STRONG DUALITY FOR METACYCLIC GROUPS

R. QUACKENBUSH and CS. SZABÓ

(Received 1 February 1999; revised 13 October 2001)

Communicated by B. Davey

Abstract

Davey and Quackenbush proved a strong duality for each dihedral group $D_m$ with $m$ odd. In this paper we extend this to a strong duality for each finite group with cyclic Sylow subgroups (such groups are known to be metacyclic).

2000 Mathematics subject classification: primary 20D10; secondary 08A05.

Keywords and phrases: metacyclic group, duality.

1. Introduction

The first strong natural duality for nonabelian groups was established by Davey and Quackenbush, see [2]. They showed that the dihedral group $D_m$ admits a strong natural duality if $m$ is odd. In this paper we generalize this result to finite groups having all Sylow subgroups cyclic. We assume that the reader is familiar with [2]. The definition of a (natural) duality is given in [1, 2]; here we give it for the special case of finite groups:

Let $G = \langle G, \cdot \rangle$ be a finite group. We call $\hat{G} = \langle G; F, P, R, \tau \rangle$ a (topological) dual structure on the same set $G$, if

(a) each $f \in F$ is a group homomorphism $f : G^n \to G$ for some $n \in \mathbb{N}$,
(b) each $f \in P$ is a group homomorphism $f : \text{dom}(f) \to G$, where $\text{dom}(f)$ is a subgroup of $G^n$ for some $n \in \mathbb{N}$,
(c) each $r \in R$ is a subgroup of $G^n$ for some $n \in \mathbb{N}$,
(d) $\tau$ is the discrete topology.

The research of the authors was supported by a grant from the NSERC of Canada. The second author was also supported by grant F023436 from the Hungarian National Science Research Foundation.

© 2002 Australian Mathematical Society 1446-8107/2000 $A2.00 + 0.00$

377
The elements of $F$, $P$ and $R$ are called operations, partial operations and relations, respectively, and we say that the structure $\hat{G}$ is algebraic over $G$. One consequence of this definition is that every $n$-ary group word is a continuous homomorphism from $\hat{G}^n$ to $\hat{G}$.

Also as a consequence of this definition we have that for each group $A$ in the quasi-variety $\mathbb{S}^{\mathbb{P}(G)}$, the set of homomorphisms from $A$ to $G$, denoted $X_A := \text{Hom}(A, G)$, is a closed substructure of $\hat{G}^{|A|}$ and for each $\tilde{X}$ in the topological quasivariety $\mathbb{S}_{c}^{\mathbb{P}(\hat{G})}$, the set of continuous homomorphisms from $\tilde{X}$ to $\hat{G}$, denoted $\tilde{A}_\tilde{X} := \text{Hom}(\tilde{X}, \hat{G})$, is a subgroup of $G^{\tilde{X}}$. Moreover, for each group $A \in \mathbb{S}^{\mathbb{P}(G)}$ there is a natural isomorphism $\hat{G}$ yields a (natural) duality for $\mathbb{S}^{\mathbb{P}(G)}$. If the analogous map $\epsilon_\tilde{X}$ also is an isomorphism for each $\tilde{X} \in \mathbb{S}_{c}^{\mathbb{P}(\hat{G})}$, then we say that $\hat{G}$ yields a full duality for $\mathbb{S}^{\mathbb{P}(G)}$.

For instance, if $G = \mathbb{Z}_m = \langle \mathbb{Z}_m; + \rangle$ and $\tilde{G}_m = \langle \mathbb{Z}_m; +, \tau \rangle$ with $F = \{+\}$, $P = \emptyset = R$, then $\tilde{G}_m$ yields a full duality for $\mathbb{S}^{\mathbb{P}(\mathbb{Z}_m)}$, which in this case is the variety of abelian groups satisfying $mx = 0$; this is a fragment of the usual Pontryagin duality for all abelian groups.

Duality theory tells us that in order to show that $\hat{G}$ yields a full duality on $\mathbb{S}^{\mathbb{P}(G)}$ it is enough to prove the following three conditions:

CLO: for each $n \in \mathbb{N}$, every continuous homomorphism $\phi: \hat{G}^n \to \hat{G}$ is a group word on $G$.

INJ: $\hat{G}$ is injective in $\mathbb{S}^{\mathbb{P}(\hat{G})}$.

STR: for any $\tilde{X} \leq \hat{G}^I$ where $I \neq \emptyset$, and for each $y \in \hat{G}^I \setminus \tilde{X}$ there exists a continuous homomorphism $\phi: \hat{G}^I \to \hat{G}$ such that $\phi|_{\tilde{X}} = 1$ while $\phi(y) \neq 1$.

When these three conditions are satisfied we call this a strong duality; thus, a strong duality is a full duality. All known full dualities are actually strong dualities. It has long been conjectured that a full duality is always strong, but this remains an open, challenging problem. We shall exhibit a strong duality for groups having cyclic Sylow subgroups.

2. Preliminary results

For the main goal of the paper we need some structure theorems for groups. The first is from Robinson, [5, page 281].

**Theorem 2.1** (Hölder, Burnside, Zassenhaus). A finite group $G$ has all its Sylow subgroups cyclic if and only if it has a representation $\mathbb{Z}_m \times \mathbb{Z}_n$ such that $(m, n) = 1$; thus, it is metacyclic.
Let $n = p_1^{a_1} \cdots p_k^{a_k}$ so that $Z_n \cong Z_{p_1^{a_1}} \times \cdots \times Z_{p_k^{a_k}}$ and $\text{Aut}(Z_n) \cong \text{Aut}(Z_{p_1^{a_1}}) \times \cdots \times \text{Aut}(Z_{p_k^{a_k}})$. Then the semidirect product $Z_n \rtimes H$ is determined by a homomorphism $\rho = (\rho_1, \ldots, \rho_k)$ from $H$ into $\text{Aut}(Z_n)$, where $\rho_i$ is the corresponding homomorphism from $H$ into $\text{Aut}(Z_{p_i^{a_i}})$ and $Z_{p_i^{a_i}} \rtimes H$ is the corresponding semidirect product. The next theorem tells us how to build recursively a strong duality for $Z_n \rtimes H$ from those for the $Z_{p_i^{a_i}} \rtimes H$. As often happens in a recursive construction, we need to assume and prove something a bit stronger in order to prove that the recursive construction is correct.

A strong duality for $K = G \rtimes H$ will be called \textit{semidirect} over $H$ if the following condition holds: let $\tilde{X}$ be a closed substructure of $(\tilde{K})^t$, $\phi: \tilde{X} \to \tilde{K}$ a continuous structure preserving map and $\phi': (\tilde{H})^t \to \tilde{K}$ a continuous structure preserving map extending the restriction of $\phi$ to $(\tilde{H})^t$; then there is a continuous structure preserving map $\psi: (\tilde{K})^t \to \tilde{K}$ extending both $\phi$ and $\phi'$.

