# CLONES OF FINITE GROUPS

KEITH A. KEARNES AND ÁGNES SZENDREI

Abstract. If $G$ is a finite group whose Sylow subgroups are abelian, then the term operations of $G$ are determined by the subgroups of $G \times G \times G$.

## 1. Introduction

Suppose that $G$ is a group and that $f\colon G^n \to G$ is a function. How can we tell if there is a group word $w = w(x_1, \ldots, x_n)$ whose interpretation in $G$ is $f$?

An operation $f\colon G^n \to G$ is called a **term operation** of $G$ if it is represented by a word (or **term**), and the collection of all term operations is called the **clone** of $G$. Our question, therefore, is how to determine membership in the clone of $G$. Since the subgroups of powers of $G$ are closed under all operations represented by words, an obvious necessary condition for $f$ to be a term operation is that all subgroups of $G^\kappa$ be closed under $f$ for all $\kappa$. This necessary condition turns out to be sufficient, and if $G$ is finite, the necessary and sufficient condition is that all subgroups of $G^k$ be closed under $f$ for all finite $k$ (see Corollary 1.4 of [5]). In fact, it may be true that one does not have to check that all finite powers of $G$ are closed under $f$, but only that for some large $k$ the subgroups of $G^k$ are closed under $f$. In this paper we prove that if $G$ has abelian Sylow subgroups and all subgroups of $G^3$ are preserved by $f$, then $f$ is a term operation.

A problem with a long history was to determine whether every group is determined up to isomorphism by the subgroup lattices of its finite powers (cf. [4], in particular Problem 7.6.11). This problem was often formulated in the following stronger form: If $\mathrm{Sub}(G^3)$ is isomorphic to $\mathrm{Sub}(H^3)$, then must $G$ be isomorphic to $H$? Both problems were resolved negatively in [3], but the result in this paper gives a related positive result. Suppose that $G$ and $H$ are finite groups with abelian Sylow subgroups, defined on the same set, and $\mathrm{Sub}(G^3) = \mathrm{Sub}(H^3)$. Then $G$ and $H$ are **term equivalent** (which means that they have the same term operations). Thus, $\mathrm{Sub}(G^3) = \mathrm{Sub}(H^3)$ implies $\mathrm{Sub}(G^\kappa) = \mathrm{Sub}(H^\kappa)$ for all $\kappa$ (but this is not enough to imply that $G \cong H$).

1991 *Mathematics Subject Classification.* Primary 20E15, Secondary 20D30, 08A40.

*Key words and phrases.* Clone, term equivalence.

This material is based upon work supported by the Hungarian National Foundation for Scientific Research (OTKA) grants no. T 034175, and T37877.

## 2. Groups With Abelian Sylow Subgroups

Our goal is to prove the following theorem.

**Theorem 2.1.** *Let $G$ be a finite group whose Sylow subgroups are abelian. A finitary operation $f$ on the underlying set of $G$ is a term operation of $G$ if and only if all subgroups of $G \times G \times G$ are closed under $f$.*

In fact, we will prove more. In Theorem 2.21 we will exhibit a relatively small family $\mathcal{F}$ of subgroups of $G \times G \times G$ such that for $f$ to be a term operation it is enough to test that all members of $\mathcal{F}$ are closed under $f$. Either of Theorems 2.1 or 2.21 implies that if $G$ and $H$ are defined on the same set and $\mathrm{Sub}(G^3) = \mathrm{Sub}(H^3)$, then $G$ and $H$ are term equivalent.

The proof of Theorem 2.1 (or Theorem 2.21) will proceed as follows. First we reduce the study of all subgroups of finite powers of $G$ to the study of a family of subgroups of products of sections of $G$. (A **section** is a quotient of a subgroup.) We give a complete description for these 'reduced' subgroups, and use this description to define a family $\mathcal{F}$ of subgroups of $G^3$ such that, for $f$ to be a term operation of $G$, it is enough to test that all members of $\mathcal{F}$ are closed under $f$. From this we conclude the proof of Theorem 2.21.

Let $n$ be a positive integer, and for $1 \leq i \leq n$ let $S_i$ be arbitrary finite groups. For any nonempty subset $I$ of $\{1, \ldots, n\}$ we let $\mathrm{pr}_I$ denote the projection homomorphism

$$\mathrm{pr}_I \colon \prod_{i=1}^{n} S_i \to \prod_{i \in I} S_i.$$

**Definition 2.2.** A subgroup $S$ of $\prod S_i$ is **subdirect** if $\mathrm{pr}_i(S) = S_i$ for every $i$. The **$i$-th coordinate kernel** $N_i$ of $S$ is the subgroup of $S_i$ defined by

$$N_i = \{s \in S_i : (1, \ldots, 1, \overset{i}{\smile}{s}, 1, \ldots, 1) \in S\}.$$

A subdirect subgroup $H$ of a product $\prod H_i$ of two or more groups is **reduced** if

(1) $|H_i| > 1$ for all $i$,
(2) $H$ has trivial coordinate kernels, and
(3) $H$ is meet irreducible in the lattice of subgroups of $\prod H_i$.

Note that conditions (1) and (2) imply that $H$ is a proper subgroup of $\prod H_i$. Hence it follows from (3) that if $H$ is reduced, then it has a unique upper cover in the lattice of subgroups of $\prod H_i$.

The next lemma reduces the study of subgroups of finite powers of $G$ to the study of reduced subgroups of direct products of sections of $G$.

**Lemma 2.3.** *Let $G$ be a group, and let $S$ be a subgroup of $G^n$ for some $n \geq 2$. For $1 \leq i \leq n$ let $S_i = \mathrm{pr}_i(S)$ be the $i$-th projection, and let $N_i$ be the $i$-th coordinate kernel of $S$.*

(1) *$N_i$ is a normal subgroup of $S_i$ for each $i$, and $N = \prod N_i$ is a normal subgroup of $S$;*
(2) *the quotient group $H = S/N$ is a subdirect subgroup of the group $\prod H_i$ where $H_i = S_i/N_i$; and*
(3) *$H$ has trivial coordinate kernels; equivalently, the projection homomorphism $\mathrm{pr}_I\colon H \to \mathrm{pr}_I(H)$ is bijective for any $(n-1)$-element subset $I$ of $\{1,\dots,n\}$.*

*Moreover,*

(4) *if $S$ is meet irreducible in the lattice of subgroups of $G^n$ then $H$ is meet irreducible in the lattice of subgroups of $\prod H_i$.*

*Proof.* For (1), the subgroup $K_i$ of $S$ consisting of all elements $(1,\dots,1,\overset{i}{\smile}{s},1,\dots,1) \in S$ is the intersection of $S$ with the kernel of the homomorphism $\mathrm{pr}_I$ for $I = \{1,2,\dots,i-1,i+1,\dots,n\}$, so $K_i$ is normal in $S$. Since $K_i \lhd S$, $\mathrm{pr}_i(K_i) = N_i$, and $\mathrm{pr}_i(S) = S_i$, it follows that $N_i \lhd S_i$. The product $\prod N_i$ is the join of the $K_i$, so this product is normal in $S$.

For (2), compose the projection homomorphism $\mathrm{pr}_i\colon S \to S_i$ with the natural homomorphism $S_i \to S_i/N_i$. This is a surjective homomorphism from $S$ to $S_i/N_i$ whose kernel consists of all tuples $(s_1,\dots,s_n) \in S$ where $s_i \in N_i$. The induced homomorphism $S \to \prod S_i/N_i$ maps $S$ onto each factor and has kernel $N$. The homomorphism $S/N \to \prod S_i/N_i$ that is guaranteed by the First Isomorphism Theorem realizes $S/N = H$ as a subdirect subgroup of $\prod S_i/N_i = \prod H_i$.

In (3) the equivalence of the two claims follows by observing that the kernel of the projection homomorphism $\mathrm{pr}_I\colon H \to \mathrm{pr}_I(H)$ for $I = \{1,\dots,i-1,i+1,\dots,n\}$ is the $i$-th coordinate kernel of $H$. By symmetry it suffices to show that the first coordinate kernel of $H$ is trivial. If $N_1h$ belongs to the first coordinate kernel of $H$, that is $(N_1h, N_2,\dots,N_n) \in H$, then we have $(h,1,\dots,1) \in S$, since $N_1 \times N_2 \times \dots \times N_n \subseteq S$. Thus $h \in N_1$, completing the proof of (3).

(4) Suppose $S$ is meet irreducible in the lattice of subgroups of $G^n$. Since $S$ contains $N = N_1 \times N_2 \times \dots \times N_n$, and is contained in $\prod S_i = S_1 \times S_2 \times \dots \times S_n$, $S$ is also meet irreducible in the interval $I[N, \prod S_i]$ of the lattice of subgroups of $G^n$. This interval is isomorphic to the lattice of subgroups of $\prod H_i = \prod (S_i/N_i) = \big(\prod S_i\big)/N$, therefore $H$ is meet irreducible in the lattice of subgroups of $\prod H_i$. □

Now we will look at reduced subgroups of direct products $\prod H_i$ where each $H_i$ can be thought of as a section of $G$, though in most lemmas below we will not need that assumption. The case when there are only two factors is easy:

**Lemma 2.4.** *For any groups $H_1, H_2$, every subdirect subgroup $H$ of $H_1 \times H_2$ that satisfies condition (2) from Definition 2.2 is (the graph of) an isomorphism $H_1 \to H_2$. In particular, every reduced subgroup of $H_1 \times H_2$ is (the graph of) an isomorphism $H_1 \to H_2$.*

*Proof.* Let $H$ be a subdirect subgroup of $H_1 \times H_2$ that satisfies condition (2) from Definition 2.2. Since the coordinate kernels of $H$ are trivial and $\mathrm{pr}_i(H) = H_i$, Lemma 2.3 (2)–(3) shows that the projection homomorphisms $\mathrm{pr}_i \colon H \to H_i$, $(h_1, h_2) \mapsto h_i$ are isomorphisms ($i = 1, 2$). Thus $H$ is the graph of the composition of the isomorphisms $(\mathrm{pr}_1)^{-1} \colon H_1 \to H$ and $\mathrm{pr}_2 \colon H \to H_2$. □

Next we consider reduced subgroups of direct products with more that two factors.

**Lemma 2.5.** *Let $H_1, \ldots, H_n$ be nontrivial finite groups where $n \geq 3$. If $H$ is a reduced subgroup of $\prod H_i = H_1 \times \cdots \times H_n$, then*

1. *$H_1, \ldots, H_n$ are subdirectly irreducible groups with isomorphic abelian minimal normal subgroups $M_1, \ldots, M_n$, and*
2. *the unique upper cover of $H$ is $K = H \prod M_i$.*

*Furthermore, for the centralizers $C_i = C_{H_i}(M_i)$ $(i = 1, 2, \ldots, n)$ of the minimal normal subgroups $M_i$ we have the following:*

3. *$H_1/C_1 \cong H_2/C_2 \cong \cdots \cong H_n/C_n$, and*
4. *there exist isomorphisms $\iota_i \colon H_1/C_1 \to H_i/C_i$ $(i = 2, \ldots, n)$ such that*

$$(h_1, h_2, \ldots, h_n) \in H \quad \Rightarrow \quad h_i C_i = \iota_i(h_1 C_1) \quad \textit{for all } i = 2, \ldots, n.$$

*Proof.* Let $K$ denote the unique upper cover of $H$ in the lattice of subgroups of $\prod H_i$. Clearly, $K$ is also a subdirect subgroup of $\prod H_i$; that is, $\mathrm{pr}_i(K) = H_i$ for all $i$. Let $M_1, \ldots, M_n$ denote the coordinate kernels of $K$; that is,

$$M_i = \{g \in H_i : (1, \ldots, 1, \overset{i}{\breve{g}}, 1, \ldots, 1) \in K\}.$$

**Claim 2.6.** $\mathrm{pr}_I(K) = \mathrm{pr}_I(H)$ *for all $(n-1)$-element subsets $I$ of $\{1, ..., n\}$, and each coordinate kernel $M_i$ of $K$ is a nontrivial normal subgroup of $H_i$. Hence $K = H \prod M_i$.*

Our assumptions on $H$ are invariant under permuting the coordinates of $H$. Therefore it suffices to prove the equality $\mathrm{pr}_I(K) = \mathrm{pr}_I(H)$ for the set $I = \{1, \ldots, n-1\}$. Let $g \neq 1$ be any element of $H_n$. Since $H$ has trivial coordinate kernels, we have $(1, \ldots, 1, g) \notin H$. Therefore the subgroup $S$ of $H_1 \times \cdots \times H_n$ generated by $H$ and the element $(1, \ldots, 1, g)$ satisfies $H \subset S$ and $\mathrm{pr}_I(S) = \mathrm{pr}_I(H)$. Since $K$ is the unique upper cover of $H$, we get that $H \subset K \subseteq S$. Hence $\mathrm{pr}_I(H) \subseteq \mathrm{pr}_I(K) \subseteq \mathrm{pr}_I(S) = \mathrm{pr}_I(H)$, forcing $\mathrm{pr}_I(K) = \mathrm{pr}_I(H)$,

$K$ properly contains $H$, but their projections onto any $n-1$ coordinates are the same. Therefore the projection homomorphisms $\mathrm{pr}_I \colon K \to \mathrm{pr}_I(K) = \mathrm{pr}_I(H)$ are not bijective for any $(n-1)$-element subset $I$ of $\{1, \ldots, n\}$. Thus the coordinate kernels $M_i$ $(1 \leq i \leq n)$ of $K$ are nontrivial. By Lemma 2.3, each $M_i$ is a normal subgroup of $H_i$ and $\prod M_i \subseteq K$. Since $\prod M_i \not\subseteq H$ (as $H$ has trivial coordinate kernels) and $K$ covers $H$, it follows that $K = H \prod M_i$.

**Claim 2.7.** *For each $i$, $M_i$ is the unique minimal normal subgroup of $H_i$.*

Since our assumptions on $H$ are invariant under permuting the coordinates of $H$, it suffices to consider the case $i = 1$. Let $N$ be any nontrivial normal subgroup of $H_1$. Clearly, both $\widehat{N} = N \times \{1\}^{n-1}$ and $\widehat{M_1} = M_1 \times \{1\}^{n-1}$ are normal subgroups of $\prod H_i$. Since $H$ has trivial coordinate kernels, $\widehat{N}$, $\widehat{M_1}$ as well as their product intersect trivially with $H$. It follows, in particular, that $H \subset H\widehat{N}$. Hence $K \subseteq H\widehat{N}$, as $K$ is the unique cover of $H$. But $\prod M_i \subseteq K$, therefore $\widehat{M_1} \subseteq H\widehat{N}$. Thus $H\widehat{N} = H(\widehat{N}\widehat{M_1})$. Since $H \cap \widehat{N} = H \cap (\widehat{N}\widehat{M_1}) = \{1\}$ and all groups appearing here are finite, we conclude that $|\widehat{N}| = |\widehat{N}\widehat{M_1}|$. Therefore $\widehat{M_1} \subseteq \widehat{N}$, and it follows that $M_1 \subseteq N$. This proves that $M_1$ is contained in each nontrivial normal subgroup of $H_1$, and hence completes the proof of Claim 2.7.

