Proof. Let $G \in \mathbb{G}_n^\Omega$ with $\gamma_2(G) \leq \zeta_1(G)$.

Algorithm. Use Order to compute $|G|$. For each prime p dividing $|G|$, write $|G| = p^e m$ where $(p, m) = 1$ and set $P := G^m$. Set $b_p := \mathsf{Bi}(P)$. Use the algorithm of Lemma 6.1 to find a direct Ω-decomposition $\mathcal{B}$ of b. Define each of the following:

$$\mathcal{X}(\mathcal{B}) = \{X_c : c : X_c \times X_c \to Z_c \in \mathcal{B}\}$$
$$\mathcal{H} = \{H \leq P : \zeta_1(P) \leq H, H/\zeta_1(P) \in \mathcal{X}(\mathcal{B})\}.$$

Use Corollary 2.34 to build a Remak Ω-decomposition $\mathcal{Z}$ of $\zeta_1(P)$. Set $\mathcal{R}_p := \mathtt{Merge}(\mathcal{Z}, \mathcal{H})$. Return $\bigcup_{p||G|} \mathcal{R}_p$.

Correctness. By Lemma 6.1 the set $\mathcal{B}$ is the unique Remak Ω-decomposition of $\mathsf{Bi}(G)$. By Theorem 5.21 and Theorem 4.13 the return a Remak Ω-decomposition of G.

Timing. The algorithm uses a constant number of polynomial time subroutines. □

We have need of one final observation which allows us to modify certain decompositions into ones that match the hypothesis Theorem 4.13(b) when the up grading pair is $(\mathfrak{N}_c, G \mapsto \zeta_c(G))$.

Lemma 6.3. *There is a polynomial-time algorithm which, given an Ω-decomposition $\mathcal{H} = \mathcal{H}\zeta_c(G)$ of a group G, returns the finest Ω-decomposition $\mathcal{K}$ refined by $\mathcal{H}$ and such that for all $K \in \mathcal{K}$, $\zeta_c(K) = \zeta_c(G)$. (The proof also shows there is a unique such $\mathcal{K}$.)*

Proof. Observe that $\mathcal{K} = \{\langle H \in \mathcal{H} : [K, H, \ldots, H] \neq 1\rangle : K \in \mathcal{K}\}$. We can create $\mathcal{K}$ by a transitive closure algorithm. □

Theorem 6.4. Find-Ω-Remak *has polynomial-time solution.*

$$\begin{tikzcd}
& & 1 & 1 & \\
1 \arrow[r] & \zeta_2(G) \arrow[r] & G \arrow[r] \arrow[u] & G/\zeta_2(G) \arrow[r] \arrow[u] & 1 \\
1 \arrow[r] & \zeta_1(G) \arrow[r] \arrow[u] & G \arrow[r] \arrow[u, equal] & G/\zeta_1(G) \arrow[r] \arrow[u] & 1 \\
& 1 \arrow[u] & 1 \arrow[u] & &
\end{tikzcd}$$

Figure 2. The relative extension $1 < \zeta_1(G) \leq \zeta_2(G) < G$. The rows and columns are exact.

Proof. Let $G \in \mathbb{G}_n^{\Omega}$.

Algorithm. If $G = 1$ then return $\emptyset$. Otherwise, compute $\zeta_1(G)$. If $G = \zeta_1(G)$ then use Abelian.Remak-Ω-Decomposition and return the result. Else, if $\zeta_1(G) = 1$ then use Minimal-Ω-Normal to find a minimal $(\Omega \cup G)$-subgroup N of G. Use Normal-Centralizer to compute $C_G(N)$. If $C_G(N) = 1$ then return $\{G\}$. Otherwise, recurse with $C_G(N)$ in the role of G to find a Remak Ω-decomposition $\mathcal{K}$ of $C_G(N)$. Call $\mathcal{H} := \text{Extend}(G, \mathcal{K})$ to create a direct Ω-decomposition $\mathcal{H}$ extending $\mathcal{K}$ maximally. Return $\mathcal{H}$.