Now and later in the paper, we make use of the following group theoretic lemma from [2].

\textbf{Lemma 2.2.} Let $G$ be a group and let $\varepsilon$ be a retraction of $G$ onto a subgroup $H$. Let $\mathcal{N}$ be the kernel of $\varepsilon$ and let

$$K := \{(u, v) \in G^2 \mid \varepsilon(u) = \varepsilon(v)\} = \bigcup\{(\varepsilon^{-1}(h))^2 \mid h \in H\} = \bigcup\{Nh \times Nh \mid h \in H\}$$

be the congruence corresponding to $\mathcal{N}$. Define a partial binary operation $\ast$, with domain $K$, by $xh \ast yh := xyh$ for all $x, y \in N$ and $h \in H$ (that is, define $u \ast v := u \varepsilon(u)^{-1} v = u \varepsilon(v)^{-1} v$ for all $(u, v) \in K$).

(a) (The restriction of) $\ast$ is a well-defined group operation on $Nh$ for each $h \in H$. Moreover, right translation by $h$ is an isomorphism of $\langle N; \varepsilon \rangle$ onto $\langle Nh; \ast \rangle$.

(b) The partial operation $\ast$ is associative wherever it is defined. It will be commutative wherever it is defined provided $\mathcal{N}$ is abelian.

(c) The map $\ast: K \to G$ is a homomorphism if and only if $\mathcal{N}$ is abelian.

\textbf{Theorem 2.3.} Let $G_1, G_2, H$ be finite groups with $G_1, G_2$ abelian, such that their sizes are pairwise relatively prime. If $K_i = G_i \rtimes H$ (given by $\rho_i: H \to \text{Aut}(G_i)$) each admits a strong duality, then a strong duality holds for $G = (G_1 \times G_2) \rtimes H$ (given by $(\rho_1, \rho_2): H \to \text{Aut}(G_1) \times \text{Aut}(G_2)$).

\textbf{Proof.} Let $\varepsilon_i$ denote the retractions of $G$ to $K_i$ by $G_j$ for $(i, j) \in \{(1, 2), (2, 1), (1, 1), (2, 2)\}$, $\varepsilon$ the retraction of $G$ to $H$ by $G_1 \times G_2$. Let $\tilde{K}_i = (K_i; F_i, P_i, R_i, \tau)$ yield a strong duality for $\text{SPP}(K_i)$. Let $s_i(n) = q_i(n)r_i(n)$ be the size of the $n$-generated free group, $F_i(n)$, in the variety generated by $K_i$, where $(q_i(n), |G_i|) = (r_i(n), |H|) = 1$. Also,
let * be the partial operation given by the translation of the group operation on \(G_1 \times G_2\) as given by Lemma 2.2. We take

\[ \tilde{G} = \langle \epsilon_1, \epsilon_2, F_1 \cup F_2 \cup P_1 \cup P_2 \cup \{\ast\}, R_1 \cup R_2, \tau \rangle; \]

note that full operations on \(G_i\) become partial operations on \(G\). Also note that \(\epsilon_1 \epsilon_2 = \epsilon_2 \epsilon_1 = \epsilon\). We will use the fact that \(\epsilon_i|_{K_{1-i}}\) is the retraction of \(K_{1-i}\) onto \(H\) by \(G_i\). Because of our assumption of strong dualities, we may assume that \(\epsilon_i|_{K_{1-i}}\) is part of the duality for \(K_{1-i}\).

Let \(g \in G^i\) for \(i\) finite or infinite, and let \(\phi: \tilde{G}^i \to \tilde{G}\) be a continuous homomorphism. Then we have \(g = \underline{g} \ast \underline{h} \ast \underline{g} \ast \underline{h}^\prime\) with \(\underline{g} \in G^i\) and \(\underline{h} \in H^i\). Then \(\epsilon_i(\underline{g}) = \underline{g} \ast \underline{h}\). Since \(\underline{g} = \underline{g} \ast \underline{g} \ast \underline{h} \ast \underline{g} \ast \underline{h}^\prime\), \(\phi\) preserves \(*\).

That is, \(\phi(g) = \phi(\underline{g} \ast \underline{h}) = \phi(\underline{g} \ast \underline{h}) = \phi(\epsilon_1(\underline{g})) \ast \phi(\epsilon_2(\underline{g})).\)

First we show that \(\text{CLO}\) holds. Due to the semidirect products involved, each \(F_i(n)\) is itself a semidirect product of a normal subgroup \(N_i(n)\) and \(F_H(n)\), the \(n\)-generated free group over \(H\). Moreover, \((|N_i(n)|, |F_H(n)|) = 1\). That is to say, \(q_i(n) = q_2(n) := 2(n)\) for all \(n \geq 0\). As each \(K_i\) is a quotient of \(G\), we have \(|F_i(n)| \geq q(n)r_i(n)r_2(n)\). We show that equality holds, as does \(\text{CLO}\), by showing that there are at most \(q(n)r_1(n)r_2(n)\) continuous homomorphisms \(\phi: \tilde{G}^n \to \tilde{G}\). Since \(\phi\) preserves \(\{\epsilon, \epsilon_1, \epsilon_2\}\), \(\phi\) maps \(K^\mu_i\) to \(K_i\) and \(H^\mu_i\) to \(H_i\). In view of the strong dualities assumed for each \(K_i\), there are at most \(q(n)r_i(n)r_2(n)\) restrictions of \(\phi\) to \(K^\mu_i \cup K^\mu_2\); we must show that this restriction has at most one extension to all of \(G^\mu\). But that was done in the last paragraph.

In order to prove \(\text{INJ}\) and that the duality will be semidirect over \(H\), let \(X \subseteq \tilde{G}^i\) be a closed substructure for some set \(I\) and \(\phi: \tilde{X} \to \tilde{G}\) a continuous homomorphism. Since \(\phi\) preserves the retractions, \(\phi|_{K^\mu_i}\) is a continuous homomorphism from \(\tilde{X} \cap \tilde{K}^\mu_i\) to \(\tilde{K}^\mu_i\). Since \(\text{INJ}\) holds for \(\tilde{K}^\mu_i\) and the dualities are semidirect over \(H\), we proceed as follows: let \(\psi_0\) be an extension of \(\phi|_{H^\mu_i}\) to \(\tilde{H}^\mu_i\) and \(\psi_i\) an extension of \(\phi|_{K^\mu_i}\) to \(\tilde{K}^\mu_i\) for \(i = 1, 2\), and note that \(\psi_0|_{H^\mu_i} = \psi_2|_{H^\mu_i}\). Let \(g \in G^\mu_i\) where \(g = \underline{g} \ast \underline{h} \ast \underline{g} \ast \underline{h}^\prime\) with \(\underline{g} \in G^\mu_i\) and \(\underline{h} \in H^\mu_i\). From what we have seen above, we must define \(\psi\) by \(\psi(g) := \psi_1(\epsilon_1(\underline{g})) \ast \psi_2(\epsilon_2(\underline{g}))\). If \(g \in \tilde{X}\), then \(\psi(\epsilon_i(\underline{g})) = \phi(\epsilon_i(\underline{g}))\), so that \(\psi\) extends \(\phi\); obviously, \(\psi\) extends \(\psi_0\). Since \(\psi_i|_{K^\mu_i}\) is a homomorphism, to show that \(\psi\) is a homomorphism, it is enough to show that \(\psi\) preserves \(\epsilon_i\). Let \(g = \underline{g} \ast \underline{h} \ast \underline{g} \ast \underline{h}^\prime\). On the one hand,