**Claim 2.8.** $M_1 \cong \cdots \cong M_n$.

It suffices to prove that $M_1 \cong M_2$. Let $\widehat{M_1} = M_1 \times \{1\}^{n-1}$ and $\widehat{M_2} = \{1\} \times M_2 \times \{1\}^{n-2}$. For $i = 1, 2$, $\widehat{M_i}$ intersects trivially with $H$ since $H$ has trivial coordinate kernels, and $K = H\widehat{M_i}$ since $\widehat{M_i} \subseteq \prod M_j \subseteq K$ and $K$ is the unique upper cover of $H$. Thus $|M_i| = |\widehat{M_i}| = [K : H]$ $(i = 1, 2)$.

Now let us consider the subgroup

$$U = \{(m, h) \in M_1 \times H_2 : (m, h, 1, \ldots, 1) \in H\}$$

of $H$. Since $\mathrm{pr}_{\{1,3,\ldots n\}}(H) = \mathrm{pr}_{\{1,3,\ldots n\}}(K)$ and $\widehat{M_1} \subseteq K$, therefore to every element $m \in M_1$ there exists $h \in H_2$ such that $(m, h) \in U$. The element $h$ is uniquely determined by $m$, because $H$ has trivial coordinate kernels, implying that the projection homomorphism $H \to \mathrm{pr}_{\{1,3,\ldots n\}}(H)$ is bijective. Thus $\mathrm{pr}_1(U) = M_1$, $\mathrm{pr}_2(U)$ is a subgroup $N_2$ of $H_2$, and $U$ is (the graph of) an isomorphism $M_1 \to N_2$. Clearly, $|N_2| = |M_1|$. Since every element of $H_2$ occurs as a second coordinate of an element of $H$ and conjugation by such an element maps $U$ into itself, it follows that $N_2$ is a normal subgroup of $H_2$. So by Claim 2.7 we have $M_2 \subseteq N_2$. We proved earlier that $|M_2| = |M_1|$ and $|M_1| = |N_2|$. Thus $N_2 = M_2$, proving that $M_1 \cong M_2$.

**Claim 2.9.** *The normal subgroup $M = H \cap \prod M_i$ of $H$ is a subdirect subgroup of $\prod M_i$ with trivial coordinate kernels. Furthermore,* $\mathrm{pr}_I(M) = \prod_{i \in I} M_i$ *for all* $(n-1)$*-element subsets $I$ of* $\{1, \ldots, n\}$.

$M$ has trivial coordinate kernels, because $M \subseteq H$ and $H$ has trivial coordinate kernels. The second part of the claim implies that $M$ is a subdirect subgroup of $\prod M_i$. Therefore it suffices to prove the second part of the claim.

The arguments in the proof of the preceding claim show that $U$ is the graph of an isomorphism $M_1 \to M_2$ and $U \times \{1\}^{n-2} \subseteq M$. Hence, in particular, $M_2 \times \{1\}^{n-2} \subseteq \mathrm{pr}_I(M)$ for $I = \{2, \ldots, n\}$. By interchanging the roles of the second and $i$-th coordinates in $H$ for any $2 < i \leq n$ we get that $\{1\}^{i-2} \times M_i \times \{1\}^{n-i} \subseteq \mathrm{pr}_I(M)$. Multiplying these subgroups yields that $\prod_{i\in I} M_i \subseteq \mathrm{pr}_I(M)$ for $I = \{2,\dots,n\}$. The reverse inclusion is obvious, which establishes the required equality $\prod_{i\in I} M_i = \mathrm{pr}_I(M)$ for $I = \{2,\dots,n\}$. Since our assumptions on $H$ are invariant under permuting the coordinates of $H$, it follows that a similar equality holds for every $(n-1)$-element subset $I$ of $\{1,\dots,n\}$.

**Claim 2.10.** *$M_1,\dots,M_n$ are abelian.*

By Claim 2.8, it suffices to show that $M_1$ is abelian. For any $\ell, m \in M_1$ the elements $\alpha = (\ell,1,1,\dots,1)$ and $\beta = (m,1,1,\dots,1)$ belong to $\prod M_i \subseteq K$. Since $\mathrm{pr}_I(K) = \mathrm{pr}_I(H)$ for all $(n-1)$-element subsets $I$, there exist elements in $H$ that agree with $\alpha$ and $\beta$ in all but any one given coordinate. Since $n \geq 3$, there exist $g \in H_2$ and $h \in H_3$ such that $(\ell,g,1,\dots,1),(m,1,h,\dots,1) \in H$. The commutator of these elements is $(\ell^{-1}m^{-1}\ell m,1,1,\dots,1) \in H$. Since $H$ has trivial coordinate kernels, $\ell^{-1}m^{-1}\ell m = 1$, for any two elements $\ell, m \in M_1$. This proves that $M_1$ is abelian.

We have now established parts (1) and (2) of Lemma 2.5.

The quotient groups in part (3) make sense, because the centralizer of a normal subgroup is normal, and hence $C_i \lhd H_i$ for all $i$. Since the normal subgroups $M_i$ are abelian, we have $M_i \subseteq C_i$ for all $i$.

Project $H$ onto the first two coordinates to get a subgroup $H_{12} = \mathrm{pr}_{\{1,2\}}(H)$ of $H_1 \times H_2$. Since $C_1 \times C_2 \lhd H_1 \times H_2$, the least subgroup of $H_1 \times H_2$ that contains $H_{12}$ and $C_1 \times C_2$ is $H_{12}(C_1 \times C_2)$, and the quotient group $V = H_{12}(C_1\times C_2)/(C_1 \times C_2)$ can naturally be considerered as a subgroup of $(H_1/C_1) \times (H_2/C_2)$, namely

$$V = \{(h_1C_1, h_2C_2) : (h_1,h_2,h_3,\dots,h_n) \in H \quad \text{for some } h_3 \in H_3,\dots,h_n \in H_n\}. \tag{2.1}$$

**Claim 2.11.** *$V$ is the graph of an isomorphism $H_1/C_1 \to H_2/C_2$.*

Let $U$ be the subgroup of $M_1 \times H_2$ defined in the proof of Claim 2.8. It was proved there that $U$ is in fact a subgroup of $M_1 \times M_2$, that is,

$$U = \{(m_1,m_2) \in M_1 \times M_2 : (m_1,m_2,1,\dots,1) \in H\},$$

and $U$ is the graph of an isomorphism $M_1 \to M_2$. Let $h = (h_1,h_2,h_3,\dots,h_n)$ and $k = (k_1,k_2,k_3,\dots,k_n)$ be arbitrary $n$-tuples from $H$. For any pair $(m_1,m_2) \in U$, conjugating the $n$-tuple $(m_1,m_2,1,\dots,1) \in H$ with $h$ and $k$ yields that the pairs $(h_1m_1h_1^{-1}, h_2m_2h_2^{-1})$ and $(k_1m_1k_1^{-1}, k_2m_2k_2^{-1})$ also belong to $U$. Now, if $h_1C_1 = k_1C_1$, then $h_1m_1h_1^{-1} = k_1m_1k_1^{-1}$ for all $m_1 \in M_1$. Since $U$ is the graph of an isomorphism $M_1 \to M_2$, it follows that $h_2m_2h_2^{-1} = k_2m_2k_2^{-1}$ for all $m_2 \in M_2$. Hence $h_2C_2 = k_2C_2$. Similarly, if $h_2C_2 = k_2C_2$ then $h_1C_1 = k_1C_1$. Thus $V$ is the graph of a bijection between (some) elements of $H_1/C_1$ and $H_2/C_2$. However, since $H$ is a subdirect subgroup of $\prod H_i$, it is clear from the description of $V$ in (2.1) that every element of $H_i/C_i$ $(i = 1,2)$ occurs as the $i$-th coordinate of some pair in $V$. Thus $V$ is in fact the graph of a bijection $H_1/C_1 \to H_2/C_2$. Since $V$ is a group, this bijection is an isomorphism, completing the proof of Claim 2.11.

Claim 2.11 shows that $H_1/C_1 \cong H_2/C_2$, and that the displayed implication in (4) holds for $i = 2$ if we choose $\iota_2$ to be the isomorphism $H_1/C_1 \to H_2/C_2$ defined by $V$. Since our assumptions on $H$ are invariant under permuting the coordinates of $H$, in the arguments above the second coordinate can be replaced by the $i$-th coordinate for any $i = 3, \dots, n$. This completes the proof of Lemma 2.5. $\square$

**Lemma 2.12.** *Let $H_1, \dots, H_n$ ($n \geq 3$) be nontrivial finite groups whose Sylow subgroups are abelian, and let $H$ be a reduced subgroup of $\prod H_i$ such that $|H_1| \leq \cdots \leq |H_n|$.*

(1) *$H_1, \dots, H_n$ are subdirectly irreducible groups such that their minimal normal subgroups $M_1, \dots, M_n$ are isomorphic elementary abelian $p$-groups for some prime $p$, and their Sylow $p$-subgroups $P_1, \dots, P_n$ are normal; in fact,*

$$P_i = C_{H_i}(M_i) \quad \textit{for all } i = 1, \dots, n.$$

(2) *There exist embeddings $\varphi_i \colon H_i \to H_n$ ($i = 1, \dots, n-1$) such that the subgroup*

$$H^* = \bigl\{ \bigl(\varphi_1(h_1), \dots, \varphi_{n-1}(h_{n-1}), h_n\bigr) : (h_1, \dots, h_n) \in H \bigr\} \tag{2.2}$$

*of $(H_n)^n$ has the following structure:*

$$\begin{aligned} H^* = \bigl\{ \bigl(x_1 c, \dots, x_{n-1} c, \psi_1(x_1) \cdots \psi_{n-1}(x_{n-1}) c\bigr) : \\ c \in Q_n \textit{ and } x_1 \in P_1^*, \dots, x_{n-1} \in P_{n-1}^* \bigr\} \end{aligned} \tag{2.3}$$

*for a complement $Q_n$ of $P_n$ in $H_n$, for some normal subgroups $P_1^*, \dots, P_{n-1}^*$ of $H_n$ in $P_n$ and some automorphisms $\psi_i$ of $P_i^*$ ($i = 1, \dots, n-1$) such that $\psi_i$ is the restriction to $P_i^*$ of an automorphism $\chi_i$ of $H_i^* = P_i^* Q_n$ which acts on $Q_n$ as the identity.*

*Proof.* We will need the following fact about finite groups with abelian Sylow subgroups.

**Claim 2.13.** *Let $G$ be a finite group whose Sylow subgroups are abelian. If $G$ is subdirectly irreducible with abelian minimal normal subgroup $N$, then $C_G(N)$ is a Sylow subgroup of $G$.*

It is proved in [1] that a finite group $G$ has abelian Sylow subgroups if and only if it satisfies the commutator law

$$[M, M \cap N] = [M, M] \cap N$$

for all $M, N \lhd H$ where $H$ is a subgroup of $G$. In particular, if $G$ is subdirectly irreducible with abelian minimal normal subgroup $N$ and $M = C_G(N)$, then

$$\{1\} = [C_G(N), N] = [C_G(N), C_G(N) \cap N] = [C_G(N), C_G(N)] \cap N.$$

Hence $C_G(N)$ is abelian. $N$ is an abelian $p$-group for some prime $p$, so — since Sylow subgroups are abelian — $N \subseteq P \subseteq C_G(N)$ for some Sylow $p$-subgroup $P$. Let $T$ be a complement of $P$ in the abelian group $C_G(N)$. Then $T$ is a characteristic subgroup of $C_G(N)$. Since $C_G(N)$ is normal in $G$, it follows that $T$ is a normal subgroup of $G$. But $N$ is the unique minimal normal subgroup of $G$ and $T$ intersects $N$ trivially. Therefore $T$ is trivial, which implies that $C_G(N) = P$.

We know from part (1) of Lemma 2.5 that the groups $H_1, \ldots, H_n$ are subdirectly irreducible, and their minimal normal subgroups $M_1, \ldots, M_n$ are abelian and isomorphic to each other. It follows in particular, that all $M_i$ are elementary abelian $p$-groups for the same prime $p$. Thus Claim 2.13 implies that $C_{H_i}(M_i) = P_i \triangleleft H_i$ for all $i$ $(i = 1, \ldots, n)$. This establishes the claims in part (1) of Lemma 2.12.

Since each $P_i$ is a normal subgroup of $H_i$, the group $P^\dagger = \prod P_i$ is a normal subgroup of $\prod H_i$. Therefore the Sylow $p$-subgroup of $H$ is $P = H \cap P^\dagger$, which is normal in $H$. This implies that $P$ has a complement in $H$. We will select a complement $Q$, and keep it fixed for the rest of the proof of Lemma 2.12. For $1 \leq i \leq n$ we let $Q_i$ denote the image of $Q$ under the projection homomorphism $\mathrm{pr}_i$ onto the $i$-th coordinate. Thus $Q_i$ is a subgroup of $H_i$.

**Claim 2.14.** *For all $i$, $Q_i$ is a complement of $P_i$ in $H_i$, and there exist isomorphisms $\kappa_i\colon Q_i \to Q_n$ $(i = 1, \ldots, n-1)$ such that*

$$Q = \big\{ \big(\kappa_1^{-1}(c), \ldots, \kappa_{n-1}^{-1}(c), c\big) : c \in Q_n \big\}.$$

If we project $H = QP$ onto the $i$-th coordinate we see that $H_i = Q_i P_i$. Since the order of $Q$ is relatively prime to $p$, its homomorphic image $Q_i$ has the same property. This implies that $Q_i$ is a complement of $P_i$ in $H_i$. Hence $Q_i \cong H_i/P_i$. With the notation of Lemma 2.5 we have $C_i = P_i$ for all $i$, so by part (4) of that lemma there exist isomorphisms $\iota_i\colon H_1/P_1 \to H_i/P_i$ $(i = 2, \ldots, n)$ such that

$$(h_1, h_2, \ldots, h_n) \in H \quad \Rightarrow \quad h_i P_i = \iota_i(h_1 P_1) \quad \text{for all } i = 2, \ldots, n. \tag{2.4}$$

Putting $\iota_1 = \mathrm{id}$ we now define the isomorphisms $\kappa_j\colon Q_j \to Q_n$ $(j = 1, \ldots, n-1)$ by the following compositions:

$$\kappa_j\colon Q_j \to H_j/P_j \xrightarrow{\iota_j^{-1}} H_1/P_1 \xrightarrow{\iota_n} H_n/P_n \to Q_n.$$

It is clear now from (2.4) that if $(q_1, q_2, \ldots, q_n) \in Q$, then $\kappa_j(q_j) = q_n$ for all $j = 1, \ldots, n-1$. Thus, for every $c \in Q_n$ the only $n$-tuple in $Q$ with last coordinate $c$ is $\big(\kappa_1^{-1}(c), \ldots, \kappa_{n-1}^{-1}(c), c\big)$. Since every $c \in Q_n$ occurs as the last coordinate of an $n$-tuple from $Q$, the displayed equality in Claim 2.14 follows.