Now $G > \zeta_1(G) > 1$. Compute $\zeta_2(G)$ and use Theorem 6.2 to construct a Remak $(\Omega \cup G)$-decomposition $\mathcal{A}$ of $\zeta_2(G)$. If $G = \zeta_2(G)$ then return $\mathcal{A}$; otherwise, $G > \zeta_2(G)$ (consider Figure 2). Use a recursive call on $G/\zeta_1(G)$ to find $\mathcal{H} = \mathcal{H}\zeta_1(G)$ such that $\mathcal{H}/\zeta_1(G)$ is a Remak Ω-decomposition of $G/\zeta_1(G)$. Apply Lemma 6.3 to $\mathcal{H}$ and then set $\mathcal{J} := \text{Merge}(\mathcal{A}, \mathcal{H})$, and return $\mathcal{J}$.

Correctness. The case $G = \zeta_1(G)$ is proved by Corollary 2.34 and the case $G = \zeta_2(G)$ is proved in Theorem 6.2.

Now suppose that $G > \zeta_1(G) = 1$. Following Lemma 5.22, G has a unique Remak Ω-decomposition $\mathcal{R}$ and there is a unique $R \in \mathcal{R}$ such that $N \leq R$ and $\langle \mathcal{R} - \{R\} \rangle \leq C_G(N)$. So if $C_G(N) = 1$ then G is directly indecomposable and the return of the algorithm is correct. Otherwise the algorithm makes a recursive call to find a Remak $(\Omega \cup G)$-decomposition $\mathcal{K}$ of $C_G(N)$. By Lemma 5.22(iv), $\mathcal{K}$ contains $\mathcal{R} - \{R\}$ and so there is a unique maximal extension of $\mathcal{K}$, namely $\mathcal{R}$, and so by Theorem 4.10, the algorithm Extend creates the Remak Ω-decomposition of G so the return in this case is correct.

Finally suppose that $G > \zeta_2(G) \geq \zeta_1(G) > 1$. There we have the commutative diagram Figure 2 which is exact in rows and columns. By Theorem 3.6, $\mathcal{H}\zeta_2(G)$ refines $\mathcal{R}\zeta_2(G)$ and so the algorithm Merge is guaranteed by Theorem 4.13 to return a Remak Ω-decomposition of G (consider Figure 3).

Timing. The algorithm enters a recursive call only if $\zeta_1(G) = 1$ or $G > \zeta_2(G) \geq \zeta_1(G) > 1$. As these two case are exclusive there is at most one recurse call made by the algorithm. The remainder of the algorithm uses polynomial time methods as indicated. □

6.2. **Proof of Theorem 1.1.** This is a corollary to Theorem 6.4 □

(6.5)

$$\begin{tikzcd}
 & & 1 & 1 & \\
1 \arrow[r] & \prod \mathcal{A} \arrow[r] & \prod \texttt{Merge}(\mathcal{A}, \mathcal{H}) \arrow[r] \arrow[u] \arrow[d, equal] & \prod \mathcal{H}/\zeta_2(G) \arrow[r] \arrow[u] & 1 \\
1 \arrow[r] & \zeta_1(G) \arrow[r] \arrow[u] & G \arrow[r] & \prod \mathcal{H}/\zeta_1(G) \arrow[r] \arrow[u] & 1 \\
 & 1 \arrow[u] & 1 \arrow[u] & &
\end{tikzcd}$$

Figure 3. The recursive step parameters feed into `Merge` to produce a Remak Ω-decomposition of G.

Corollary 6.6. FindRemak *has a deterministic polynomial-time solution for matrix* Γ_d*-groups.*

Proof. This follows from Section 2.6, Remark 2.35, and Theorem 6.4. □

6.3. **General operator groups.** Now we suppose that $G \in \mathbb{G}_n$ is a Ω-group for a general set Ω of operators. That is, $\Omega\theta \subseteq \operatorname{End} G$. To solve Remak-$\Omega$-Decomposition in full generality it suffices to reduce to the case where Ω acts as automorphisms on G, where we invoke Theorem 6.4. For that suppose we have $\omega\theta \in \operatorname{End} G - \operatorname{Aut} G$. By Fitting lemma we have that:

$$G = \ker \omega^{\ell(G)} \times \operatorname{im} \omega^{\ell(G)}. \tag{6.7}$$