\[ \psi(\epsilon_1(\underline{g})) = \psi_1(\epsilon_1(\epsilon_1(\underline{g}))) \ast \psi_2(\epsilon_2(\epsilon_1(\underline{g}))) = \psi_1(\underline{g} \ast \underline{h} \ast \underline{g} \ast \underline{h}^\prime). \]

On the other hand,

\[ \epsilon_1(\psi(\underline{g})) = \epsilon_1(\psi_1(\underline{g} \ast \underline{h} \ast \underline{g} \ast \underline{h}^\prime)). \]
Let $\psi_1(g, h) = g_1 h$ and $\psi_2(g, h) = g_2 h'$ where $g_i \in G_i$ and $h, h' \in H$. In order for $g_1 h \ast g_2 h'$ to be defined, we need to show that $h = h'$. We do this by showing that $\psi_1(h) = h$ and $\psi_2(h) = h'$; since $\psi_1(h) = \psi_2(h)$, the result follows. Using the fact that $\varepsilon_2$ commutes with $\psi_1$, we have

$$h = \varepsilon_2(g, h) = \varepsilon_2(\psi_1(g, h)) = \psi_1(\varepsilon_2(g, h)) = \psi_1(h).$$

Similarly, $\psi_2(h) = h'$. Then,

$$\varepsilon_1(\psi_1(g, h) \ast \psi_2(g, h)) = \varepsilon_1(g_1 h \ast g_2 h) = \varepsilon_1(g_1 g_2 h) = g_1 h.$$

Finally, $g, h = g_1 h \ast h = \psi_1(g, h) \ast \psi_2(h)$, showing that $\psi$ preserves $\varepsilon_1$. In a similar manner it preserves $\varepsilon_2$ and so it is a homomorphism.

To complete the proof of $\text{INJ}$ we need to prove that $\psi$ is continuous. By construction, both $\psi_1$ and $\psi_2$ are continuous. Using the same finite subset of $I$ given by the continuity of $\psi_i$, it is straightforward to prove the continuity of $\psi_1 \circ \varepsilon_i$. Note that $\ast$ is continuous because it has finite domain. Thus, $\psi$ is a composition of continuous maps and so it is continuous. Moreover, we have shown that the duality is semidirect over $H$.

To show $\text{STR}$ we first note that restricted to $K_1^f$, $\text{STR}$ holds. Also recall that $\phi$ is defined on $g \in G^f$ if and only if it is defined on $\varepsilon_i(g) \in K_i^f$ for $i = 1, 2$. Let $\tilde{X} \leq \tilde{G}^f$ be a closed substructure and $\gamma \in G^f - X$ for some set $I \neq \emptyset$; we define $\phi(\gamma) := 1$ for all $\gamma \in X$. Then, without loss of generality, we may assume that either $\gamma \in H^f$ or $\varepsilon_1(\gamma) \notin \varepsilon_1(X)$; in either case, $\varepsilon_1(\gamma) \notin \varepsilon_1(X)$. Now we invoke $\text{STR}$ for $K_i^f$ with respect to $\varepsilon_1(\gamma)$ and proceed as in the proof of $\text{INJ}$ for $\tilde{G}^f$, and we are done. We leave to the reader the verification that the value of this extension at $\gamma$ is not 1.

3. The case $n = p^g$

Thus, we can build up our strong duality for finite metacyclic groups from that for metacyclic groups of the form $G = Z_{p^g} \times Z_m$, where $(p, m) = 1$. In this section we show that there is a strong duality semidirect over $Z_m$ for these groups. We assume that $G$ is not abelian.

Let $Z_{p^g} = \langle a \rangle$, $Z_m = \langle b \rangle$ and $a^y \equiv bab^{-1} = a^k$ for some $k \in \mathbb{N}$. Let $\gamma \in \text{Aut}(Z_{p^g})$ be such that $\gamma(a) = a^b$ and let the order of $\gamma$ be $d$ (this means that $ba = a^k b$ and that $a = \gamma^d(a) = a^{k^d}$, so that $p^d | (k^d - 1)$). As $G$ is not abelian, $d > 1$; for the same reason, $p > 2$, and so $\text{Aut}(Z_{p^g}) \cong Z_{p^d - 1}(p - 1)$. On the one hand, as there is a group homomorphism from $Z_m$ to $\text{Aut}(Z_{p^g})$ sending $b$ to $\gamma$, $d|m$ and so $(d, p) = 1$. On the other hand, as $d | p^d - 1(p - 1)$ and $(d, p) = 1$, we have that $d | (p - 1)$. Thus,
b^d a = a^d b^d = ab^d and so \((b^d)\) is in the center of \(G\). Let us suppose that \(ab^j = b^j/a\). Then \(a = (a)^b = a^{k^j}\); hence, \(\gamma^j(a) = a\) and so \(d\) divides \(j\). Thus,

\[
C_G(a^d) = \langle a, b^d \rangle, \quad C_G(b^j) = \langle b \rangle \text{ if } d \nmid j, \\
C_G(b^j) = G \text{ if } d \mid j, \quad Z(G) = \langle b^j \rangle.
\]

When \(Z(G) \neq 1\) (that is, \(d < m\)), there are some complications. For instance, consider the case \(p^6 = 3, m = 4\) and \(a^d = a^{-1}\). In this 12-element group we have \(Z(G) = \langle b^j \rangle\) and \(G/Z(G) \cong S_3\). But \(S_3\) is not in the quasivariety generated by \(G\) (as \(S_3\) is monolithic but not a subgroup of \(G\)). Thus, the quasivariety generated by \(G\) is not the variety generated by \(G\). However, the variety generated by \(G\) is the quasivariety generated by \(Z_4 \times S_3\), see Olshanskii [3]. In general, the variety generated by \(G = Z_{p^6} \rtimes Z_{m}\) is the quasivariety generated by

\[
Z_m \times (G/Z(G)) \cong Z_m \times (Z_{p^6} \rtimes (Z_m/Z(G))) \cong Z_m \times (Z_{p^6} \rtimes Z_d).
\]

In case \(Z(G) \neq 1\), we will need to work ‘over the center’ by using the following partial operation.