Now we will look at some subgroups of $\prod H_i$ that contain $H = QP$. Since $Q$ is a complement of the Sylow $p$-subgroup $P$ in $H$, its order is relatively prime to $p$. Thus $Q$ intersects trivially with $P^\dagger$ as well. Let $H^\dagger = QP^\dagger$. Clearly, $P^\dagger$ is a normal subgroup of $H^\dagger$. Therefore $Q$ acts on $P^\dagger$ by conjugation. There is a natural way to consider $P^\dagger$ as a $Q$-module (or equivalently, a module over the group ring $\mathbf{Z}_{p^f}[Q]$ for any power $p^f$ of $p$ exceeding the exponent of $P^\dagger$) as follows: module addition is the abelian group operation of $P^\dagger$, and for any $u \in Q$, module multiplication by $u$ is conjugation by $u$.

**Claim 2.15.** *Every group $H^\circ$ with $Q \subseteq H^\circ \subseteq H^\dagger$ decomposes as $H^\circ = QP^\circ$ where $P^\circ = H^\circ \cap P^\dagger$ is a normal Sylow $p$-subgroup in $H^\circ$, and hence $P^\circ$ is a $Q$-submodule of $P^\dagger$. Moreover, the mapping $H^\circ \to P^\circ$ is a lattice isomorphism between the interval $I[Q, H^\dagger]$ in the subgroup lattice of $\prod H_i$ and the lattice of $Q$-submodules of $P^\dagger$.*

To prove the first part of the claim, let $H^\circ$ be a subgroup of $H^\dagger$ such that $Q \subseteq H^\circ$. Since $P^\dagger$ is a normal Sylow $p$-subgroup of $H^\dagger$, it follows that $P^\circ = H^\circ \cap P^\dagger$ is a normal Sylow $p$-subgroup of $H^\circ$. Thus $P^\circ$ is closed under conjugation by elements of $Q$, implying that it is a $Q$-submodule of $P^\dagger$. Now we show that $H^\circ = QP^\circ$. Since $QP^\circ \subseteq H^\circ$ and

$$Q \cong H^\dagger/P^\dagger = H^\circ P^\dagger/P^\dagger \cong H^\circ/(H^\circ \cap P^\dagger) = H^\circ/P^\circ \supseteq QP^\circ/P^\circ \cong Q,$$

the inclusion $\supseteq$ in the displayed formula cannot be proper. This completes the proof of the equality $H^\circ = QP^\circ$ and the first statement of the claim.

The facts established in the preceding paragraph show that $H^\circ \to P^\circ$ is an injective and monotone mapping of the interval $I[Q, H^\dagger]$ of the subgroup lattice of $\prod H_i$ into the lattice of $Q$-submodules of $P^\dagger$. It remains to show that this mapping is surjective. Let $R$ be a $Q$-submodule of $P^\dagger$. Then $R$ is a subgroup of $P^\dagger$ that is closed under conjugation by elements of $Q$. Since $H^\dagger = QP^\dagger$ and $P^\dagger$ is abelian, it follows that $R$ is closed under conjugation by all elements of $H^\dagger$. Thus $R$ is a normal $p$-subgroup of $H^\dagger$. Hence the group $QR$ belongs to the interval $I[Q, H^\dagger]$, and has normal Sylow $p$-subgroup $R$. The proof of Claim 2.15 is complete.

The interval $I[Q, H^\dagger]$ contains $H = QP$ as well as its unique upper cover $K = H \prod M_i = Q(P \prod M_i)$. The isomorphism described in Claim 2.15 ensures that the image $P$ of $H$ has a unique upper cover in the lattice of $Q$-submodules of $P^\dagger$. Therefore $P^\dagger/P$ is a subdirectly irreducible $Q$-module of $p$-power exponent.

The next claim describes the submodules of such modules.

**Claim 2.16.** *Let $G$ be a finite group whose order is not divisible by the prime $p$, and let $W$ be a finite subdirectly irreducible $G$-module whose additive exponent is $p^e$. Then every submodule of $W$ has the form $p^j W$ for some $0 \le j \le e$. Hence the submodule lattice of $W$ is a chain of length $e$.*

Let $S$ be the unique minimal submodule of $W$, and let $A$ denote the submodule of $W$ that consist of all elements $w \in W$ such that $pw = 0$. Both $A$ and $p^{e-1}W$ are nontrivial submodules of $W$ because the exponent of $W$ is $p^e$. Thus we have $S \subseteq p^{e-1}W \subseteq A$. It follows that $A$ is a subdirectly irreducible $G$-module. The exponent of $A$ is $p$, therefore $A$ is a module over the group ring $\mathbf{Z}_p[G]$. By Maschke's Theorem $\mathbf{Z}_p[G]$ is semisimple, and hence every subdirectly irreducible $\mathbf{Z}_p[G]$-module is simple. Thus $A$ is simple, which implies that $S = p^{e-1}W = A$.

Next we show that the submodules of $W$ form a chain. Suppose not, and consider a counterexample $W$ of smallest size. Then the unique minimal submodule $A$ of $W$ has more than one upper cover, since otherwise $W/A$ would be a smaller subdirectly irreducible $G$-module whose submodule lattice is not a chain. Let $V, V'$ be two distinct upper covers of $A$. Then $V, V' \not\subseteq A$ implies that the submodules $pV, pV'$ of $W$ are nontrivial. We have $pV \subseteq V$ and $pV \neq V$, because $pV = V$ would imply $p^eV = V$, which is impossible, because $p^eV$ is trivial. Thus $pV = A$, and similarly $pV' = A$. Let $v \in V \setminus A$ be arbitrary. Then $pv \in A$ but $pv \neq 0$. Since $pV' = A$, there exists $v' \in V'$ such that $pv' = pv$. Thus $p(v - v') = 0$, implying that $v - v' \in A$. Hence $v = v' + (v - v') \in V \cap V' = A$, which contradicts the choice of $v$. This proves that the submodules of $W$ form a chain.

The submodules $W_j = p^jW$ $(j = 0, \dots, e)$ of $W$ form a chain $W_0 \supset W_1 \supset \cdots \supset W_{e-1} \supset W_e$ where $W_0 = W$, $W_e$ is the trivial submodule of $W$, and the inclusions are proper, because the exponent of $W$ is $p^e$. To complete the proof it suffices to show that the quotient module $W_{j-1}/W_j$ is simple for all $j = 1, \dots, n$. We know that the submodule lattice of $W_{j-1}/W_j$ is a chain, because it is isomorphic to the interval $I[W_j, W_{j-1}]$ in the submodule lattice of $W$. Therefore $W_{j-1}/W_j$ is subdirectly irreducible. In addition, the exponent of $W_{j-1}/W_j$ is $p$. Therefore the same argument as we used for $A$ implies that $W_{j-1}/W_j$ is simple. This completes the proof of Claim 2.16

**Claim 2.17.** *Each $P_i$, considered as a $Q$-module where module multiplication by $q = (q_1, \dots, q_n)$ is conjugation by $q_i$, has a $Q$-module embedding in $P^\dagger/P$. In particular, $P_n$ is isomorphic as a $Q$-module to $P^\dagger/P$.*

Let $\widehat{P}_i$ denote the subgroup $\{1\}^{i-1} \times P_i \times \{1\}^{n-i}$ of $P^\dagger$. Then $\widehat{P}_i$ is a normal subgroup of $H^\dagger$, so it is a $Q$-submodule. The $Q$-module structure of $P_i$ was defined so that the natural mapping $P_i \to \widehat{P}_i$ is a $Q$-module isomorphism. For each $i$ the $Q$-submodule $\widehat{P}_i$ of $P^\dagger$ intersects trivially with $P$, because the coordinate kernels of $P$ are trivial. Therefore the natural isomorphism $P_i \to \widehat{P}_i$ followed by the isomorphism $\widehat{P}_i \to \widehat{P}_iP/P$ and the identical embedding $\widehat{P}_iP/P \to P^\dagger/P$ is a $Q$-module embedding of $P_i$ in $P^\dagger/P$.

Now we will use our assumption $|H_1| \leq \cdots \leq |H_n|$. By Claim 2.14 the complements $Q_i$ of the Sylow $p$-subgroups $P_i$ in $H_i$ are isomorphic to each other, therefore $|Q_1| = \cdots = |Q_n|$. Hence $|P_1| \leq \cdots \leq |P_n|$. Let $p^{e_i}$ denote the exponent of $P_i$, and let $e = \max e_i$. Then $p^e$ is the exponent of $P$ as well as of $P^\dagger$. Hence the exponent of $P^\dagger/P$ is at most $p^e$. But since all $P_i$ are embeddable in $P^\dagger/P$, the exponent of $P^\dagger/P$ is equal to $p^e$.

By our discussion preceding Claim 2.16, $P^\dagger/P$ is a subdirectly irreducible $Q$-module. Hence by Claim 2.16 it has a unique submodule of exponent $p^{e_i}$ for each $i$, namely $p^{e-e_i}(P^\dagger/P)$. Moreover, $e_i \le e_j$ if and only if $p^{e-e_i}(P^\dagger/P) \subseteq p^{e-e_j}(P^\dagger/P)$. Therefore the $Q$-module embeddings $P_i \to P^\dagger/P$ found earlier yield that for each $i$, $P_i$ is isomorphic, as a $Q$-module, to the submodule $p^{e-e_i}(P^\dagger/P)$ of $P^\dagger/P$. Hence the inequalities $|P_1| \le \cdots \le |P_n|$ imply that $e_1 \le \cdots \le e_n$. Thus $e = e_n$ and $P_n$ is isomorphic, as a $Q$-module, to $p^{e-e_n}(P^\dagger/P) = P^\dagger/P$.

**Claim 2.18.** *For $I = \{1, \dots, n-1\}$ we have $\mathrm{pr}_I(P) = \prod_{i\in I} P_i$.*

By the preceding claim $P^\dagger/P$ is isomorphic to $P_n$. Thus $|P| = |P^\dagger|/|P_n| = \prod_{i\in I}|P_i|$. However, the projection homomorphism $\mathrm{pr}_I\colon P \to \prod_{i\in I} P_i$ is injective, because $P$ has trivial coordinate kernels. Therefore it is onto, that is, $\mathrm{pr}_I(P) = \prod_{i\in I} P_i$.

**Claim 2.19.** *For each $i$ ($i = 1, \dots, n-1$) there exists an embedding $\varphi_i\colon H_i \to H_n$ such that $\varphi_i$ restricts to $Q_i$ as the isomorphism $\kappa_i\colon Q_i \to Q_n$ from Claim 2.14.*

Let $i$ be a fixed index ($1 \le i \le n-1$). By Claim 2.17 there exists a $Q$-module embedding $\lambda_i\colon P_i \to P_n$. This means that $\lambda_i$ is a group embedding $P_i \to P_n$ which commutes with the module multiplication by every element $q = (q_1, \dots, q_n)$ of $Q$. The definition of the $Q$-module structure of $P_i$ in Claim 2.17 implies that for $\lambda_i$ the property of commuting with multiplication by $q = (q_1, \dots, q_n)$ is equivalent to the following condition:

$$\lambda_i(q_i x q_i^{-1}) = q_n\big(\lambda_i(x)\big)q_n^{-1} \qquad \text{for all} \quad x \in P_i.$$

The description of the elements of $Q$ in Claim 2.14 shows that $q_i$, $q_n$ appear as $i$-th and $n$-th coordinates of an element of $Q$ exactly when $q_n = \kappa_i(q_i)$. Thus $\lambda_i$ is a group embedding $P_i \to P_n$ such that

$$\lambda_i(uxu^{-1}) = \big(\kappa_i(u)\big)\big(\lambda_i(x)\big)\big(\kappa_i(u)\big)^{-1} \qquad \text{for all} \quad x \in P_i,\ u \in Q_i.$$

This allows us to extend $\lambda_i$ to a group embedding $\varphi_i$ of $H_i = Q_iP_i = P_iQ_i$ into $H_n = Q_nP_n = P_nQ_n$ as follows: for any $x \in P_i$ and $u \in Q_i$ let

$$\varphi_i(xu) = \big(\lambda_i(x)\big)\big(\kappa_i(u)\big).$$

To check that $\varphi_i$ is indeed a group embedding, observe first that $\varphi_i$ is well-defined and one-to-one, since $Q_i$ intersects trivially with $P_i$, $Q_n$ intersects trivially with $P_n$, and $\lambda_i, \kappa_i$ are one-to-one. Now let $xu, yv$ ($x, y \in P_i$, $u, v \in Q_i$) be arbitrary elements of $H_i$. Then

$$\begin{aligned}\big(\varphi_i(xu)\big)\big(\varphi_i(yv)\big) &= \big(\lambda_i(x)\big)\big(\kappa_i(u)\big)\big(\lambda_i(y)\big)\big(\kappa_i(v)\big)\\ &= \big(\lambda_i(x)\big)\big((\kappa_i(u))(\lambda_i(y))(\kappa_i(u))^{-1}\big)\big(\kappa_i(u)\big)\big(\kappa_i(v)\big)\\ &= \big(\lambda_i(x)\big)\big(\lambda_i(uyu^{-1})\big)\big(\kappa_i(u)\big)\big(\kappa_i(v)\big)\\ &= \big(\lambda_i(x(uyu^{-1}))\big)\big(\kappa_i(uv)\big)\\ &= \varphi_i\big(x(uyu^{-1})uv\big)\\ &= \varphi_i\big((xu)(yv)\big).\end{aligned}$$

Thus $\varphi_i$ is a group embedding. The definition of $\varphi_i$ shows that $\varphi_i$ restricts to $Q_i$ as $\kappa_i$ and to $P_i$ as $\lambda_i$. This concludes the proof of Claim 2.19.

Now we complete the proof of part (2) of Lemma 2.12. To construct the subgroup $H^*$ of $H_n^n$ as described in the lemma, we use the embeddings $\varphi_1, \dots, \varphi_{n-1}$ from Claim 2.19. Namely, we let $H^*$ be the image of $H$ under the embedding

$$\varphi = \varphi_1 \times \cdots \times \varphi_{n-1} \times \mathrm{id}\colon H_1 \times \cdots \times H_{n-1} \times H_n \to H_n^n.$$

Since $\varphi_i$ restricts to $Q_i$ as $\kappa_i$, the description of $Q$ in Claim 2.14 shows that the image of the subgroup $Q$ of $H$ under $\varphi$ will be the diagonal subgroup

$$Q^* = \{(c, \dots, c, c) : c \in Q_n\} \tag{2.5}$$

of $H^*$.