To compute such a decomposition we compute $\operatorname{im} \omega^{\ell(G)}$ and then apply Direct-Ω-Complement to compute $\ker \omega^{\ell(G)}$. As Ω is part of the input, we may test each $\omega \in \Omega$ to find those ω where $\omega\theta \notin \operatorname{Aut} G$, and with each produce a direct Ω-decomposition. The restriction of ω to the constituents induces either zero map, or an automorphism. Thus the remaining cases are handled by Theorem 6.4. □

7. An example

Here we give an example of the execution of the algorithm for Theorem 6.4 which covers several of the interesting components (but of course fails to address all situations). We will operate without a specific representation in mind, since we are interested in demonstrating the high-level techniques of the algorithm for Theorem 6.4.

We trace through how the algorithm might process the group

$$G = D_8 \times Q_8 \times \mathrm{SL}(2,5) \times \big(\mathrm{SL}(2,5) \circ \mathrm{SL}(2,5)\big).$$

First the algorithm recurses until it reaches the group

$$\hat{G} = G/\zeta_2(G) \cong \mathrm{PSL}(2,5)^3.$$

At this point it finds a minimal normal subgroup N of $\hat{G}$, of which there are three, so we pick $N = \mathrm{PSL}(2,5) \times 1 \times 1$. Next the algorithm computes a Remak decomposition of $C_G(N) = 1 \times \mathrm{PSL}(2,5) \times \mathrm{PSL}(2,5)$. At this point the algorithm returns the unique Remak decomposition

$$\mathcal{Q} := \{\mathrm{PSL}(2,5) \times 1 \times 1, 1 \times \mathrm{PSL}(2,5) \times 1, 1 \times 1 \times \mathrm{PSL}(2,5)\}.$$

These are pulled back to the set $\{H_1, H_2, H_3\}$ of subgroups in G.

Next the algorithm constructs a Remak G-decomposition of $\zeta_2(G)$. For that the algorithm constructs the bilinear map of commutation from $\zeta_2(G)/\zeta_1(G) \cong \mathbb{Z}_2^4$ into $\gamma_2(\zeta_2(G)) = \langle z_1, z_2\rangle \cong \mathbb{Z}_2^2$, i.e.

$$b := \mathsf{Bi}(\zeta_2(G)) : \mathbb{Z}_2^4 \times \mathbb{Z}_2^4 \to \mathbb{Z}_2^2$$

Below we have described the structure constants for b in a nice basis but remark that unless we already know the direct factors of $\zeta_2(G)$ it is unlikely to have such a natural form.

$$b(u,v) = u \begin{bmatrix} 0 & z_1 & & \\ -z_1 & 0 & & \\ & & 0 & z_2 \\ & & -z_2 & 0 \end{bmatrix} v^t, \qquad \forall u, v \in \mathbb{Z}_2^4. \tag{7.1}$$

A basis for the centroid of b is computed:

$$C(b) = \left\{ \left(\begin{bmatrix} a & 0 & & \\ 0 & a & & \\ & & b & 0 \\ & & 0 & b \end{bmatrix}, \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \right) : a, b \in \mathbb{Z}_2 \right\} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2. \tag{7.2}$$

Next, the unique frame $\mathcal{E} = \{(I_2 \oplus 0_2, 1 \oplus 0), (0_2 \oplus I_2, 0 \oplus 1)\}$ of $C(b)$ is built and used to create the subgroups $\mathcal{K} := \{D_8 \times Z(Q_8), Z(D_8) \times Q_8\}$ in $\zeta_2(G)$. Here, using an arbitrary basis $\mathcal{X}$ for $\zeta_1(G) = \mathbb{Z}_2^2 \times \mathbb{Z}_4^2$, the algorithm $\texttt{Merge}(\mathcal{X}, \mathcal{K})$ constructs a Remak decomposition $\mathcal{A} := \{H, K, C_1, C_2\}$ of $\zeta_2(G)$ where $H \cong D_8$, $K \cong Q_8$, and $C_1 \cong C_2 \cong \mathbb{Z}_4$.