**Lemma 3.1.** The mapping \(\star \colon G \times Z(G) \to G\) such that \(g \star c = gc\) is a group homomorphism.

We shall show that \(\mathcal{S}_G, \mathcal{P}(\tilde{G})\) is a dual quasivariety of \(\mathcal{ISP}(G)\), where

\[
\tilde{G} = \langle G; 1, \alpha, +, \ast, \circ, \tau \rangle.
\]

Here, \(1\) is the constant operation and \(\alpha\) is the automorphism of \(G\) fixing \(a\) and mapping \(b\) to \(ab\) (we omit the routine but ugly computation that shows that such an \(\alpha\) exists). The four operations \(+\), \(\ast\), \(\circ\), \(\tau\) are each obtained from the restriction of the group operation \(\cdot\) to certain subgroups of \(G^2\); each operation is a homomorphism. Thus, \(+\) is the restriction of the group operation \(\cdot\) to the abelian group \(Z_m = \langle b \rangle\). Next, \(\ast\) is the binary partial operation obtained via Lemma 2.2 from \(Z_{p^6}\) and \(Z_m\). More precisely, the domain of \(\ast\) is \(\bigcup_{n=0}^{p^6-1} (Z_{p^6}b^{j^n} \times Z_{p^6}b^{j^n})\), and the operation is the translation of the group multiplication: \(a^{2j^n} \ast a^{2j^n}b^{j^n} = a^{2j^n}b^{j^n}\). By Lemma 2.2, \(\ast\) is an algebraic binary partial operation. Let \(\varepsilon : G \to Z_m\) where \(\varepsilon(a^{2j^n}) = b^{j^n}\) is the retraction of \(G\) onto \(Z_m\) by \(Z_{p^6} = \langle a \rangle\). Note that if a map preserves \(\ast\) then it automatically preserves \(\varepsilon\), since \(\varepsilon(a^{2j^n}) = a^{2j^n} \ast a^{-1}b^{j^n}\) and \(a^{-1}b^{j^n}\) is generated from \(a^{2j^n}\) by \(\ast\). The binary partial operation \(\circ\) is the restriction of the group operation \(\cdot\) to the abelian group \(Z_{p^6} \times Z(G)\). Finally, the binary partial operation \(\ast\) is as given by Lemma 3.1. As always, \(\tau\) is the discrete topology.

First we show that the condition CLO holds.
LEMMA 3.2. \(|\text{Hom}(\tilde{G}^n, \tilde{G})| \leq m^n(p^\beta)^{(d^* - 1)(n - 1) + n}\).

PROOF. The proof is essentially the same as that of Proposition 4 of [2]. Let \(\phi \in \text{Hom}(\tilde{G}^n, \tilde{G})\). Since + is the original group operation on \(\mathbb{Z}_m\), and \(\phi\) preserves +, the restriction, \(\phi|_{\mathbb{Z}_m^\nu}\), is an abelian group homomorphism into \(\mathbb{Z}_m\). There are \(m^n\) such homomorphisms. Next, we examine the possible extensions of each such homomorphism. Let \(h = (h_1, \ldots, h_n) \in (\mathbb{Z}_m)^n\) and \(\epsilon^{-1}(h) = \mathbb{Z}_m h_1 \times \cdots \times \mathbb{Z}_m h_n = S_h\). \(S_h\) is an abelian group isomorphic to \((\mathbb{Z}_m)^n\) under the operation \(*\) with \(h\) as its identity element. \(S_h\) must be mapped into \(\epsilon^{-1}(\phi(h))\) which under \(*\) is isomorphic to a subgroup of \(\mathbb{Z}_m\), and \(\phi|_{S_h}\) must be an abelian group homomorphism from \(\langle S_h, * \rangle\) to its image. Since \(\phi\) preserves \(\alpha\), it is already defined on \(\alpha(h)\), hence on \(\langle \alpha(h), * \rangle\) which is a subgroup of size \(p^\beta\) of \(\langle S_h, * \rangle\) if \(h \neq 1\), and is \(|h|\) if \(h = 1\). So there are at most \((p^\beta)^{n-1}\) extensions to \(S_h\) if \(h \neq 1\) and at most \((p^\beta)^n\) if \(h = 1\). Finally, let \(h' \in (\mathbb{Z}_m)^n\) be such that \(h^{-1}h' = (Z(G))^n\). Then because of \(*\), if we know \(\phi\) on \(S_h\), then we know \(\phi\) on \(S_{h'}\). Since \(|\mathbb{Z}_m/Z(G)| = d\), the number of continuous homomorphisms from \(\tilde{G}^n\) to \(\tilde{G}\) is not more than \(m^n(p^\beta)^{(d^* - 1)(n - 1) + n}\). \(\square\)

In [2], the proof is completed by a reference to the known result that this upper bound is the size of the \(n\)-generated free group in the variety generated by the given group. In the present case, we do not have such a formula at hand. However, since every word is a continuous homomorphism, we only need to construct an \(n\)-generated group of the appropriate size in the variety generated by \(G\). One of the referees of an earlier version of this paper gave an alternate proof by showing that the variety generated by \(G\) is the product variety \(\mathcal{V}_{p,\mathcal{V}}\), whose free spectrum is known. The proof we give here is more elementary and has the advantage that it is a more general approach to producing dualities – one ‘merely’ constructs sufficiently large \(n\)-generated algebras.

LEMMA 3.3. Let \(a \in \langle a \rangle^d\) and \(g \in G^d\) be such that if \(\langle g \rangle_t = b^i a^t\), then \(0 \leq t \leq d - 1\). Then for every \(0 \leq t \leq d - 1\) the group generated by \(a\) and \(g\) contains a vector \(\underline{a}\) such that \(\langle a \rangle_t = \langle a \rangle_{t'}\) if \(\langle a \rangle_t = b^i a^t\) and \(\langle a \rangle_{t'} = b^i a^{t'}\) otherwise.

PROOF. Consider \(a = (a^{u_1}, \ldots, a^{u_s})\) and \(g = (b^i a^{v_1}, \ldots, b^i a^{v_s})\). Without loss of generality, we may assume that \(i_u \neq i_v\) for \(u, v \leq s\) and that for \(v > s\) there is \(u \leq s\) with \(i_u = i_v\). Form the \(s \times s\) matrix whose \((u, v)\) component is the exponent of \(a\) in the \(v\)-th component of \(a^{u_v}\). Then this matrix is a constant multiple of the Vandermonde-matrix \(V = V(k^{v_1}, k^{v_2}, \ldots, k^{v_s})\), where the constant is

\[
\left(\prod_{j=1}^{q} u_j\right)^{k^{s} r_{k+1}^{v_1}}.
\]
Notice that this constant is not divisible by \( p \). The determinant of \( V \) is

\[
\det V = \prod_{0<j<d} (k^j - k^i).
\]

As \( k^i - k^j = k^i(k^{j-i} - 1) \) is coprime with \( p \), \( \det V \) is a unit in \( \mathbb{Z}_{p^d}^* \); hence, \( V \) is invertible and the vectors asserted by the lemma are expressible in the terms of the vectors \( \underline{a}^t \).