Let $P^*$ denote the image of $P$ under $\varphi$, and for each $i$ ($i = 1, \dots, n-1$) let $P_i^*$ denote the image of $P_i$ under $\varphi_i$. As $\varphi_i$ agrees with $\lambda_i$ on $P_i$ and $\lambda_i$ is a $Q$-module embedding, it follows that $P_i^*$ is a subgroup of $P_n$ that is closed under conjugation by elements of $Q_n$. $P_i^*$ is also closed under conjugation by elements of $P_n$, because $P_n$ is abelian. Thus $P_i^*$ is a normal subgroup of $H_n = Q_nP_n$. Since $P$ is a normal Sylow $p$-subgroup of $H$ with complement $Q$, therefore $P^*$ is a normal Sylow $p$-subgroup of $H^*$ with complement $Q^*$. Since $P$ is a subdirect subgroup of $\prod P_i$ with trivial coordinate kernels and $\varphi$ acts coordinatewise, the image $P^*$ is a subdirect subgroup of $\prod P_i^*$ ($\subseteq P_n^n$) with trivial coordinate kernels. Moreover, the property of $P$ established in Claim 2.18 will also carry over to $P^*$, that is, we have

$$\mathrm{pr}_I(P^*) = \prod_{i\in I} P_i^* \qquad \text{for} \quad I = \{1, \dots, n-1\}. \tag{2.6}$$

For each $i$ ($i = 1, \dots, n-1$) let $\widehat{T_i}$ consist of all elements of $P^*$ of the form $(1, \dots, 1, x_i, 1, \dots, 1, x_n)$ where $x_i$ is in the $i$-th position. Since $P^*$ is a normal subgroup of $H^*$, so is $\widehat{T_i}$. To focus on the nontrivial coordinates only, let

$$T_i = \{(x_i, x_n) \in P_i^* \times P_n : (1, \dots, 1, x_i, 1, \dots, 1, x_n) \in \widehat{T_i}\}.$$

Clearly, $T_i$ is a subgroup of $P_i^* \times P_n$. The displayed equation (2.6) above implies that to every $x_i \in P_i^*$ there exists $x_n \in P_n$ such that $(x_i, x_n) \in T_i$. Since $P^*$ has trivial coordinate kernels, this $x_n$ is uniquely determined by $x_i$, and $x_i$ is also uniquely determined by its matching $x_n$. Thus $T_i$ is (the graph of) an injective group homomorphism $\psi_i \colon P_i^* \to P_n$, and

$$\widehat{T}_i = \{(1, \dots, 1, x_i, 1, \dots, 1, \psi_i(x_i)) : x_i \in P_i^*\}. \tag{2.7}$$

Now we make use of the fact that $\widehat{T}_i$ is closed under conjugation by elements of $Q^*$. If $(x_i, x_n) \in T_i$ and $c \in Q_n$, then conjugating the $n$-tuple $(1, \dots, 1, x_i, 1, \dots, 1, x_n) \in \widehat{T}_i$ by $(c, \dots, c) \in Q^*$ yields that $(cx_ic^{-1}, cx_nc^{-1}) \in T_i$. This means that $\psi_i$ satisfies the following condition:

$$\psi_i(cx_ic^{-1}) = c\psi_i(x_i)c^{-1} \qquad \text{for all} \quad c \in Q_n,\ x_i \in P_i^*. \tag{2.8}$$

Consequently, $\psi_i \colon P_i^* \to P_n$ is not only an injective group homomorphism, it is also an injective $Q$-module homomorphism. Since the $Q$-submodules of $P_n$ form a chain, no two distinct submodules of $P_n$ are of the same order. Therefore the image of $P_i^*$ under $\psi_i$ must be $P_i^*$, so $\psi_i$ is an automorphism of $P_i^*$.

To establish that $\psi_i$ is the restriction of an appropriate automorphism $\chi_i$ of $H_i^*$, as claimed in Lemma 2.12, observe first that $H_i^* = P_i^* Q_n$ is a subgroup of $H_n$, because $P_i^* \triangleleft H_n$. Since every element of $H_i^*$ can be written uniquely as a product $xc$ with $x \in P_i^*$ and $c \in Q_n$, we get a well-defined mapping $\chi_i \colon H_i^* \to H_i^*$ by setting $\chi_i(xc) = \psi_i(x)c$ for all $x \in P_i^*$ and $c \in Q_n$. It follows that $\chi_i$ is injective because $\psi_i$ is such. Clearly $\chi_i$ restricts to $P_i^*$ as $\psi_i$, and to $Q_n$ as the identity. It remains to check that $\chi_i$ is a homomorphism. For any $x, y \in P_i^*$ and $c, d \in Q_n$ we have $cyc^{-1} \in P_i^*$, as $P_i^* \triangleleft H_n$. Therefore, using the definition of $\chi_i$ and condition (2.8), we get that

$$\begin{aligned}
\chi_i(xc)\chi_i(yd) &= \psi_i(x)c\psi_i(y)d \\
&= \psi_i(x)\bigl(c\psi_i(y)c^{-1}\bigr)cd \\
&= \psi_i(x)\psi_i(cyc^{-1})cd \\
&= \psi_i\bigl(x(cyc^{-1})\bigr)cd \\
&= \chi_i\bigl(x(cyc^{-1})cd\bigr) \\
&= \chi_i(xcyd).
\end{aligned}$$

Next we prove that $P^*$ is the product of its subgroups $\widehat{T}_i$ $(i = 1, \dots, n-1)$. Since every element of $P_i^*$ occurs as the $i$-th coordinate of an $n$-tuple in $\widehat{T}_i$, it follows that $\mathrm{pr}_I(\widehat{T}_1 \cdots \widehat{T}_{n-1}) = \prod_{i \in I} P_i^*$ holds for $I = \{1, \dots, n-1\}$. Thus $|\widehat{T}_1 \cdots \widehat{T}_{n-1}| \geq \prod_{i \in I} |P_i^*|$. The analogous equation (2.6) for $P^*$ combined with the fact that $P^*$ has trivial coordinate kernels yields that $|P^*| = \prod_{i \in I} |P_i^*|$. Thus $P^* = \widehat{T}_1 \cdots \widehat{T}_{n-1}$, as claimed.

Finally, since $Q^*$ is a complement of $P^*$ in $H^*$, we get that $H^* = P^*Q^* = \widehat{T}_1 \cdots \widehat{T}_{n-1}Q^*$. Using the descriptions (2.5) and (2.7) for $Q^*$ and $T_i^*$, we get the equality (2.3) for $H^*$. This completes the proof of Lemma 2.12. $\square$

It is easy to see that if the Sylow subgroups of $G$ are abelian, then the Sylow subgroups of all sections of $G$ are also abelian. Thus Lemma 2.12 suggests that if the Sylow subgroups of $G$ are abelian, then a reduced subgroup $H$ of a direct product of sections $H_i$ of $G$ can be constructed from two kinds of 'building blocks': isomorphisms between sections of $G$ and some subgroups of cubes of sections $H_0$ of $G$ which have the following form:

$$\{(x_1c, x_2c, x_1x_2c) : x_1, x_2 \in P_0,\ c \in Q_0\} \tag{2.9}$$

where $P_0$ is a nontrivial normal Sylow subgroup of $H_0$ and $Q_0$ is a complement of $P_0$ in $H_0$. It is straightforward to check that since the Sylow subgroup $P_0$ of $H_0$ is abelian, (2.9) is indeed a subgroup of $H_0^3$.

For an isomorphism $\sigma\colon H_1 \to H_2$ where $H_i = S_i/N_i$ $(i = 1, 2)$ are sections of $G$ we will denote by $\Gamma[\sigma]$ the graph of $\sigma$ (as a subgroup of $H_1 \times H_2$), and by $\Gamma_{N_1,N_2}[\sigma]$ its inverse image under the natural homomorphism $S_1 \times S_2 \to (S_1/N_1) \times (S_2/N_2) = H_1 \times H_2$. Hence

$$\Gamma_{N_1,N_2}[\sigma] = \{(s_1, s_2) \in S_1 \times S_2 : N_2s_2 = \sigma(N_1s_1)\}.$$

**Lemma 2.20.** *Every subgroup of $G^2$ has the form $\Gamma_{N_1,N_2}[\sigma]$ for an isomorphism $\sigma\colon H_1 \to H_2$ between some sections $H_i = S_i/N_i$ $(i = 1, 2)$ of $G$.*

*Proof.* Let $S$ be a subgroup of $G^2$. For $i = 1, 2$ let $S_i = \mathrm{pr}_i(S)$, and let $N_i$ be the $i$-th coordinate kernel of $S$. By Lemma 2.3, $N = N_1 \times N_2$ is a normal subgroup of $S$, and $H = S/N$ is a subdirect subgroup of the group $H_1 \times H_2$ where $H_i = S_i/N_i$. Moreover, $H$ satisfies condition (2) from Definition 2.2. Thus Lemma 2.4 shows that $H = \Gamma[\sigma]$ for some isomorphism $\sigma\colon H_1 \to H_2$. Hence $S = \Gamma_{N_1,N_2}[\sigma]$, as claimed. $\square$

For a section $H_0 = S_0/N_0$ of $G$ the subgroup of $H_0^3$ in (2.9) will be denoted by $\Upsilon[P_0, Q_0]$, and its inverse image under the natural homomorphism $S_0^3 \to (S_0/N_0)^3 = H_0^3$ by $\Upsilon_{N_0}[P_0, Q_0]$. Thus

$$\Upsilon_{N_0}[P_0, Q_0] = \{(s_1d, s_2d, s_1s_2d) : N_0s_1, N_0s_2 \in P_0,\ N_0d \in Q_0\}.$$

**Theorem 2.21.** *Let $G$ be a finite group whose Sylow subgroups are abelian. A finitary operation $f$ on the underlying set of $G$ is a term operation of $G$ if and only if the following subgroups of $G^2$ and $G^3$ are closed under $f$:*

(i) *all subgroups of $G^2$, and*
(ii) *all subgroups $\Upsilon_{N_0}[P_0, Q_0]$ of $G^3$ where $P_0$ is a normal Sylow subgroup of a section $H_0 = S_0/N_0$ of $G$ and $Q_0$ is a complement of $P_0$ in $H_0$.*

(Note that $f$ preserves all subgroups of $G^2$ if and only if it preserves some subgroups of $G^3$, namely the subgroups of $G \times G \times \{1\}$.)

*Proof.* An operation on the underlying set of $G$ is a term operation of $G$ if and only if all subgroups of finite powers of $G$ are closed under $f$. Therefore the statement of the theorem is equivalent to the following: all subgroups of finite powers of $G$ are closed under $f$ if the subgroups listed in (i) and (ii) are closed under $f$. To prove this we will make use of the following fact.

**Claim 2.22.** *Let $g$ be an operation on a set $A$, and let $T_i$ $(i \in I)$, $T, T'$ be subsets of finite powers of $A$.*

- *If all $T_i$ $(\subseteq A^k)$ $(i \in I)$ are closed under $g$, then so is $\bigcap_{i \in I} T_i$.*
- *If $T$ and $T'$ are closed under $g$, then so is $T \times T'$.*
- *If $T$ is closed under $g$, then so is every set that arises from $T$ by performing a fixed permutation on the coordinates of $T$.*
- *If $T$ $(\subseteq A^k)$ is closed under $g$, then so is $\mathrm{pr}_I(T)$ for all nonempty $I \subseteq \{1, \dots, k\}$.*

By definition, $T$ is closed under $g$ if and only if $T$ is (the underlying set of) a subalgebra of some finite power of the algebra $(A; g)$. Thus the statement of the claim can be rephrased as follows: the collection of all subalgebras of finite powers of $(A; g)$ is closed under intersection, direct product, permuting coordinates, and projecting onto some coordinates. Hence the proof of the claim is straightforward.

Now let $f$ be an operation on $G$, and let us assume that the subgroups of $G^2$ and $G^3$ listed in (i)–(ii) are closed under $f$. We want to argue that all subgroups of finite powers of $G$ must then be closed under $f$.

If $S$ is a subgroup of $G$, then $S^2$ is a subgroup of $G^2$ such that $S = \mathrm{pr}_1(S^2)$. Since by assumption $S^2$ is closed under $f$, it follows from Claim 2.22 that $S$ is also closed under $f$. Hence $f$ can be restricted to any subgroup $S$ of $G$. The restriction of $f$ to $S$ will be denoted by $f^S$.

Let $S/N$ be a section of $G$, and consider the subgroup $\Gamma_{N,N}[\mathrm{id}_{S/N}]$ of $G^2$ where $\mathrm{id}_{S/N}$ is the identity isomorphism $S/N \to S/N$. Clearly, $\Gamma_{N,N}[\mathrm{id}_{S/N}]$ is the congruence relation of $S$ with kernel $N$. Only elements of $S$ are involved in this relation, therefore the assumption that the subgroup $\Gamma_{N,N}[\mathrm{id}_{S/N}]$ of $G^2$ is closed under $f$, means that the congruence of $S$ with kernel $N$ is closed under $f^S$ (an operation on $S$). Thus $f^S$ (and hence $f$) has a natural action on the quotient $S/N$, which we will denote by $f^{S/N}$.

Now consider an arbitrary subgroup $S$ of some finite power $G^n$ of $G$. Our goal is to show that $S$ is closed under $f$. The case $n = 1$ was settled above, while the case $n = 2$ is part of our assumptions. Therefore we will assume from now on that $n \geq 3$ and that all subgroups of $G^{n-1}$ are closed under $f$. We may also assume that $S$ is meet irreducible in the lattice of subgroups of $G^n$. The reason for this is that every subgroup of $G^n$ is an intersection of meet irreducible subgroups, and if some subgroups are closed under $f$, then so is their intersection (cf. Claim 2.22).

For each $i$ $(1 \leq i \leq n)$ let $S_i = \mathrm{pr}_i(S)$, let $N_i$ be the $i$-th coordinate kernel of $S$, and let $H_i = S_i/N_i$. Clearly, $S$ is a subdirect subgroup of $\prod S_i$. If $|H_i| = 1$ for some $i$, say $i = 1$, then $N_1 = S_1$ and $S_1 \times \{1\}^{n-1}$ is a subgroup of $S$. This implies that $S = S_1 \times \mathrm{pr}_{2,\dots,n}(S)$. Here $S_1$ is a subgroup of $G$ and $\mathrm{pr}_{2,\dots,n}(S)$ is a subgroup of $G^{n-1}$. Since by our assumptions $S_1$ as well as $\mathrm{pr}_{2,\dots,n}(S)$ are closed under $f$, it follows from Claim 2.22 that their direct product is closed under $f$. Hence $S$ is closed under $f$ in this case. Therefore from now on we will assume that $|H_i| > 1$ for all $i$. Lemma 2.3 shows that the group $H = S/\prod N_i$ is a subdirect subgroup of $\prod H_i$, $H$ has trivial coordinate kernels, and $H$ is meet irreducible in the lattice of subgroups of $\prod H_i$. Thus $H$ is a reduced subgroup of $\prod H_i$.