Finally, the algorithm $\texttt{Merge}(\mathcal{A}, \mathcal{H})$ returns a Remak decomposition of G. To explain the merging process we trace that algorithm through as well.

Let $R = \mathrm{SL}(d,q) \times 1 \times 1$ and $S = 1 \times (\mathrm{SL}(d,q) \circ \mathrm{SL}(d,q))$. These groups are directly indecomposable direct factors of G and serve as the hypothesized directions of for the direct chain used by $\texttt{Merge}$. Without loss of generality we index the H's so that $H_2 = R\zeta_2(G)$ and $H_1H_3 = S\zeta_2(G)$ and

$$G/\zeta_2(G) = \mathrm{PSL}(d,q) \times \mathrm{PSL}(d,q) \times \mathrm{PSL}(d,q) = H_2/\zeta_2(G) \times H_1/\zeta_2(G) \times H_3/\zeta_2(G).$$

Furthermore, $\zeta_2(H_i) = \zeta_2(G)$ for all $i \in \{1,2,3\}$. Therefore, $(\mathcal{A}, \mathcal{H})$ satisfies the hypothesis of Theorem 4.13.

The loop in $\texttt{Merge}$ begins with $\mathcal{K}_0 = \mathcal{A}$ and seeks to extend $\mathcal{A}$ to H_1 by selecting an appropriate subset $\mathcal{A}_1 \subseteq \mathcal{K}_0 = \mathcal{A}$ and finding a complement $\lfloor H_1 \rfloor \leq H_1$ such that $\mathcal{K}_1 = \mathcal{A}_1 \sqcup \{\lfloor H_1 \rfloor\}$ is a direct decomposition of H_1. The configuration at this stage is seen in Figure 4. By Theorem 4.10, we have $H, K \in \mathcal{A}_1$ (as those lie outside the center) and one of the C_i's (though no unique choice exists there).

In the second loop iteration we extend $\mathcal{K}_1$ to a $\mathfrak{N}_2$-refined direct decomposition if H_1H_2. This selects a subset $\mathcal{A}_2 \subseteq \mathcal{K}_1 \cap \zeta_2(G)$. Also H_1 and H_2 are in different directions, specifically $H_2 = R\zeta_2(G)$ and $H_1 \leq S\zeta_2(G)$, so the algorithm is forced to include $\lfloor H_1 \rfloor \in \mathcal{K}_2$ (cf. Theorem 4.10(iii)) and then creates a complement $\lfloor H_2 \rfloor \cong \mathrm{SL}(2,5)$ to $\langle \mathcal{A}_2, \lfloor H_1 \rfloor\rangle$. The configuration is illustrated in Figure 5. As

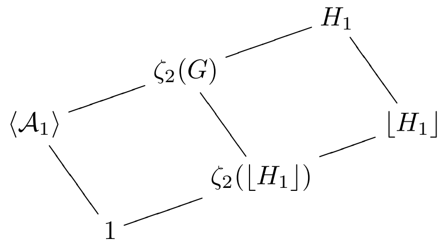

Figure 4. The lattice encountered during the first iteration of the loop in the algorithm $\texttt{Merge}(\mathcal{A}, \{H_1, H_2, H_3\})$.

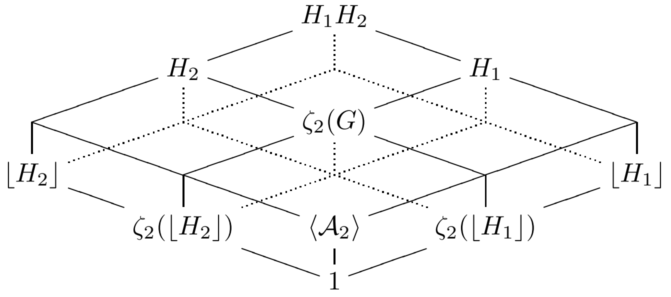
H_1H_2
H_2
H_1
$\zeta_2(G)$
$\lfloor H_2\rfloor$
$\lfloor H_1\rfloor$
$\zeta_2(\lfloor H_2\rfloor)$
$\langle\mathcal{A}_2\rangle$
$\zeta_2(\lfloor H_1\rfloor)$
1

Figure 5. The lattice encountered during the second iteration of the loop in the algorithm $\texttt{Merge}(\mathcal{A}, \{H_1, H_2, H_3\})$.

before, we have $H, K \in \mathcal{K}_2$ as well, but the cyclic groups are now gone as the centers of $\lfloor H_i\rfloor$, $i \in \{1, 2\}$, fill out a direct decomposition of $\zeta_2(G)$.