**Definition.** Let \( \underline{a} \in \langle a \rangle^k \) and \( \underline{g} \in \underline{G}^k \). The vectors created in the previous lemma are called the separation of \( \underline{a} \) by \( \underline{g} \) at the exponent \( t \).

**Example 1.** Let \( \underline{a} = (1, a, a^2, 1, a^3, a, a) \) and \( \underline{g} = (b, a, ba^2, b^3a, b, b^3a, b^3) \). Then \( \underline{g}_0 = (1, a, 1, 1, 1, 1, 1) \), \( \underline{g}_1 = (1, 1, a^2, 1, a^3, 1, 1) \), \( \underline{g}_3 = (1, 1, 1, 1, 1, a) \). It is clear that \( \underline{g} = \prod_{i=0}^{n-1} \underline{g}_i \), and \( \underline{g}_0 = (1, \ldots, 1) \) if \( t \) does not occur in \( \underline{g} \) as an exponent of \( a \) in some component.

We exhibit an \( n \)-generated subgroup \( \underline{D} \) of \( \underline{G}^{(d^n - 1)(n-1) + n} \) of the appropriate size. We define an \( n \)-by-\([(d^n - 1)(n-1) + n] \) matrix \( M \) with entries from \( \underline{G} \), and take the group generated by its rows. We define \( M \) by giving its columns. Take all the vectors \( \underline{b} \) from \( (b)^n \) such that if \( \langle \underline{b} \rangle_i = \underline{b}_r \), then \( 0 \leq r \leq d - 1 \). For each such \( \underline{b} \) take the vectors \( \underline{b}_i \) (\( 1 \leq i \leq n \)), that are the same as \( \underline{b} \) except that the \( i \)-th coordinate is multiplied by \( \underline{a} \) from the right. For each \( \underline{b} \) we omit the first \( \underline{b}_i \) which does not contain \( a \) as a coordinate. For example if \( \underline{b} = (1, 1, b, b^2, b^3, 1, b)^T \) we omit \( b_1 = (1, 1, ba, b^2, b^3, 1, ba)^T \). We get \( n \) vectors from \( (1, \ldots, 1)^T \) and \( n - 1 \) from each \( \underline{b} \neq (1, \ldots, 1)^T \). These vectors will be the columns of \( M \). Given an element \( \tilde{v} \in \underline{G}^{(d^n - 1)(n-1) + n} \), we will index the coordinates of \( \tilde{v} \) by the columns of \( M \).

**Definition.** \( \underline{b} \) is called the \( b \)-part of \( \tilde{b} \); a column of \( M \) distinct from \( \underline{b}_i \) but with the same \( b \)-part is called a \( b \)-mate of \( \underline{b}_i \). A row vector of length \( (d^n - 1)(n-1) + n \) with an \( a \) in coordinate \( \underline{b}_i \), and a \( 1 \) in all other coordinates is called the \( a \)-part of \( \underline{b}_i \).

**Lemma 3.4.** In the variety generated by \( \underline{G} \), there is an \( n \)-generated group of size at least \( m^n (p^d)^{(d^n - 1)(n-1) + n} \).

**Proof.** We show that \( \underline{D} \), the group generated by the rows of \( M \), is a group of the required size. We show that \( \underline{D} \) contains

1. a subgroup \( \underline{H}_1 \) of size \( (p^d)^{(d^n - 1)(n-1) + n} \),
2. a subgroup \( \underline{H}_2 \) of size \( m^n \).

Since the orders of \( \underline{H}_1 \) and \( \underline{H}_2 \) are coprime, the group generated by them has size at least \( m^n (p^d)^{(d^n - 1)(n-1) + n} \).
In order to show (1), let \( \bar{g} = (b^a, \ldots, b^c, a, \ldots, b^d) \) be a column of \( M, v \) the row of \( M \) with \( b^i \) entry in coordinate \( i \). First we construct a vector \( w' \in D \) having \( a \) as its \( \bar{g} \) coordinate, and 1 in all coordinates which are \( b \)-mates of \( \bar{g} \). Let \( w' = w \) if \( t_i = 0 \); notice that at a \( b \)-mate coordinate of \( \bar{g} \) the entry is 1. If \( t_i \neq 0 \), consider \( \bar{g} \) and its \( b \)-mates (in total, \( n-1 \) columns). Then by the construction of \( M \) there is a unique row \( \bar{u} \) which contains no \( a \) in any of these columns, but only a fixed power of \( b, b' \); this row corresponds to the first component of the \( b \)-part of \( \bar{g} \) which is not 1. If \( m \) does not divide \( r, t_i \), let \( w'' = \frac{w''_0}{m(r_i)} \). Then the \( \bar{g} \) coordinate of \( w'' \) is \( a^i \), where

\[
\zeta = \frac{k(r_i) - 1}{k(r_i) - 1},
\]

and the coordinate of every \( b \)-mate of \( \bar{g} \) is 1. Since \( m \) does not divide \( r, t_i \), \( p \) does not divide \( \zeta \) and so there is a \( u \in \mathbb{N} \) such that

\[
zu \equiv 1 \quad (\text{mod } p^\beta).
\]

Hence, \((a^i)^u = a\). Let \( w' = (w'')^u \). If \( m \) divides \( r, t_i \), then \( m \) does not divide \( r + t_i, t_i \); so let us use \( v \cdot w' \) instead of \( w' \) to construct \( w'' \) and \( w' \). The \( \bar{g} \) coordinate of \( w' \) is \( a \), and the coordinate of every \( b \)-mate of \( \bar{g} \) is 1.

We next construct \( w_0 \in D \cap \langle a \rangle^{(a-1)(a-1)n} \) with the same property. Since \((m, p) = 1\), there is an \( x \in \mathbb{N} \) such that

\[
x \equiv 1 \quad (\text{mod } p^\beta); \quad x \equiv 0 \quad (\text{mod } m).
\]

Let \( \bar{w}_0 = (w')^x \). Then \( \bar{w}_0 \in D \cap \langle a \rangle^{(a-1)(a-1)n} \) with \( a \) in its \( \bar{g} \) coordinate, and the coordinate of every \( b \)-mate of \( \bar{g} \) is 1.