**Claim 2.23.** *$S$ is closed under the operation $f$ if and only if $H$ is closed under the operation $f^{H_1} \times \cdots \times f^{H_n}$ which acts in the $i$-th coordinate as $f^{H_i} = f^{S_i/N_i}$ for all $i$ $(1 \leq i \leq n)$.*

By definition, '$S$ is closed under $f$' means that $S$ is closed under the coordinatewise application of $f$ to elements of $S$. Since the $i$-th coordinates of elements of $S$ all belong to $S_i$, when we apply $f$ coordinatewise to elements of $S$, in the $i$-th coordinate we use only its restriction $f^{S_i}$ to $S_i$. In other words, $S$ is closed under the coordinatewise action of $f$ if and only if $S$ is closed under the operation $f^{S_1} \times \cdots \times f^{S_n}$. By construction, $H$ arises from $S$ by factoring out its normal subgroup $N_1 \times \cdots \times N_n$, and $S$ is the full inverse image of $H$ under the product homomorphism

$$S_1 \times \cdots \times S_n \to (S_1/N_1) \times \cdots \times (S_n/N_n) = H_1 \times \cdots \times H_n.$$

Therefore it is easy to see that $S$ is closed under the operation $f^{S_1} \times \cdots \times f^{S_n}$ if and only if $H$ is closed under the operation $f^{S_1/N_1} \times \cdots \times f^{S_n/N_n}$. This proves Claim 2.23.

In particular, we can apply Claim 2.23 to the subgroups $\Gamma_{N_1,N_2}[\sigma]$ and $\Upsilon_{N_0}[P_0, Q_0]$ in place of $S$. (These subgroups have coordinate kernels $N_1, N_2$ and $N_0, N_0, N_0$, respectively.) Thus the assumption that these subgroups are closed under $f$ translates, in the spirit of Claim 2.23, into the following statements.

**Claim 2.24.** (1) *If $\sigma\colon H_1 \to H_2$ is an isomorphism between sections of $G$, then the graph $\Gamma[\sigma]$ of $\sigma$ is closed under the operation $f^{H_1} \times f^{H_2}$.*

(2) *If $H_0 = S_0/N_0$ is a section of $G$, $P_0$ is a normal Sylow subgroup of $H_0$ and $Q_0$ is a complement of $P_0$ in $H_0$, then the subgroup $\Upsilon[P_0, Q_0]$ of $H_0^3$ is closed under the operation $f^{H_0}$.*

In view of Claim 2.23 it remains to check that $H$ is closed under the operation $f^{H_1} \times \cdots \times f^{H_n}$. We established earlier that $H$ is a reduced subgroup of $\prod H_i$. Here all $H_i$ are sections of $G$, therefore the property of $G$ that its Sylow subgroups are abelian, is inherited by all $H_i$. Thus Lemma 2.12 applies to $H$. We will use all the notation introduced in Lemma 2.12. The assumption $|H_1| \leq \cdots \leq |H_n|$ does not restrict generality, because it can be achieved by permuting the coordinates of the original subgroup $S$, and according to Claim 2.22, permuting coordinates does not affect closure under $f$.

Our goal is to show that $H$ is closed under the operation $f^{H_1} \times \cdots \times f^{H_n}$. First we will look at the subgroup $H^*$ of $H_n^n$.

**Claim 2.25.** *$H^*$ is closed under $f^{H_n}$.*

Claim 2.24 provides a collection of subgroups of $H_n^2$ and $H_n^3$ that are closed under $f^{H_n}$; among them are

- the subgroups $\Gamma[\chi_i]$ $(i = 1, \ldots, n-1)$ of $H_n^2$ where $\chi_i$ is the automorphism of the subgroup $H_i^*$ of $H_n$ from Lemma 2.12, and
- the subgroup $\Upsilon[P_n, Q_n]$ of $H_n^3$ where $P_n$ is the normal Sylow subgroup of $H_n$ and $Q_n$ is a complement of $P_n$ in $H_n$, as in Lemma 2.12.

We will prove Claim 2.25 by showing that $H^*$ can be constructed from these subgroups, using the constructions described in Claim 2.22.

We start with defining a sequence $\Upsilon_k$ of subgroups of $H_n^k$ $(k \geq 2)$ as follows:

$$\Upsilon_k = \{(x_1c, x_2c, \ldots, x_kc, x_1x_2\cdots x_kc) : c \in Q_n,\ x_1, x_2, \ldots, x_k \in P_n\}.$$

Clearly, $\Upsilon_2 = \Upsilon[P_n, Q_n]$. The following equality shows how to construct $\Upsilon_{k+1}$ from $\Upsilon_k$ and $\Upsilon_2$:

$$\begin{aligned}\Upsilon_{k+1} = \{(y_1, \ldots, y_k, y_{k+2}, y_{k+3}) \in H_n^{k+2} &: \text{there exists } y_{k+1} \in H_n \text{ such that} \\ &(y_1, \ldots, y_k, y_{k+1}) \in \Upsilon_k \text{ and } (y_{k+1}, y_{k+2}, y_{k+3}) \in \Upsilon_2\}.\end{aligned} \tag{2.10}$$

To prove (2.10) let $\Upsilon'_{k+1}$ denote the set on the right hand side, and consider an arbitrary $(k+2)$-tuple $(y_1, \ldots, y_k, y_{k+2}, y_{k+3})$ from $H_n^{k+2}$. By definition, we have $(y_1, y_2, \ldots, y_k, y_{k+2}, y_{k+3}) \in \Upsilon'_{k+1}$ if and only if there exists an element $y_{k+1} \in H_n$ such that $(y_1, y_2, \ldots, y_k, y_{k+1}) \in \Upsilon_k$ and $(y_{k+1}, y_{k+2}, y_{k+3}) \in \Upsilon_2$. These conditions mean that

$$(y_1, y_2, \ldots, y_k, y_{k+1}) = (x_1c, x_2c, \ldots, x_kc, x_1x_2\cdots x_kc)$$

for some $c \in Q_n$ and $x_1, x_2, \ldots, x_k \in P_n$, and

$$(y_{k+1}, y_{k+2}, y_{k+3}) = (x'_1c', x_{k+1}c', x'_1x_{k+1}c')$$

for some $c' \in Q_n$ and $x'_1, x_{k+1} \in P_n$. In particular, $x_1x_2\cdots x_kc = y_{k+1} = x'_1c'$. But in $H_n = P_nQ_n$ every element can be written uniquely as a product of an element from $P_n$ and an element from $Q_n$. Therefore the displayed equalities hold exactly when $x_1x_2\cdots x_k = x'_1$ and $c = c'$. In that case $y_{k+3} = x'_1x_{k+1}c' = x_1x_2\cdots x_kx_{k+1}c$ and

$$(y_1, y_2, \ldots, y_k, y_{k+2}, y_{k+3}) = (x_1c, x_2c, \ldots, x_kc, x_{k+1}c, x_1x_2\cdots x_kx_{k+1}c).$$

This proves the equality in (2.10).

Now, using the description of $H^*$ in (2.3) we can express $H^*$ with $\Upsilon_n$ and $\Gamma[\chi_i]$ $(i = 1, \ldots, n-1)$ as follows:

$$H^* = \{(y_1, \ldots, y_{n-1}, z_n) \in H_n^n : \text{there exist } z_1, \ldots, z_{n-1} \in H_n \text{ such that } (y_i, z_i) \in \Gamma[\chi_i] \text{ for } i = 1, \ldots, n-1 \text{ and } (z_1, \ldots, z_n) \in \Upsilon_{n-1}\}. \tag{2.11}$$

To prove this equality let $H'$ denote the right hand side of (2.11), and consider an arbitrary $n$-tuple $(y_1, \ldots, y_{n-1}, z_n)$ from $H_n^n$. By definition, $(y_1, \ldots, y_{n-1}, z_n)$ belongs to $H'$ if and only if for some elements $z_1, \ldots, z_{n-1} \in H_n$ we have $(y_i, z_i) \in \Gamma[\chi_i]$ for $i = 1, \ldots, n-1$ and $(z_1, \ldots, z_n) \in \Upsilon_{n-1}$. These conditions mean that $z_i = \chi_i(y_i)$ for all $i = 1, \ldots, n-1$ and

$$(z_1, z_2, \ldots, z_{n-1}, z_n) = (x_1'c, x_2'c, \ldots, x_{n-1}'c, x_1'x_2' \cdots x_{n-1}'c)$$

for some $c \in Q_n$ and $x_1', x_2', \ldots, x_{n-1}' \in P_n$. In particular, the last displayed equality implies that for all $i = 1, \ldots, n-1$ we have $z_i = x_i'c$, while the equality $z_i = \chi_i(y_i)$ implies that $z_i$ belongs to the range $H_i^* = P_i^* Q_n$ of $\chi_i$. Therefore $x_i' \in P_i^*$. Since the automorphism $\chi_i$ of $H_i^*$ restricts to $P_i^*$ as $\psi_i$ and to $Q_n$ as the identity, we get that $y_i = \psi_i^{-1}(x_i')c$ for all $i$. So, with the notation $x_i = \psi_i^{-1}(x_i')$ we get that $x_i \in P_i^*$ and $x_i' = \psi_i(x_i)$ for all $i$, moreover,

$$(y_1, \ldots, y_{n-1}, z_n) = (x_1c, \ldots, x_{n-1}c, \psi_1(x_1) \cdots \psi_{n-1}(x_{n-1})c).$$

This finishes the proof of the equality (2.11).

We can rewrite the right hand sides of (2.10) and (2.11) in a form that shows more explicitly that these subgroups do indeed arise from $\Upsilon_2 = \Upsilon[P_n, Q_n]$ and $\Gamma[\chi_i]$ by the constructions described in Claim 2.22. As for (2.10), the set of all $(k+3)$-tuples $(y_1, \ldots, y_k, y_{k+1}, y_{k+2}, y_{k+3}) \in H_n^{k+3}$ such that $(y_1, \ldots, y_k, y_{k+1}) \in \Upsilon_k$ and $(y_{k+1}, y_{k+2}, y_{k+3}) \in \Upsilon_2$ is the set $(\Upsilon_k \times H_n^2) \cap (H_n^k \times \Upsilon_2)$. The right hand side of (2.10) consists of all $(k+2)$-tuples $(y_1, \ldots, y_k, y_{k+2}, y_{k+3})$ that arise from such $(k+3)$-tuples by omitting their coordinate $y_{k+1}$. Therefore

$$\Upsilon_{k+1} = \mathrm{pr}_{1,\ldots,k,k+2,k+3}\big((\Upsilon_k \times H_n^2) \cap (H_n^k \times \Upsilon_2)\big). \tag{2.12}$$

Similarly, since the set of all $(2n-1)$-tuples $(y_1, z_1, \ldots, y_{n-1}, z_{n-1}, z_n) \in H_n^{2n-1}$ satisfying $(y_i, z_i) \in \Gamma[\chi_i]$ for all $i = 1, \ldots, n-1$ is the set $\Gamma[\chi_1] \times \cdots \times \Gamma[\chi_{n-1}] \times H_n$ while the set of all $(2n-1)$-tuples $(y_1, \ldots, y_{n-1}, z_1 \ldots, z_{n-1}, z_n) \in H_n^{2n-1}$ satisfying $(z_1, \ldots, z_{n-1}, z_n) \in \Upsilon_{n-1}$ is the set $H_n^{n-1} \times \Upsilon_{n-1}$, it follows that

$$H^* = \mathrm{pr}_{1,\ldots,n-1,2n-1}\big((\Gamma[\chi_1] \times \cdots \times \Gamma[\chi_{n-1}] \times H_n)^\dagger \cap (H_n^{n-1} \times \Upsilon_{n-1})\big) \tag{2.13}$$

where $^\dagger$ indicates that the coordinates $(y_1, z_1, \ldots, y_{n-1}, z_{n-1}, z_n)$ of the group $\Gamma[\chi_1] \times \cdots \times \Gamma[\chi_{n-1}] \times H_n$ have to be reordered in the form $(y_1, \ldots, y_{n-1}, z_1 \ldots, z_{n-1}, z_n)$ before intersecting with $H_n^{n-1} \times \Upsilon_{n-1}$.

This completes the proof of Claim 2.25.

Now we prove that $H$ is closed under the operation $f^{H_1}\times\cdots\times f^{H_n}$. In the equality (2.2) that relates $H$ to $H^*$ the embedding $\varphi_i\colon H_i\to H_n$ $(i=1,\dots,n-1)$ maps onto the subgroup $H_i^*$ of $H_n$, since $H^*$ is a subdirect subgroup of $H_1^*\times\cdots\times H_{n-1}^*\times H_n$. Therefore we can consider each $\varphi_i$ $(i=1,\dots,n-1)$ as an isomorphism $H_i\to H_i^*$. For $i=n$ let $\varphi_n$ be the identity map of $H_n$. So, by (2.2) we have

$$H=\bigl\{\bigl(\varphi_1^{-1}(h_1),\dots,\varphi_n^{-1}(h_n)\bigr):(h_1,\dots,h_n)\in H^*\bigr\}.$$

In view of Claim 2.24 the graph $\Gamma[\varphi_i^{-1}]$ of each group isomorphism $\varphi_i^{-1}\colon H_i^*\to H_i$ is closed under the operation $f^{H_i^*}\times f^{H_i}$. Hence $\varphi_i^{-1}$ is an isomorphism between the algebras $(H_i^*;f^{H_i^*})$ and $(H_i;f^{H_i})$. By Claim 2.25 $H^*$ is closed under the coordinatewise action of the operation $f^{H_n}\times\cdots\times f^{H_n}$. However, for $1\le i\le n-1$ we have $\mathrm{pr}_i(H^*)=H_i^*$, therefore when we check the closure of $H$ under $f^{H_n}\times\cdots\times f^{H_n}$, then in the $i$-th coordinate we apply $f^{H_n}$ only to elements of the subgroup $H_i^*$ of $H_n$, that is, we in fact apply $f^{H_i^*}$ instead of $f^{H_n}$. This shows that $H^*$ is closed under the coordinatewise action of the operation $f^{H_1^*}\times\cdots\times f^{H_{n-1}^*}\times f^{H_n}$. Since $H$ arises from $H^*$ by applying the isomorphisms $\varphi_i^{-1}\colon(H_i^*;f^{H_i^*})\to(H_i;f^{H_i})$ coordinatewise in the first $n-1$ coordinates, it follows that $H$ is closed under the coordinatewise action of the operation $f^{H_1}\times\cdots\times f^{H_{n-1}}\times f^{H_n}$.