Finally, in the third loop iteration, the direction is back towards S and so the extension $\mathcal{K}_3$ of $\mathcal{K}_2$ to $H_1H_2H_3$ contains $\lfloor H_2\rfloor$ and is $\mathfrak{N}_2$-refined. However, the group $\lfloor H_1\rfloor$ is not a direct factor of G as it is one term in nontrivial central product. Therefore that group is replaced by a subgroup $\lfloor H_1H_3\rfloor \cong \mathrm{SL}(d, q) \circ \mathrm{SL}(d, q)$. The final configuration is illustrated in Figure 6. $\mathcal{K}_3$ is a Remak decomposition of G.

8. Closing remarks

Historically the problem of finding a Remak decomposition focused on groups given by their multiplication table since even there there did not seem to be a polynomial-time solution. It was known that a Remak decomposition could be found by checking all partitions of all minimal generating sets of a group G and so the problem had a sub-exponential complexity of $|G|^{\log|G|+O(1)}$. That placed it in the company of other interesting problems including testing for an isomorphism between two groups [21]. Producing an algorithm that is polynomial-time in the size of the group's multiplication table (i.e. polynomial in $|G|^2$) was progress, achieved independently in [14] and [34]. Evidently, Theorem 1.1 provides a polynomial-time solution for groups input in this way (e.g. use a regular representation). With a few observations we sharpen Theorem 1.1 in that specific context to the following:

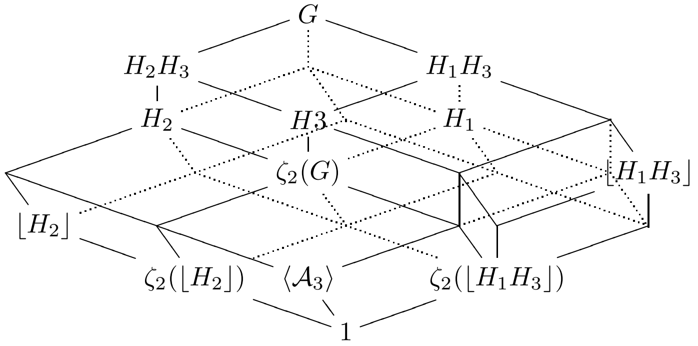
G
H_2H_3
H_1H_3
H_2
$H3$
H_1
$\zeta_2(G)$
$\lfloor H_1H_3 \rfloor$
$\lfloor H_2 \rfloor$
$\zeta_2(\lfloor H_2 \rfloor)$
$\langle \mathcal{A}_3 \rangle$
$\zeta_2(\lfloor H_1H_3 \rfloor)$
1

FIGURE 6. The lattice of encountered during the third iteration of the loop in the algorithm $\texttt{Merge}(\mathcal{A}, \{H_1, H_2, H_3\})$.

Theorem 8.1. *There is a deterministic nearly-linear-time algorithm which, given a group's multiplication table, returns a Remak decomposition of the group.*

Proof. The algorithm for Theorem 6.4 is polynomial in $\log |G|$. As the input length here is $|G|^2$, it suffices to show that the problems listed in Section 2.6 have $O(|G|^2 \log^c |G|)$-time or better solutions. Evidently, ORDER, MEMBER, SOLVE each have brute-force linear-times solutions. PRESENTATION can be solved in linear-time by selecting a minimal generating set $\{g_1, \ldots, g_\ell\}$ (which has size $\log |G|$) and acting on the cosets of $\{\langle g_i, \ldots, g_\ell \rangle : 1 \leq i \leq \ell\}$ produce defining relations of the generators in fashion similar to [32, Exercise 5.2]. For MINIMAL-NORMAL, begin with an element and takes it normal closure. If this is a proper subgroup recurse, otherwise, try an element which is not conjugate to the first and repeat until either a proper normal subgroup is discovered or it is proved that group is simple. That takes $O(|G|^2)$-time. The remaining algorithms PRIMARY-DECOMPOSITION, IRREDUCIBLE, and FRAME have brute force linear-time solutions. Thus, the algorithm can be modified to run in times $O(|G|^2 \log^c |G|)$. □

Section 3 lays out a framework which permits for a local view of the direct products of group. We have some lingering questions in this area.