Now we recursively construct the \( a \)-part of \( \bar{g} \). Suppose for \( \bar{h} \neq \bar{g} \) that \( (w_0)_{\bar{h}} \neq 1 \). Then the \( b \)-part of \( \bar{h} \) differs from the \( b \)-part of \( \bar{g} \), say at component \( j \). Look at \( \bar{w}_0 \), the separation of \( \bar{w}_0 \) by the \( j \)-th row of \( M \) at the exponent \( t_j \), where \( t_j \) is the \( j \)-th component of the \( b \)-part of \( \bar{g} \). Then \( (w_0)_{\bar{h}} = a \) and \( (w_0)_{\bar{h}} = 1 \). As separation preserves the entry 1, iteration eventually produces the \( a \)-part of \( \bar{g} \). Clearly, the set of all \( a \)-parts of the columns of \( M \) generates a group of the required size.

In order to show (2), express \( \varepsilon(w) \) with \( v \) and \( H_i \). These elements belong to \( \langle b \rangle^{(a-1)(a-1)n} \) and clearly generate a group \( H_2 \) of order \( m^n \).

Now we have everything to show that \( \text{CLO} \) holds:

**Theorem 3.5.** Each continuous homomorphism from \( \bar{G}^n \) to \( \bar{G} \) is a word.

**Proof.** By construction, each word is a continuous homomorphism. But by Lemma 3.2 and Lemma 3.4, there are at most as many continuous homomorphisms as there are words. \( \square \)
Corollary 3.6. The size of the \( n \)-generated free group in the variety generated by \( G \) is \( m^t(p^t)^{(a^t-1)\alpha - 1 + \eta} \) and the \( n \)-generated free group is a semidirect product:
\[
(Z_{\mu^t})^{(a^t-1)\alpha - 1 + \eta} \rtimes \mathbb{Z}_m.
\]

Let us now try to prove \( \text{INJ} \) and \( \text{STR} \) and show that the duality is semidirect over \( \mathbb{Z}_m \). Thus, choose \( \bar{X} \leq \bar{G}^I \) with \( I \) not empty, \( y \in \bar{G}^I \sim \bar{X} \), and \( \phi \in \text{Hom}(\bar{X}, \bar{G}) \). We want to extend \( \phi \) to \( \psi \in \text{Hom}(\bar{G}^I, \bar{G}) \) so that if \( \phi \equiv 1 \), then \( \psi(y) \neq 1 \). Also, if \( \phi' \in \text{Hom}(\bar{G}_m, \bar{G}) \) extends \( \phi|_{\bar{Z}_m^I} \), then we want to find \( \psi \in \text{Hom}(\bar{G}^I, \bar{G}) \) extending both \( \phi \) and \( \phi' \).

Definition. Define \( X_m := X \cap \mathbb{Z}_m^I \), \( X_p := X \cap (Z_{\mu^t} \times Z(G))^I \), and for \( h \in \mathbb{Z}_m - (Z(G))^I \), define \( X_h := X \cap (a)^I \). Note that \( \bot \in X_m \), \( \bot \in X_p \), but that \( X_h \) may be empty. Each of \( X_m \), \( X_p \), \( X_h \) is closed.

Lemma 3.7. (a) \( + \) is fully defined on \( X_m \) and \( \langle X_m; +, \tau \rangle \) is a closed substructure of \( \langle Z_m^I; +, \tau \rangle \), to which Pontryagin duality for abelian groups of exponent \( m \) applies; (b) \( \circ \) is fully defined on \( X_p \) and \( \langle X_p; \circ, \tau \rangle \) is a closed substructure of \( \langle (Z_{\mu^t} \times Z(G))^I; \circ, \tau \rangle \), to which Pontryagin duality for abelian groups of exponent \( p^t \) applies; (c) for \( h \in \mathbb{Z}_m^I - (Z(G))^I \), \( * \) is fully defined on \( X_h \) and \( \langle X_h; *, \tau \rangle \) is a closed substructure of \( \langle (a)^I \mathbb{Z}_m; *, \tau \rangle \), to which Pontryagin duality for abelian groups of exponent \( p^t \) applies; (d) the effect of \( * \) is that for any \( c \in X \cap Z(G)^I \), \( \langle X_h; *, \alpha, \tau \rangle \) is isomorphic to \( \langle X_h; *, \alpha, \tau \rangle \) via multiplication by \( c \).

Proof. Everything is clear except for part (d) where we need to prove closure under \( \alpha \) and its preservation under multiplication. This follows from the fact that in \( G \), \( \alpha(bc) = \alpha(b)c \), which we now prove. Since \( \alpha(bc) = \alpha(b)\alpha(c) \), we need to show that \( \alpha(c) = c \). Recalling that \( Z(G) = (b^d) \), this reduces to showing that \( \alpha(b^d) = b^d \). But \( \alpha(b^d) = (\alpha(b))^d = (ab)^d = a'b^d \) for some \( s \). On the other hand, we must have \( \alpha(b^d) \in Z(G) \). This means that \( a^d = 1 \) and \( a(b^d) = b^d \).

Thus, \( \phi|_{X_m} \) is a continuous \( \circ \)-homomorphism. By Pontryagin duality for abelian groups of exponent \( p^t \) \( \mu \), there is a continuous \( \circ \)-homomorphism \( \phi_1 : (Z_{\mu^t} \times Z(G))^I \to Z_{\mu^t} \times Z(G) \) which extends \( \phi|_{X_m} \). Also, since \( Z(G) \leq Z_m \) and \( (p, m) = 1 \), we may assume that \( \phi_1 \) extends \( \phi|_{Z(G)^I} \).

Now define \( X'_m := X_m (Z(G))^I \); clearly, \( X'_m \) is closed under \( + \). Define \( \phi_2 : X'_m \to Z_m \) by \( \phi_2(x) := \phi(x) \phi_1(x) \) for \( x \in X_m \) and \( c \in Z(G)^I \).

Lemma 3.8. \( X'_m \) is a closed subset of \( Z_m \), and \( \phi_2 \) is a continuous \( + \)-homomorphism.
\[ \text{PROOF.} \] Let \( z \notin X'_n \), and so \( z \notin X_m \). Thus, there is a finite \( F \subseteq I \) such that \( z' \big|_F = z \big|_F \) implies that \( z' \notin X_m \). For \( z \in Z(G)^F \) choose \( d(z) \in Z(G)^I \) with \( d(z) \big|_F = z \) and with \( d(z^{-1}) = (d(z))^{-1} \); note that there are only finitely many such \( d(z) \). Then \( z d(z) \notin X_m \) as \( z \notin X_m \), implying that \( z d(z) \notin X_m \). Consequently, there is a finite \( E \subseteq I \) such that \( z = z d(z) \big|_E \) implies that \( z \notin X_m \). Define \( E := F \cup \bigcup \{ E_z \mid z \in Z(G)^F \} \); \( E \) is finite. Choose \( z' \) so that \( z' \big|_E = z \big|_E \). Suppose that \( z' \in X_m \); then \( z' = x' z' \) for some \( x' \in X_m \) and \( z' \in Z(G)^I \). Take \( z := z' \big|_E \). Then \( z d(z^{-1}) \in X_m \) as \( z' \in X_m \). But \( z d(z^{-1}) \big|_E = z d(z^{-1}) \big|_{E-z} \) so that \( z d(z^{-1}) \notin X_m \), implying that \( z' \notin X_m \). Thus, the clupset \( \{ z' \mid z \in E \} \) is disjoint from \( X_m \) and \( X_m \) is closed.