Applying Claim 2.23 we get that $S$ is closed under $f$. This completes the proof of Theorem 2.21. □

## 3. Examples and Problems

Let $G$ be a finite group and let $\mathbf{A}_k$ be the algebra whose underlying set is $G$ and whose operations are all finitary operations on the set $G$ which preserve the subgroups of $G^k$. Since operations from the clone of $G$ preserve all subgroups of powers, it follows that $\mathrm{Clo}(G)\subseteq\mathrm{Clo}(\mathbf{A}_k)$ for all $k$. Any operation in $\mathrm{Clo}(\mathbf{A}_k)$ preserves all subgroups of $G^k$, hence all subgroups of $G^{k-1}\times\{1\}$, hence preserves all subgroups of $G^{k-1}$. This shows that

$$\mathrm{Clo}(G)\subseteq\cdots\subseteq\mathrm{Clo}(\mathbf{A}_3)\subseteq\mathrm{Clo}(\mathbf{A}_2)\subseteq\mathrm{Clo}(\mathbf{A}_1),$$

while $\mathrm{Clo}(G)=\bigcap_{k\in\mathbb{N}}\mathrm{Clo}(\mathbf{A}_k)$ by the fact (mentioned in the Introduction) that the clone of a finite group consists of the operations that preserve the subgroups of finite powers. We will say that the clone of $G$ is **determined** by the subgroups of $G^k$ if $\mathrm{Clo}(G)=\mathrm{Clo}(\mathbf{A}_k)$. The main result of the previous section is that if $G$ has abelian Sylow subgroups, then the clone of $G$ is determined by the subgroups of $G^3$. In this section we look at the equality $\mathrm{Clo}(G)=\mathrm{Clo}(\mathbf{A}_k)$ for other groups and other values of $k$. First we present some useful facts.

**Lemma 3.1.** *Let $G$ be a finite group.*

(1) *If $k\ge1$, then $\mathbf{A}_k$ and $G$ have the same subalgebras.*
(2) *If $k\ge2$, then $\mathbf{A}_k$ and $G$ have the same congruences and the same unary term operations.*

*Let $\theta_N$ denote the congruence on $G$ associated to $N \lhd G$.*

(3) *If $k \geq 3$, then $[\theta_G, \theta_G]$ in $\mathbf{A}_k$ equals $\theta_{[G,G]}$.*
(4) *If $k \geq 4$, then $[\theta_M, \theta_N]$ in $\mathbf{A}_k$ equals $\theta_{[M,N]}$.*

*Proof.* Since $\mathbf{A}_k$ is an expansion of $G$, the subalgebras of $\mathbf{A}_k$ are subgroups of $G$. If $k \geq 1$, then every subgroup of $G$ is a subalgebra of $\mathbf{A}_k$ by the remarks at the beginning of this section.

The part of item (2) concerning congruences follows from the fact that the same subsets of $G^2$ are subalgebras for both $\mathbf{A}_k$ and $G$ if $k \geq 2$, and the congruences on either are the subalgebras of the square that are equivalence relations.

To see that $\mathbf{A}_k$ and $G$ have the same unary term operations when $k \geq 2$ it suffices to show that if $t(x)$ is a term operation of $\mathbf{A}_k$, then it is of the form $t(x) = x^m$ for some $m$. Assume that $t(x)$ is a term operation of $\mathbf{A}_k$. Since $k \geq 2$, the operation $t$ preserves the subgroups of $G$. Hence for any $g \in G$ we have $t(g) \in \langle g \rangle$, and therefore $t(g) = g^{e(g)}$ for some integer $e(g)$ (possibly depending on $g$) that is unique modulo the order $|g|$ of $g$.

**Claim 3.2.** *If $|b|$ divides $|a|$, then $e(a) \equiv e(b) \pmod{|b|}$. Hence $t(b) = b^{e(a)}$.*

Since $t$ maps the subgroup $\langle (a,b) \rangle$ of $G^2$ into itself, there exists some $f \in \mathbb{Z}$ such that $t(a,b) = (a,b)^f = (a^f, b^f)$. But we also have $t(a,b) = (t(a), t(b)) = (a^{e(a)}, b^{e(b)})$, so $e(a) \equiv f \pmod{|a|}$ and $e(b) \equiv f \pmod{|b|}$. Since $|b|$ divides $|a|$, we get $e(a) \equiv f \equiv e(b) \pmod{|b|}$, and therefore $t(b) = b^{e(b)} = b^{e(a)}$.

Choose a prime $p$ dividing $|G|$, and choose an element $a \in G$ of maximum $p$-power order. Claim 3.2 guarantees that $t(x) = x^{e(a)}$ for any $x$ of $p$-power order. Now suppose that $|G|$ is divisible by $r$ different primes, and that $a_1, \ldots, a_r$ are elements of maximum prime power order for each of those primes. Choose an integer $m$ such that $m \equiv e(a_i) \pmod{|a_i|}$ for all $i$. Then $m$ is unique modulo the exponent of the group, and $t(x) = x^m$ whenever $x$ has prime power order. In fact, we claim that $t(x) = x^m$ for all $x$. To see this, choose any $c \in G$ and set $e = e(c)$. Then $t(d) = d^e$ whenever $|d|$ divides $|c|$, in particular $t(x) = x^e$ if $x \in \langle c \rangle$. Therefore, on any Sylow $p$-subgroup of $\langle c \rangle$ both $t(x) = x^e$ and $t(x) = x^m$ hold, proving that $e$ and $m$ are congruent modulo any prime power divisor of $|c|$. This means that $t(c) = c^e = c^m$, completing the proof that $t(x) = x^m$ for any $x \in G$.

For items (3) and (4), the fact that $\mathbf{A}_k$ is an expansion of $G$ for all $k$ implies that $[\theta_M, \theta_N] \geq \theta_{[M,N]}$ for all $k$. To prove equality we may work modulo $\theta_{[M,N]}$ since this is a congruence on both $\mathbf{A}_k$ and $G$ when $k \geq 2$. This reduces (3) to the statement: if $G$ is abelian, then so is $\mathbf{A}_3$. This is easy to prove directly for arbitrary groups $G$, but certainly follows from Theorem 2.1 for finite $G$.

For item (4), the subalgebras of $G^4 = G^{2\times 2}$ and $\mathbf{A}_k^4 = \mathbf{A}_k^{2\times 2}$ generated by the matrices

$$\begin{bmatrix} a & a \\ b & b \end{bmatrix} \qquad \text{and} \qquad \begin{bmatrix} c & d \\ c & d \end{bmatrix}$$

with $(a, b) \in \theta_M$ and $(c, d) \in \theta_N$ are the same if $k \geq 4$. But the value of $[\theta_M, \theta_N]$ depends only on this subalgebra according to Theorem 4.9 of [2], so the commutator of congruences coincides on $\mathbf{A}_k$ and $G$. $\square$

**Example 3.3.** In this example we show that $\mathrm{Clo}(G) \subsetneq \mathrm{Clo}(\mathbf{A}_1)$ for any group $G$.

The **discriminator operation** on a set is the ternary operation defined by

$$d(x, y, z) := \begin{cases} z, & \text{if } x = y; \\ x, & \text{otherwise.} \end{cases}$$

If $G$ is any group and $a, b, c \in G$, then $d(a, b, c)$ is either $a$ or $c$, hence certainly belongs to the subgroup generated by $\{a, b, c\}$. This shows that all subgroups of $G$ are closed under the discriminator. If the discriminator were a term operation of $G$, then it would be a term operation of any nontrivial cyclic subgroup of $G$. If some cyclic subgroup had infinitely many (or $m$) elements, then when written additively $d$ could be represented in the form $d(x, y, z) = \alpha x + \beta y + \gamma z$ with $\alpha, \beta, \gamma \in \mathbb{Z}$ (or $\mathbb{Z}_m$). Since $d(x, x, y) = y = d(y, x, y) = d(y, x, x)$ we derive that $\alpha + \beta = 0$, $\gamma = 1$, $\beta = 0$, $\alpha + \gamma = 1$, $\alpha = 1$ and $\beta + \gamma = 0$ all hold. It is clearly impossible to find integers (modulo $m$, $m > 1$) satisfying these conditions.

**Example 3.4.** In this example we show that there do exist some finite groups satisfying $\mathrm{Clo}(G) = \mathrm{Clo}(\mathbf{A}_2)$. First we show that if $G$ is a finite group with a normal subgroup $P$ of prime order such that $G/P$ has smaller exponent than $G$, then $\mathrm{Clo}(G) \subsetneq \mathrm{Clo}(\mathbf{A}_2)$. Then we show that the converse is true when $G$ is abelian.

**Theorem 3.5.** *If a finite group $G$ has a normal subgroup $P$ of prime order such that $G/P$ has smaller exponent than $G$, then the clone of $G$ is not determined by the subgroups of $G^2$.*

*Proof.* Suppose that $t(\mathbf{x})$ is an $n$-ary term operation of $G$ and that $t(G^n) \subseteq P$. We will prove that if $d(x, y, z)$ is the discriminator operation on $P$, then $d\big(t(\mathbf{x}), t(\mathbf{y}), t(\mathbf{z})\big)$ is compatible with all subgroups of $G^2$. In the reverse direction, we will show that if $t(x)$ is a nonconstant *unary* term operation of $G$ such that $t(G) \subseteq P$, then $d\big(t(x), t(y), t(z)\big)$ is not in the clone of $G$. Finally, we will explain how these two facts establish the theorem.

Assume that $t(\mathbf{x})$ is an $n$-ary term operation of $G$ and that $t(G^n) \subseteq P$. To establish that $d\big(t(\mathbf{x}), t(\mathbf{y}), t(\mathbf{z})\big)$ is compatible with the subgroups of $G^2$ we must show that if $(a_i, a_i'), (b_i, b_i'), (c_i, c_i') \in G^2$ for $i = 1, \ldots, n$, then

$$d\big((t(\mathbf{a}), t(\mathbf{a}')), (t(\mathbf{b}), t(\mathbf{b}')), (t(\mathbf{c}), t(\mathbf{c}'))\big) \in \langle \{(a_i, a_i'), (b_i, b_i'), (c_i, c_i') \mid 1 \leq i \leq n\} \rangle.$$

We have $\big(t(\mathbf{a}), t(\mathbf{a}')\big) \in \langle\{(a_i, a_i') \mid 1 \le i \le n\}\rangle$, $\big(t(\mathbf{b}), t(\mathbf{b}')\big) \in \langle\{(b_i, b_i') \mid 1 \le i \le n\}\rangle$, and $\big(t(\mathbf{c}), t(\mathbf{c}')\big) \in \langle\{(c_i, c_i') \mid 1 \le i \le n\}\rangle$ since $t$ is a group term. Next, we argue that $d\big((t(\mathbf{a}), t(\mathbf{a}')), (t(\mathbf{b}), t(\mathbf{b}')), (t(\mathbf{c}), t(\mathbf{c}'))\big)$ belongs to the subgroup of $G^2$ generated by $\big\{\big(t(\mathbf{a}), t(\mathbf{a}')\big), \big(t(\mathbf{b}), t(\mathbf{b}')\big), \big(t(\mathbf{c}), t(\mathbf{c}')\big)\big\}$. Since the image of $t$ is contained in $P$, it suffices to show that the subgroups of $P^2$ are closed under $d$. Suppose that $(u, u'), (v, v'), (w, w') \in P^2$. If $d\big((u, u'), (v, v'), (w, w')\big) \in \{(u, u'), (w, w')\}$, then there is nothing to prove. Otherwise $d\big((u, u'), (v, v'), (w, w')\big) = (w, u')$ (if $u = v$ and $u' \neq v'$) or $d\big((u, u'), (v, v'), (w, w')\big) = (u, w')$ (if $u \neq v$ and $u' = v'$). Both arguments are similar, so assume the latter. In this case $u \neq v$ while $u' = v'$, so the subgroup generated by $\{(u, u'), (v, v')\}$ contains $P \times \{1\}$. If the subgroup generated by $\{(u, u'), (v, v'), (w, w')\}$ contains more than this, then it contains all of $P^2$, hence contains $d\big((u, u'), (v, v'), (w, w')\big) = (u, w')$ and we are done. Otherwise the subgroup generated by $\{(u, u'), (v, v'), (w, w')\}$ is exactly $P \times \{1\}$, in which case $u' = v' = w' = 1$. In this case, $d\big((u, u'), (v, v'), (w, w')\big) = (u, w') = (u, u')$.

Now suppose that $t(x) = x^m$ is a nonconstant unary term operation, $t(G) \subseteq P$, and $|P| = p$. Since $P$ is generated by the image of the term operation $t$, $P$ is normal. The exponent $e$ of $G$ does not divide $m$, since $t$ is nonconstant, but the exponent $f$ of $G/P$ does divide $m$ since $t(G) \subseteq P$. Therefore $e = fp$, and there is an element $u \in G$ of $p$-power order such that $u^m \neq 1$. If $d(x^m, y^m, z^m)$ is a term operation of $G$, then it is a term operation of the cyclic subgroup $\langle u \rangle$, which has order $p^k$ for some $k$. Any ternary term of a cyclic subgroup can be represented as $\alpha x + \beta y + \gamma z$ for some $\alpha, \beta, \gamma \in \mathbb{Z}_{p^k}$ when written additively. Arguing as we did at the end of Example 3.3, one sees that $d(x^m, y^m, z^m)$ is not a term operation.

To complete the proof of the theorem, assume that $G$ has a normal subgroup $P$ of prime order such that $G/P$ has smaller exponent $f$ than the exponent of $G$. Then $t(x) = x^f$ is a nonconstant unary term operation whose image is contained in $P$. By the first part of the proof $d(x^f, y^f, z^f)$ is compatible with the subgroups of $G^2$, while by the second part of the proof $d(x^f, y^f, z^f)$ is not a term operation of $G$. $\square$

The proof of Theorem 3.5 suggests the following problem. Recall that a subgroup $P$ of $G$ is **verbal** if it is generated by the union of the images of some term operations.

**Problem 3.6.** Prove or disprove: if $G$ is a finite group with a verbal subgroup of prime order, then the clone of $G$ is not determined by the subgroups of $G^2$.

Our proof of Theorem 3.5 shows that if $P$ is generated by the image of $t(\mathbf{x})$, then $d\big(t(\mathbf{x}), t(\mathbf{y}), t(\mathbf{z})\big)$ preserves the subgroups of $G^2$, but the proof does not show that this operation is not in $\mathrm{Clo}(G)$ except when $t$ is unary. Problem 3.6 could be solved by showing that $d\big(t(\mathbf{x}), t(\mathbf{y}), t(\mathbf{z})\big)$ is not in $\mathrm{Clo}(G)$ in general.