(1) What is the best series of subgroups to use for the algorithm of Theorem 6.4?

    Corollaries 3.14 and 3.21 offer alternatives series to use in the algorithm. There is an option for a top-down algorithm based on down graders. That may allow for a black-box algorithm since verbal subgroups can be constructed in black-box groups; see [32, Section 2.3.4].

(2) Is their a parallel NC solution for REMAK-Ω-DECOMPOSITION?

    We can speculate how this may proceed. First, select an appropriate series $1 \leq G_1 \leq \cdots \leq G_n = G$ for G and distribute and use parallel linear algebra methods to find Remak decompositions $\mathcal{A}_{i0}$ of each G_{i+1}/G_i, for $1 \leq i < n$. Then for $0 \leq j \leq \log n$, for each $1 \leq i \leq n/2^j$ in parallel compute $\mathcal{A}_{i(j+1)} := \text{MERGE}(\mathcal{A}_{ij}, \mathcal{A}_{(i+1)j})$. When $j = \lfloor \log n \rfloor$ we have a direct decomposition $\mathcal{A}_{1 \log n}$ of G and have used poly-logarithmic time.

Unfortunately, Theorem 4.13(a) is not satisfied in these recursions, so we cannot be certain that the result is a Remak decomposition.

Acknowledgments

I am indebted to W. M. Kantor for taking a great interest in this work and offering guidance. Thanks to E. M. Luks, C.R.B. Wright, and Á. Seress for encouragement and many helpful remarks.

References

[1] S. A. Ašmanov, Verbal subgroups of complete direct products of groups, Uspehi Mat. Nauk 25 (3(153)) (1970) 259–260.

[2] R. Baer, Groups with abelian central quotient group, Trans. Amer. Math. Soc. 44 (3) (1938) 357–386.

[3] C. W. Curtis, I. Reiner, Methods of representation theory. Vol. I, John Wiley & Sons Inc., New York, 1981.

[4] W. Eberly, M. Giesbrecht, Efficient decomposition of associative algebras over finite fields, J. Symbolic Comput. 29 (3) (2000) 441–458.

[5] H. Fitting, Über die direkten Produktzerlegungen einer Gruppe in direkt unzerlegbare Faktoren, Math. Z. 39 (1) (1935) 16–30.

[6] P. Hall, Verbal and marginal subgroups, J. Reine Angew. Math. 182 (1940) 156–157.

[7] I. N. Herstein, Noncommutative rings, The Carus Mathematical Monographs, No. 15, Published by The Mathematical Association of America, 1968.

[8] D. F. Holt, S. Rees, Testing modules for irreducibility, J. Austral. Math. Soc. Ser. A 57 (1) (1994) 1–16.

[9] G. Ivanyos, Fast randomized algorithms for the structure of matrix algebras over finite fields (extended abstract), in: Proceedings of the 2000 International Symposium on Symbolic and Algebraic Computation (St. Andrews), ACM, New York, 2000, pp. 175–183 (electronic).

[10] G. Ivanyos, K. Lux, Treating the exceptional cases of the MeatAxe, Experiment. Math. 9 (3) (2000) 373–381.

[11] N. Jacobson, Lie algebras, Interscience Tracts in Pure and Applied Mathematics, No. 10, Interscience Publishers (a division of John Wiley & Sons), New York-London, 1962.

[12] W. M. Kantor, E. M. Luks, Computing in quotient groups, in: STOC '90: Proceedings of the twenty-second annual ACM symposium on Theory of computing, ACM, New York, NY, USA, 1990, pp. 524–534.