Next, we need to see that \( \phi_2 \) is well defined; let \( x = x' x' \in X_m \) and \( x = x' x' \in X_m \). We need to see that \( \phi'(x) \phi_1 (x') = \phi' (x') \phi_1 (x') \). But in \( X_m \) we have \( x' x' = (x')^{-1} x' \in X_m \), so that \( \phi_1 (x') \phi_1 (x') = \phi_1 (x') \phi_1 (x') = \phi_1 (x') \phi_1 (x') \). From \( x = x' x' \) and as \( x' x' \in X_m \), we have \( \phi'(x') = \phi'(x' x') = \phi'(x') \phi_1 (x') \phi_1 (x') \), and the result follows.

Finally, continuity follows since \( \phi' \) and \( \phi_1 \) are continuous by assumption, \( \cdot \) is continuous since it has a finite domain and thus, \( \phi_2 \) is a composition of continuous functions, and so is continuous.

If \( \phi_1 \) extends \( \phi' \big|_{Z(G)^I} \), then \( \phi_2 = \phi' \big|_{Z(G)^I} \). By Pontryagin duality for abelian groups of exponent \( m \), there is a continuous + -homomorphism \( \phi_3 : (Z_m)^I \rightarrow Z_m \) which extends \( \phi_1 \); we may assume that \( \phi_3 = \phi' \). Thus, if we can prove \( \text{INJ} \) and \( \text{STR} \), then the duality will be semidirect over \( Z_m \). We now describe \( Y \), the substructure of \( G' \) generated by \( Z_m^I \cup \{ x \in (Z_m)^I \mid x \cdot \} \), prove that \( Y \) is closed, define an extension \( \phi_4 \) of \( \phi' \) to \( Y \) and prove that \( \phi_4 \) is a continuous homomorphism.

**Definition.** We define \( Y \) to be \( \bigcup \{ Y_b \mid b \in (Z_m)^I \} \), where

(a) for \( b \in Z(G)^I \), \( Y_b := \langle a \rangle b \), else
(b) for \( b \in X_m \), \( Y_b := X_b \), else
(c) for \( b \in X_m \) with \( b = b c \) where \( b' \in X_m \) and \( c \in Z(G)^I \), \( Y_b := X_b c \), else
(d) \( Y_b := \langle a (b) \rangle \).

**Lemma 3.9.** \( Y \) is a closed subset of \( G' \).

**Proof.** Let \( Y' := \bigcup \{ Y_b \mid b \in X_m \} \), and note that \( Y' = X (Z(G))^I \). Then \( Y = \bigcup \{ a (Z_m)^I \} \subseteq Y' \). As \( Z_m^I \) is closed, so is each \( \langle a \rangle (Z_m)^I \). As \( a \) has finite order, there are only finitely many such sets. Thus, we need only prove that \( Y' \) is closed. Let \( y' \notin Y' \). First suppose that \( e(y') \notin X_m \). As \( X_m \) is closed, there is a finite \( F \subseteq I \) such that \( y | F = y' | F \) implies that \( y | F \notin X_m \) so that \( y \notin Y' \). Otherwise, let \( e(y') = b' = b c \) with \( b \in X_m \) and \( c \in Z(G)^I \). Define \( y := y' c^{-1} \) and note that \( y \in Y_b - X \). As \( x \) is closed, there is a finite \( F \subseteq I \) such that \( y | F = y' | F \) implies that \( y \notin X \). Hence, if
where $\mathcal{F}_q$, then $\mathcal{F}_q | Y_\tau = \mathcal{F}_q | Y_\tau$, and so $\mathcal{F}_q | Y_\tau \not\equiv Y_\tau$ implying that $\mathcal{F}_q \not\equiv Y'$. That is, we have shown that if $y' \not\in Y'$, then there is an open neighbourhood of $y'$ disjoint from $Y'$, so that $Y'$ is closed.

**Lemma 3.10.** $Y$ is a substructure of $\mathcal{G}^I$.

**Proof.** This readily follows from Lemma 3.7.

**Definition.** We define $\phi_4 : Y \rightarrow G$ by choosing $y \in Y_\tau$ where $b \in Z_m$.

(a) for $b \in Z(G)^I$, define $\phi_4(y) := \phi_1(y)$, else

(b) for $b \in X_m$, define $\phi_4(y) := \phi'(y)$, else

(c) for $b' \in X_m$ with $b' = b' c$ where $b' \in X_m$ and $c \in Z(G)^I$, define $\phi_4(y) := \phi'(y c^{-1}) \phi_1(c)$, else

(d) $b \in Z_m - X_m$ with $a(b) = ab$ for some $a \in \langle a \rangle^I$ so that $y = (a)^I b$ for some $i$, and we define $\phi_4(y) := \phi_1(a)^I \phi_4(b)$.

**Lemma 3.11.** $\phi_4 \in \text{Hom}(\tilde{Y}, \mathcal{G})$.

**Proof.** We have already proved that $\tilde{Y}$ is a closed substructure of $\mathcal{G}^I$. Inspection of the definition of $\phi_4$ shows that it is a function from $Y$ into $G$. Since $\phi_4$ extends $\phi_3$, it preserves $+$, and since $\phi_4$ extends $\phi_1$, it preserves $\circ$. It is easily checked that $\phi_4$ preserves $\ast$ on each $Y_\tau$. For $\ast$, cases (a) - (c) are straightforward; we prove case (d). Note that both $b$ and $b c$ fall into case (d). Let $y \in Y$ and $c \in Z(G)^I$; we must show that $\phi_3(y \ast c) = \phi_3(y) \ast \phi_3(c)$. Thus, $\phi_3(y \ast c) = \phi_3(y c) = \phi_3(a^I b c) = \phi_1(a^I) \phi_1(b) \phi_1(c) = \phi_4(y) \ast \phi_4(c)$. Finally, using the fact that $\alpha$ fixes each element of $Z_m \times Z(G)$ and that $\alpha$ commutes with multiplication by any element of $Z(G)^I$, we see that $\phi_4$ preserves $\alpha$. That is, $\phi_4$ is a homomorphism. For continuity, recall that $Y = \bigcup \langle (a')^I \rangle \cup Y(Z(G))^I$. Now, $\phi_4|_{Z_m}$ is continuous. Likewise for each $i$, $\phi_4|_{\langle (a')^I \rangle}$ is continuous. Next, note that for $y \in Y_\tau$ where $b \in X_m$ and $c \in Z(G)^I$, $\phi_4(y) = \phi'(y c^{-1}) \phi_1(c)$ is the composition of continuous functions and so is continuous. Thus, we have decomposed $Y$ into finitely many closed sets such that the restriction of $\phi_4$ to each is continuous. Consequently, $\phi_4$ is continuous.