If $G$ has cyclic Sylow subgroups, then it satisfies the hypotheses of Theorem 3.5. Therefore the clone of such a group is not determined by the subgroups of its square although the clone is determined by the subgroups of its cube by the result of Section 2.

Next we prove that the converse of Theorem 3.5 holds for abelian groups.

**Theorem 3.7.** *The following conditions on a finite abelian group $G$ are equivalent:*
(i) *the clone of $G$ is determined by the subgroups of $G^2$;*
(ii) *$G$ has no verbal subgroups of prime order;*
(iii) *the two largest invariant factors of $G$ are equal.*

*Proof.* If $G$ is a finite abelian group, then $G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_{k+1}}$ with $n_1 \mid \cdots \mid n_{k+1}$, where $n_1, \ldots, n_{k+1}$ are the invariant factors.

To prove the implication (i)$\Rightarrow$(ii) assume that (ii) fails and that $P$ is a verbal subgroup of $G$ of prime order $p$. Suppose that $t(x_1, \ldots, x_n) = m_1x_1 + \cdots + m_nx_n$ is a term operation whose image generates $P$. Then each of the term operations $t(0, \ldots, 0, x_i, 0, \ldots, 0) = m_ix_i$ also has image in $P$, and at least one of them is nonconstant since they sum to $t(x_1, \ldots, x_n)$. Therefore $P$ is generated by the image of a unary term operation, say $s(x) = mx$. The quotient $G/P$ then has exponent dividing $m$ (since $s(G) \subseteq P$), but the exponent of $G$ does not divide $m$ (since $s$ is nonconstant). This shows that the exponent of $G/P$ is less than the exponent of $G$, so Theorem 3.5 proves that condition (i) fails.

If (iii) fails, then $n_k \neq n_{k+1}$, so for any prime $p$ that divides $n_{k+1}/n_k$ the term operation $s(x) := (n_{k+1}/p) \cdot x$ has image $P = \{0\} \times \cdots \times \{0\} \times (n_{k+1}/p)\mathbb{Z}_{n_{k+1}}$, which has size $p$. Therefore $G$ has a verbal subgroup of prime order, which is excluded by (ii). This established the implication (ii) $\Rightarrow$ (iii).

Finally, to show that (iii) $\Rightarrow$ (i), suppose that $n_k = n_{k+1}$ and that $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k} \times \mathbb{Z}_{n_k}$. Recall that $\mathbf{A}_2$ is the algebra whose underlying set is $G$ and whose defining operations are those compatible with the subgroups of $G^2$. These operations include the term operations of $G$, so $\mathbf{A}_2$ generates a congruence permutable variety. $\mathbf{A}_2$ has the same subalgebras as $G$, and $\mathbf{A}_2^2$ has the same subalgebras as $G^2$. The latter of these properties implies that $\mathbf{A}_2$ and $G$ have the same congruences. Therefore $\mathbf{A}_2$ has the same kind of direct factorizations as $G$, which gives us that $\mathbf{A}_2 \cong \mathbf{B}_1 \times \cdots \times \mathbf{B}_k \times \mathbf{B}_{k+1}$ where the equality of the congruences of $G$ and $\mathbf{A}_2$ implies that the projections onto the largest two factors $\mathbb{Z}_{n_k} \times \mathbb{Z}_{n_k}$ and $\mathbf{B}_k \times \mathbf{B}_{k+1}$ have the same congruences. Since $\mathbb{Z}_{n_k} \times \mathbb{Z}_{n_k}$ is the square of an abelian group, the projection kernels together with the diagonal normal subgroup generate a $0, 1$-sublattice of normal subgroups isomorphic to the 5-element modular nondistributive lattice $\mathbf{M}_3$. Therefore $\mathbf{B}_k \times \mathbf{B}_{k+1}$ has a $0, 1$-sublattice of congruences isomorphic to $\mathbf{M}_3$, so by Exercise 1 of Chapter 3 of [2] the algebra $\mathbf{B}_k \times \mathbf{B}_{k+1}$ is abelian, and therefore both factors $\mathbf{B}_k$ and $\mathbf{B}_{k+1}$ are abelian. For any $i < k$ we can select a subgroup $H_i \leq \mathbb{Z}_{n_k}$ with $H_i \cong \mathbb{Z}_{n_i}$. Then $\mathbb{Z}_{n_i} \times H_i$ is a quotient of a subgroup of $G$, and the corresponding quotient of a subalgebra of $\mathbf{A}_2$ has the form $\mathbf{B}_i \times \mathbf{H}_i$ for a subalgebra $\mathbf{H}_i \leq \mathbf{B}_{k+1}$. Since $\mathbb{Z}_{n_i} \times H_i \cong \mathbb{Z}_{n_i} \times \mathbb{Z}_{n_i}$ is the square of an abelian group, we can repeat the above argument to prove that $\mathbf{B}_i \times \mathbf{H}_i$

is abelian. By projection we get that each $\mathbf{B}_i$ is abelian, and therefore the product $\mathbf{A}_2$ is abelian.

It follows from the structure theorem for abelian algebras in congruence modular varieties in [2] that $\mathbf{A}_2$ has the same polynomial operations as a module. Since $\mathbf{A}_2$ has all the term operations of $G$ (in particular, the identity element of $G$ is a constant operation of $\mathbf{A}_2$), and since $\mathbf{A}_2$ has the same subalgebras as $G$ (in particular the identity element of $G$ is a 1-element subalgebra of $\mathbf{A}_2$), it follows that $\mathbf{A}_2$ has the term operations of a module whose additive group is the same as $G$ and whose unary term operations are the same as those of $G$ (according to Lemma 3.1 (2)). This proves that $\mathrm{Clo}(\mathbf{A}_2) = \mathrm{Clo}(G)$. □

Theorem 3.7 describes all finite abelian groups $G$ whose clone is determined by the subgroups of $G^2$. This result leads us to pose the following problem.

**Problem 3.8.** Is there a nonabelian finite group $G$ whose clone is determined by the subgroups of $G^2$?

Next we turn to the equality $\mathrm{Clo}(G) = \mathrm{Clo}(\mathbf{A}_k)$ for $k > 3$. Natural questions concerning this equality are

**Problem 3.9.** Is it true that for every finite group $G$ there is a $k$ such that $\mathrm{Clo}(G) = \mathrm{Clo}(\mathbf{A}_k)$?

and

**Problem 3.10.** Is it true that there is a $k$ such that $\mathrm{Clo}(G) = \mathrm{Clo}(\mathbf{A}_k)$ for every finite group?

In view of the results of the previous section one might ask if $k = 3$ works in Problem 3.10. We will see that it does not. In the next example we will show that Problem 3.9 has a positive solution for nilpotent groups. We do not know the answer for Problem 3.10 even for nilpotent groups, but we will show that the smallest $k$ is greater than 3 for the quaternion group.

**Example 3.11.** In this example we show that if $G$ is a finite nonabelian nilpotent group, then $\mathrm{Clo}(G) = \mathrm{Clo}(\mathbf{A}_k)$ for $k = |G|^{[G:Z(G)]-1}$. In general, we expect that smaller values of $k$ will work, but we show here that $k = 3$ does not work for the quaternion group. (In fact, $\mathrm{Clo}(Q) = \mathrm{Clo}(\mathbf{A}_5) \subsetneqq \mathrm{Clo}(\mathbf{A}_4)$ if $Q$ is the quaternion group.)

**Lemma 3.12.** *Let $G$ be a group, and assume that $\mathcal{C}$ is a clone on the set $G$ containing $\mathrm{Clo}(G)$. If $\mathcal{C} \neq \mathrm{Clo}(G)$, then there is an operation $t \in \mathcal{C} \setminus \mathrm{Clo}(G)$ such that*

(1) $t(x_1, x_2, \ldots, x_{i-1}, 1, x_{i+1}, x_{i+2}, \ldots, x_n) = 1$ *for* $1 \leq i \leq n$, *and*
(2) $t(x_1, x_2, \ldots, x_{i-1}, x_i, x_i, x_{i+2}, \ldots, x_n) = 1$ *for* $1 \leq i \leq n-1$.

*If $t \in \mathcal{C} \setminus \mathrm{Clo}(G)$ satisfies* (1) *and $t \in \mathrm{Clo}(\mathbf{A}_3)$, then*

(3) $t(G^n) \subseteq [G, G]$,

*while if* $t \in \mathcal{C} \setminus \mathrm{Clo}(G)$ *satisfies* (1) *and* $t \in \mathrm{Clo}(\mathbf{A}_4)$*, then*

(4) $t(a_1, \ldots, a_n) = t(b_1, \ldots, b_n)$ *whenever* $a_i \equiv b_i \pmod{Z(G)}$ *for all* $i$.

*Proof.* We will use the notation $t(\mathbf{x})[x_i/s]$ to represent the operation obtained from an operation $t(\mathbf{x})$ by substituting the operation $s$ for the variable $x_i$ of $t$. In this notation, item (1) of the theorem is the statement $t(\mathbf{x})[x_i/1] = 1$, and item (2) is $t(\mathbf{x})[x_{i+1}/x_i] = 1$.

Assume that $\mathcal{C} \neq \mathrm{Clo}(G)$, and choose an operation $r_0(x_1, \ldots, x_n)$ of least arity for the property that $r_0 \in \mathcal{C} \setminus \mathrm{Clo}(G)$. For $1 \leq i \leq n$ let

$$r_i(\mathbf{x}) = r_{i-1}(\mathbf{x}) \cdot (r_{i-1}(\mathbf{x})[x_i/1])^{-1}.$$

Each $r_{i-1}(\mathbf{x})[x_i/1]$ is in $\mathcal{C}$ and has smaller arity than $r_0$, so $r_{i-1}(\mathbf{x})[x_i/1] \in \mathrm{Clo}(G)$. Since each of $r_i(\mathbf{x})$ and $r_{i-1}(\mathbf{x})$ are constructible from the other, the group operations, and $r_{i-1}(\mathbf{x})[x_i/1]$ ($\in \mathrm{Clo}(G)$), it follows that $r_i \in \mathrm{Clo}(G)$ if and only if $r_{i-1} \in \mathrm{Clo}(G)$; therefore $r_i \notin \mathrm{Clo}(G)$ for any $i$. Moreover, it is clear from the definition that $r_i(\mathbf{x})[x_j/1] = 1$ whenever $j \leq i$. Thus $r_n \in \mathcal{C} \setminus \mathrm{Clo}(G)$ is an operation for which item (1) holds.

In order to arrange that item (2) also holds, let $s_0(\mathbf{x}) = r_n(\mathbf{x})$. For $1 \leq i \leq n-1$ let $s_i(\mathbf{x}) = s_{i-1}(\mathbf{x}) \cdot (s_{i-1}(\mathbf{x})[x_{i+1}/x_i])^{-1}$. As above, each $s_i \in \mathcal{C} \setminus \mathrm{Clo}(G)$, and item (1) holds for each $s_i$. It is easy to check that $s_i(\mathbf{x})[x_{j+1}/x_j] = 1$ for $j \leq i$, so if $t := s_{n-1}$ then both (1) and (2) hold for $t$.

For item (3), assume that $t \in \big(\mathcal{C} \cap \mathrm{Clo}(\mathbf{A}_3)\big) \setminus \mathrm{Clo}(G)$. By Lemma 3.1 (2), $t$ must depend on at least two variables. From (1) we get

$$t(1, 1, g_3, \ldots, g_n) = 1 = t(g_1, 1, g_3, \ldots, g_n),$$

so

$$1 = t(1, g_2, g_3, \ldots, g_n)\ [\theta_G, \theta_G]\ t(g_1, g_2, g_3, \ldots, g_n).$$

By Lemma 3.1 (3) we get that $t(\mathbf{g}) \in [G, G]$ for any $\mathbf{g} \in G^n$.

For item (4) it suffices to show that

$$t(a_1, \ldots, a_{i-1}, \underline{a_i}, b_{i+1}, \ldots, b_n) = t(a_1, \ldots, a_{i-1}, \underline{b_i}, b_{i+1}, \ldots, b_n)$$

for each $i$, since each of these is a special case of (4) and a string of equalities of this type establishes that $t(a_1, \ldots, a_n) = t(b_1, \ldots, b_n)$. So assume that $a_i \equiv b_i \pmod{Z(G)}$. Then since

$$t(1, a_2, \ldots, a_{i-1}, a_i, b_{i+1}, \ldots, b_n) = 1 = t(1, a_2, \ldots, a_{i-1}, b_i, b_{i+1}, \ldots, b_n)$$

it follows that

$$t(a_1, a_2, \ldots, a_{i-1}, a_i, b_{i+1}, \ldots, b_n)\ [\theta_G, \theta_{Z(G)}]\ t(a_1, a_2, \ldots, a_{i-1}, b_i, b_{i+1}, \ldots, b_n).$$

But by Lemma 3.1 (4) the relation $[\theta_G, \theta_{Z(G)}] = \theta_{[G, Z(G)]} = \theta_{\{1\}}$ is the equality relation, so we are done. $\square$

**Theorem 3.13.** *If $G$ is a nonabelian nilpotent group and $\mathcal{C}$ is a clone such that $\mathrm{Clo}(G) \subsetneq \mathcal{C} \subseteq \mathrm{Clo}(\mathbf{A}_4)$, then $\mathcal{C} \setminus \mathrm{Clo}(G)$ contains an operation $t$ of arity $\leq [G : Z(G)] - 1$ satisfying conditions (1)–(4) of Lemma 3.12. Hence $\mathrm{Clo}(G)$ is determined by the subgroups of $G^k$ for $k = |G|^{[G:Z(G)]-1}$.*

*Proof.* Let $c$ denote the nilpotence class of $G$. We have $c > 1$ since $G$ is nonabelian.

**Claim 3.14.** $c < [G : Z(G)] - 1$.

The nilpotence class of $G$ is $c > 1$, therefore the nilpotence class of $G/Z(G)$ is $c - 1$, which is $\leq \log_2([G : Z(G)]) - 1$ since $\log_2([G : Z(G)])$ is an upper bound on the length of the normal subgroup lattice of $G$ and the descending central series of a nonabelian nilpotent group cannot be a maximal chain in this lattice. (I.e., $G/[G, G]$ cannot have prime order.) Therefore $c \leq \log_2([G : Z(G)]) < [G : Z(G)] - 1$.

**Claim 3.15.** *If $t \in \mathcal{C}$ is a nonconstant operation that satisfies Lemma 3.12 (1) and has arity exceeding $c$, then $t \notin \mathrm{Clo}(G)$.*

We must show that if $t(x_1, \ldots, x_n) \in \mathrm{Clo}(G)$ satisfies Lemma 3.12 (1), and $n > c$, then $t$ is constant. By collecting commutators we may represent $t$ as

$$t(x_1, \ldots, x_n) = \left(\prod x_i^{e_i}\right)\left(\prod [x_i, x_j]^{f_{ij}}\right) \cdots \text{(higher weight commutators)} \cdots .$$

Lemma 3.12 (1) implies that $t[x_i/1] = 1$ for any $i$, so the commutator terms without $x_i$ can be omitted from this representation. Since this can be done for every $i$, we may assume that all variables appear in every commutator term in the representation. But since the number of variables exceeds $c$, this forces $t$ to be constant.