[13] W. M. Kantor, E. M. Luks, P. D. Mark, Sylow subgroups in parallel, Journal of Algorithms 31 (1999) 132–195.

[14] N. Kayal, T. Nezhmetdinov, Factoring groups efficiently, in: Electronic Colloquium on Computational Complexity, No. 74, 2008.

[15] W. Krull, Über verallgemeinerte endliche Abelsche Gruppen., M. Z. 23 (1925) 161–196.

[16] A. G. Kurosh, The theory of groups, Chelsea Publishing Co., New York, 1960, translated from the Russian and edited by K. A. Hirsch. 2nd English ed. 2 volumes.

[17] E. M. Luks, Computing in solvable matrix groups, 1992, pp. 111–120.

[18] E. M. Luks, Finding direct complements, lecture notes, University of Oregon Algebraic Algorithms seminar (August 9, 2005).

[19] J. H. Maclagan-Wedderburn, On the direct product in the theory of finite groups, Ann. of Math. (2) 10 (4) (1909) 173–176.

[20] B. R. McDonald, Finite rings with identity, Marcel Dekker Inc., New York, 1974, pure and Applied Mathematics, Vol. 28.

[21] G. L. Miller, On the $n^{log}\, n$ isomorphism technique: A preliminary report, Tech. Rep. TR17, Rochester, Rochester (March 1977).

[22] T. Miyazaki, Deterministic algorithms for management of matrix groups, in: Groups and computation, III (Columbus, OH, 1999), vol. 8 of Ohio State Univ. Math. Res. Inst. Publ., de Gruyter, Berlin, 2001, pp. 265–280.

[23] A. G. Myasnikov, Definable invariants of bilinear mappings, Sibirsk. Mat. Zh. 31 (1) (1990) 104–115, 220.

[24] H. Neumann, Varieties of groups, Springer-Verlag New York, Inc., New York, 1967.

[25] P. Neumann, Some algorithms for computing with finite permutation groups, in: Proceedings of groups—St. Andrews 1985, vol. 121 of London Math. Soc. Lecture Note Ser., Cambridge Univ. Press, Cambridge, 1986.

[26] O. Ore, On the foundation of abstract algebra. I., Ann. of Math 2 (1935) 406–437.

[27] R. Remak, Über die Zerlegung der endlichen Gruppen in direkte unzerlegbare Faktoren., J. f ur Math. 139 (1911) 293–308.

[28] D. J. S. Robinson, A course in the theory of groups, vol. 80 of Graduate Texts in Mathematics, Springer-Verlag, New York, 1993.

[29] L. Rónyai, Computations in associative algebras, in: Groups and computation (New Brunswick, NJ, 1991), vol. 11 of DIMACS Ser. Discrete Math. Theoret. Comput. Sci., Amer. Math. Soc., Providence, RI, 1993, pp. 221–243.

[30] J. J. Rotman, An introduction to the theory of groups, vol. 148 of Graduate Texts in Mathematics, 4th ed., Springer-Verlag, New York, 1995.

[31] O. Schmidt, Sur les produits directs., S. M. F. Bull. 41 (1913) 161–164.

[32] Á. Seress, Permutation group algorithms, vol. 152 of Cambridge Tracts in Mathematics, Cambridge University Press, Cambridge, 2003.

[33] R. B. Warfield, Jr., Nilpotent groups, Springer-Verlag, Berlin, 1976, lecture Notes in Mathematics, Vol. 513.

[34] J. B. Wilson, Group decompositions, Jordan algebras, and algorithms for p-groups, University of Oregon, 2008, doctoral dissertation.

[35] J. B. Wilson, Decomposing p-groups via jordan algebras, Journal of Algebra 322 (2009) 2642–2679.

[36] J. B. Wilson, Finding central decompositions of p-groups, J. Group theory 12 (2009) 813–830.

[37] C. R. B. Wright, Direct factors – bitesize version, lecture notes, University of Oregon Algebraic Algorithms seminar (August 9, 2005).

Department of Mathematics, The Ohio State University, Columbus, OH 43210
E-mail address: wilson@math.ohio-state.edu