Now we prove the first statement in Theorem 3.13, which asserts the existence of an operation $t \in \mathcal{C} \setminus \mathrm{Clo}(G)$ of arity $\leq [G : Z(G)] - 1$ satisfying conditions (1)–(4) of Lemma 3.12. Choose $r_0 \in \mathcal{C} \setminus \mathrm{Clo}(G)$ of minimal arity. Perform the modifications of Lemma 3.12 to produce an operation $t \in \mathcal{C} \setminus \mathrm{Clo}(G)$ of the same arity satisfying (1) and (2). Since $t \in \mathrm{Clo}(\mathbf{A}_4)$, (3) and (4) will be satisfied as well. We argue next that the arity of $t$ is $\leq [G : Z(G)] - 1$.

Suppose that the arity of $t$ is greater than $[G : Z(G)] - 1$. Since $t \notin \mathrm{Clo}(G)$ it is not the constant operation with value 1, so there exist elements $a_i \in G$ such that $t(a_1, \ldots, a_n) \neq 1$. Let $T$ be a transversal in $G$ for $Z(G)$ which contains the element 1. Using Lemma 3.12 (4), replace each $a_i$ with the element $b_i \in T$ that belongs to the same coset of $Z(G)$. Then $t(b_1, \ldots, b_n) = t(a_1, \ldots, a_n) \neq 1$, so in particular we cannot have $b_i = 1$ for any $i$. This means that there are at most $|T| - 1 = [G : Z(G)] - 1$ distinct $b_i$'s. Since the arity of $t$ exceeds this number there must exist $i \neq j$ with $b_i = b_j$. We claim that $t(\mathbf{x})[x_j/x_i] \in \mathcal{C} \setminus \mathrm{Clo}(G)$, contradicting the minimality assumption concerning the arity of $t$. The operation $t(\mathbf{x})[x_j/x_i]$ belongs to $\mathcal{C}$ because it is obtained from $t$ by identifying two variables. It is nonconstant since the substitution $x_i = b_i$ for all $i \neq j$ into $t(\mathbf{x})[x_j/x_i]$ yields the value $t(b_1,\dots,b_n)\neq 1$ although any substitution where $x_i=1$ for some $i$ yields the value 1. The operation $t(\mathbf{x})[x_j/x_i]$ has arity one less than the arity of $t$, so this arity is $\geq [G:Z(G)]-1>c$ by Claim 3.14. Hence by Claim 3.15 the operation $t(\mathbf{x})[x_j/x_i]$ cannot belong to $\mathrm{Clo}(G)$. This completes the proof that $\mathcal{C}$ contains an operation $t$ of arity $\leq [G:Z(G)]-1$ satisfying conditions (1)–(4) of Lemma 3.12.

It is shown in Proposition 1.3 of [5] that the only $\ell$-ary operations on $G$ preserving the subgroups of $G^{|G|^\ell}$ are the term operations of $G$. Therefore, if $k=|G|^{[G:Z(G)]-1}$, then $\mathrm{Clo}(\mathbf{A}_k)$ and $\mathrm{Clo}(G)$ have the same $([G:Z(G)]-1)$-ary term operations. We showed above that if $\mathcal{C}\subseteq \mathrm{Clo}(\mathbf{A}_4)$, then $\mathcal{C}\setminus \mathrm{Clo}(G)$ is empty or contains an operation of arity $\leq [G:Z(G)]-1$. Since $|G|^{[G:Z(G)]-1}>4$ when $G$ is nonabelian and nilpotent, it follows that $\mathrm{Clo}(\mathbf{A}_k)\setminus\mathrm{Clo}(G)$ is empty when $k=|G|^{[G:Z(G)]-1}$. Therefore $\mathrm{Clo}(\mathbf{A}_k)=\mathrm{Clo}(G)$ when $k=|G|^{[G:Z(G)]-1}$. □

Now we consider the clone of the quaternion group $Q=\{1,-1,i,-i,j,-j,k,-k\}$.

**Theorem 3.16.** $\mathrm{Clo}(Q)$ *is determined by the subgroups of* $Q^5$.

*Proof.* From Theorem 3.13 we know that if $\mathcal{C}\subseteq \mathrm{Clo}(\mathbf{A}_4)$ is a clone on $Q$ properly containing $\mathrm{Clo}(Q)$, then $\mathcal{C}\setminus\mathrm{Clo}(Q)$ contains an operation of arity $[Q:Z(Q)]-1=3$ satisfying (1)–(4) of Lemma 3.12. This is a nonconstant ternary operation $t(x,y,z)$ such that

(1) $t(1,y,z)=t(x,1,z)=t(x,y,1)=1$,
(2) $t(x,x,z)=t(x,y,y)=1$,
(3) $t(Q,Q,Q)\subseteq [Q,Q]=\{1,-1\}$, and
(4) $t(a_1,a_2,a_3)=t(b_1,b_2,b_3)$ if $a_\ell\equiv b_\ell \pmod{Z(G)}$ for all $\ell$.

We will argue that if $t$ is a nonconstant ternary operation on $Q$ satisfying (1)–(4), then $t$ does not preserve the subgroups of $Q^5$.

If $t$ is nonconstant, it follows from (1) and (3) that there is a tuple $(a_1,a_2,a_3)$ such that $t(a_1,a_2,a_3)=-1$. From the properties (1)–(4) of $t$ we may assume (after reordering the variables of $t$, permuting the roles of $i,j$ and $k$, and changing $a_1,a_2$ and $a_3$ modulo $Z(G)$) that $(a_1,a_2,a_3)=(i,j,i)$ or $(i,j,k)$.

If $t(i,j,i)=-1$, then for $\mathbf{u}=(i,i,i,i,1),\mathbf{v}=(j,j,i,i,1)$ and $\mathbf{w}=(i,j,i,j,1)$ we have $t(\mathbf{u},\mathbf{v},\mathbf{w})=(-1,1,1,1,1)$. But $(-1,1,1,1,1)$ is not in the subgroup of $Q^5$ generated by $\{\mathbf{u},\mathbf{v},\mathbf{w}\}$, as one can verify. This shows that $t$ does not preserve some subgroup of $Q^5$ if $t(i,j,i)=-1$.

If instead $t(i,j,k)=-1$, then for $\mathbf{u}=(i,1,i,i,i),\mathbf{v}=(j,j,j,1,i)$ and $\mathbf{w}=(k,k,1,k,i)$ we have $t(\mathbf{u},\mathbf{v},\mathbf{w})=(-1,1,1,1,1)$. Again $(-1,1,1,1,1)$ is not in the subgroup of $Q^5$ generated by $\{\mathbf{u},\mathbf{v},\mathbf{w}\}$. This shows that $t$ does not preserve some subgroup of $Q^5$ if $t(i,j,k)=-1$.

Altogether we have shown that if $\mathcal{C}\subseteq\mathrm{Clo}(\mathbf{A}_4)$ is a clone properly containing $\mathrm{Clo}(Q)$, then $\mathcal{C}$ contains an operation that fails to preserve some subgroup of $Q^5$. Hence $\mathrm{Clo}(\mathbf{A}_5)=\mathrm{Clo}(Q)$. □

**Theorem 3.17.** $\mathrm{Clo}(Q)$ *is not determined by the subgroups of* $Q^3$.

*Proof.* In fact, $\mathrm{Clo}(Q)$ is not determined by the subgroups of $Q^4$. The proof for exponent 4 is like the proof for exponent 3 but much longer and is omitted. Both arguments show by examining all cases that the operation

$$t(x,y,z) = \begin{cases} -1, & \text{if } [x,y]=[y,z]=[x,z]=-1; \\ 1, & \text{otherwise} \end{cases}$$

preserves all subgroups of $Q^3$ (or $Q^4$). It is clear that this operation is not in $\mathrm{Clo}(Q)$, since it is a nonconstant operation on $Q$ satisfying properties (1)–(4) from the proof of Theorem 3.16. To prove that $t$ preserves the subgroups of $Q^3$, we must show that if $\mathbf{a},\mathbf{b},\mathbf{c}\in Q^3$, then $t(\mathbf{a},\mathbf{b},\mathbf{c})\in\langle \mathbf{a},\mathbf{b},\mathbf{c}\rangle$.

Since $t(Q,Q,Q)\subseteq\{1,-1\}$, the element $t(\mathbf{a},\mathbf{b},\mathbf{c})$ may be assumed (after permuting coordinates in $Q^3$ if necessary) to be $(1,1,1),(-1,1,1),(-1,-1,1)$ or $(-1,-1,-1)$.

**Case 1.** $t(\mathbf{a},\mathbf{b},\mathbf{c})=(-1,-1,-1)$.

If $\mathbf{a}=(a_1,a_2,a_3),\mathbf{b}=(b_1,b_2,b_3),\mathbf{c}=(c_1,c_2,c_3)$ and $t(\mathbf{a},\mathbf{b},\mathbf{c})=(-1,-1,-1)$, then $a_\ell,b_\ell,c_\ell\in\{\pm i,\pm j,\pm k\}$ for all $\ell$. In this circumstance, $t(\mathbf{a},\mathbf{b},\mathbf{c})=(-1,-1,-1)=\mathbf{a}^2\in\langle \mathbf{a},\mathbf{b},\mathbf{c}\rangle$.

**Case 2.** $t(\mathbf{a},\mathbf{b},\mathbf{c})=(-1,-1,1)$.

In this case, $[a_\ell,b_\ell]=[a_\ell,c_\ell]=[b_\ell,c_\ell]=-1$ for $\ell=1$ or 2. For $\ell=3$ we must have either $[a_3,b_3]=1$, or $[a_3,c_3]=1$, or $[b_3,c_3]=1$. If $[a_3,b_3]=1$, then $t(\mathbf{a},\mathbf{b},\mathbf{c})=(-1,-1,1)=[\mathbf{a},\mathbf{b}]\in\langle \mathbf{a},\mathbf{b},\mathbf{c}\rangle$, and the cases $[a_3,c_3]=1$ and $[b_3,c_3]=1$ can be handled similarly.

**Case 3.** $t(\mathbf{a},\mathbf{b},\mathbf{c})=(-1,1,1)$.

Here we have $[a_\ell,b_\ell]=[a_\ell,c_\ell]=[b_\ell,c_\ell]=-1$ when $\ell=1$. We do not have all three equalities when $\ell=2$ (or 3), so after relabeling we may assume that $[a_2,b_2]=1$. If now $[a_3,b_3]=1$, then $t(\mathbf{a},\mathbf{b},\mathbf{c})=(-1,1,1)=[\mathbf{a},\mathbf{b}]\in\langle \mathbf{a},\mathbf{b},\mathbf{c}\rangle$ and we are done. We may assume henceforth that $[a_3,b_3]=-1$, in which case $(-1,1,-1)=[\mathbf{a},\mathbf{b}]\in\langle \mathbf{a},\mathbf{b},\mathbf{c}\rangle$.

Since $[a_3,b_3]=-1$, then we must have either $[a_3,c_3]=1$ or $[b_3,c_3]=1$. After relabeling again we may assume that $[b_3,c_3]=1$. If $[b_2,c_2]=1$ also, then $(-1,1,1)=[\mathbf{b},\mathbf{c}]\in\langle \mathbf{a},\mathbf{b},\mathbf{c}\rangle$ and we are done. Therefore assume henceforth that $[b_2,c_2]=-1$, in which case $(-1,-1,1)=[\mathbf{b},\mathbf{c}]\in\langle \mathbf{a},\mathbf{b},\mathbf{c}\rangle$.

Finally, our assumptions that $-1=[a_1,b_1]=[b_2,c_2]=[a_3,b_3]$ imply that $b_1,b_2,b_3\in\{\pm i,\pm j,\pm k\}$. Therefore $\mathbf{b}^2=(-1,-1,-1)\in\langle \mathbf{a},\mathbf{b},\mathbf{c}\rangle$. Now that we know $(-1,1,-1),(-1,-1,1),(-1,-1,-1)\in\langle \mathbf{a},\mathbf{b},\mathbf{c}\rangle$ we may conclude that $(-1,1,1)=(-1,1,-1)\cdot(-1,-1,1)\cdot(-1,-1,-1)\in\langle \mathbf{a},\mathbf{b},\mathbf{c}\rangle$.

**Case 4.** $t(\mathbf{a},\mathbf{b},\mathbf{c})=(1,1,1)$.

$t(\mathbf{a},\mathbf{b},\mathbf{c})=(1,1,1)\in\langle \mathbf{a},\mathbf{b},\mathbf{c}\rangle$ since $(1,1,1)$ belongs to every subgroup of $Q^3$. □

We conclude with a final problem. Although the clone of a finite group $G$ is not determined by the subgroups of $G^3$ in general, it may be that the third power is sufficient to distinguish the clone of one group from the clone of another group on the same set.

**Problem 3.18.** Suppose that $G$ and $H$ are groups defined on the same set. Show that $\mathrm{Sub}(G^3) = \mathrm{Sub}(H^3)$ implies $\mathrm{Clo}(G) = \mathrm{Clo}(H)$.

## References

[1] R. Freese and R. McKenzie, *Residually small varieties with modular congruence lattices*, Trans. Amer. Math. Soc. **264** (1981), no. 2, 419–430.
[2] R. Freese and R. McKenzie, *Commutator Theory for Congruence Modular Varieties*, London Mathematical Society Lecture Note Series **125**, Cambridge University Press, Cambridge, 1987.
[3] K. A. Kearnes and Á. Szendrei, *Groups with Identical Subgroup Lattices in all Powers*, J. Group Theory (to appear).
[4] R. Schmidt, *Subgroup lattices of groups*, de Gruyter Expositions in Mathematics, vol. 14, Walter de Gruyter & Co., Berlin, 1994.
[5] Á. Szendrei, *Clones in Universal Algebra*, Séminaire de Mathématiques Supérieures, vol. 99, Les Presses de l'Université de Montréal, Montréal, 1986.

(Keith Kearnes) Department of Mathematics, University of Colorado, Boulder, CO 80309-0395, U.S.A.
*E-mail address*: `Keith.Kearnes@Colorado.EDU`

(Ágnes Szendrei) Bolyai Institute, University of Szeged, Aradi vértanúk tere 1, H–6720 Szeged, Hungary, and Department of Mathematics, University of Colorado, Boulder, CO 80309-0395, U.S.A.
*E-mail address*: `a.szendrei@math.u-szeged.hu, szendrei@euclid.colorado.edu`