**Theorem 3.12.** Without loss of generality, we may assume that $Z_m^I \cup (Z_{\rho \tau} \times Z(G))^I \subseteq X$.

**Proof.** By Lemma 3.9 - Lemma 3.11, $\tilde{Y}$ is a closed substructure of $\mathcal{G}^I$ containing $\tilde{X}$, and $\phi_4 \in \text{Hom}(\tilde{Y}, \mathcal{G})$ extends $\phi'$. We need to verify that for $y \in Y - X$, we could have chosen $\phi_4$ so that $\phi_4(y) \neq 1$. If $y \in (Z_{\rho \tau} \times Z(G))^I$, then we could have chosen $\phi_4$ so that $\phi_4(y) = \phi_1(y) \neq 1$. Now let $y \in Y_\tau$ for $b \not\in Z(G)^I$. As $Y_\tau \subseteq X$ for $b \in X_m$, we have either $b \in X_m - X_\tau$ or $b \in Z_m^I - X_\tau$. In the first case, $b = b' c$ with
\( b' \in X, c \in Z(G)^I - X \) and \( yc^{-1} \in X \). Then \( \phi_i(y) = \phi'(yc^{-1}) \phi_i(c) \) if \( \phi'(yc^{-1}) \neq 1 \), then we could have taken \( \phi_i(c) = 1 \), and otherwise have taken \( \phi_i(c) \neq 1 \). Finally, if \( b \in Z_m - X_m \), then we could have taken \( \phi_i(b) \neq 1 \); as \( \phi_i(y) = d \phi_i(b) \) for some \( i \), \( \phi_i(y) \neq 1 \).

**Theorem 3.13.** Let \( b \in Z_m ' \); without loss of generality, we may assume that \( (a) ' \in b(Z(G))^I \subseteq X \).

**Proof.** We assume that \( Z_m ' \cup (Z_p^\infty \times Z(G))^I \subseteq X \). The proof is similar to that of Theorem 3.12 and the lemmas preceding it. We state, but do not prove, how to proceed. Let \( Y = X \cup (a) ' \in b(Z(G))^I \); \( \tilde{Y} \) is a closed substructure of \( (G)^I \) containing \( \tilde{X} \). Next, \( X_b \) is a closed substructure of \( (a) ' \in b ; \tau \), and \( \phi_i|_{X_b} \) is a continuous homomorphism. Hence, by Pontryagin duality for abelian groups of exponent \( p^\infty \), there is a continuous homomorphic extension \( \phi_b \) of \( \phi_i|_{X_b} \) to \( (a) ' \in b \). Now define \( \phi_0 : Y \rightarrow G \) by \( \phi_0(y) := \phi(y) \) for \( y \in X \), and otherwise for \( y \in X_b \), define \( \phi_0(y) := \phi_i(yc^{-1}) \phi_i(c) \). Then \( \phi_0 \) is a well-defined continuous homomorphism on \( \tilde{Y} \) extending \( \phi_i \). If \( y \in Y - X \), then we may assume \( y \in (a) ' \in b \) and so could have chosen \( \phi_i \) so that \( \phi_i(y) \neq 1 \).

We note two immediate corollaries.

**Corollary 3.14.** If **INJ** holds, then so does **STR**.

**Corollary 3.15.** If \( I \) is finite, then this special case of **INJ**, where \( \tilde{X} \) is a substructure (necessarily closed) of \( \tilde{G}^I \), holds.

It is tempting to invoke the second corollary by noting that as \( \phi' \) is continuous, it depends only on some finite subset \( F \subseteq I \). Just project \( X \) into \( G^F \) and extend the projection of \( \phi' \). Unfortunately, since \( \tilde{G} \) involves proper partial functions, the projection of \( X \) need not be a substructure and the projection of \( \phi' \) need not be extendable to a structure preserving map on \( G^F \). We can invoke Theorem 3.13 to extend \( \phi' \) to a homomorphism on \( G^I \), but we have no reason to believe that this extension is continuous. The following lemma from [2] is the key to ensuring continuity of an extension.

**Lemma 3.16.** Let \( A \) and \( I \) be sets with \( A \) finite. Suppose that, for every finite \( F \subseteq I \), each element of \( A^F \) is labeled either ‘good’ or ‘bad’ and that if \( F \subseteq F \) and \( x \in A^F \) is ‘bad’, then so is \( x|_F \in A^F \). Then either there is a finite \( F \subseteq I \) such that each element of \( A^F \) is ‘good’ or there is an \( x \in A^I \) such that \( x|_F \) is ‘bad’ for each finite \( F \subseteq I \).
Let us apply Lemma 3.16 to $Z_m^I$. For $h \in Z_m^I$ and finite $F \subseteq I$, define

$$\Gamma^h_F := \{(x|_F, \phi'(x)) \mid x \in X \text{ and } \varepsilon(x|_F) = h|_F\}.$$ 

Notice that $\Gamma^h_F = \Gamma^F_F$ if $h|_F = b|_F$. Call $b|_F$ ‘good’ if $\Gamma^b_F$ is a subset of the graph of a $\ast$-preserving map defined on $\varepsilon^{-1}(b|_F) = \varepsilon^{-1}(b)|_F$; otherwise, call $b|_F$ ‘bad’. Let $F' \subseteq F$ and let $\pi$ denote the natural restriction map from $\varepsilon^{-1}(b)|_F$ to $\varepsilon^{-1}(b)|_{F'}$. If $\gamma$ is an extension of $\Gamma^b_F$ to a $\ast$-preserving map on the $\ast$-substructure generated by $\varepsilon^{-1}(b|_F)$, then $\gamma \circ \pi$ is an extension of $\Gamma^b_F$ to a $\ast$-preserving map on the $\ast$-substructure generated by $\varepsilon^{-1}(b|_{F'})$. Hence ‘badness’ is hereditary in the sense required by Lemma 3.16.

Thus, by Lemma 3.16, either

(a) there is a finite subset $F$ of $I$ such that every member $h$ of $Z_m^I$ is ‘good’,

or

(b) there exists $h \in Z_m^I$ such that for all finite $F \subseteq I$, $h|_F$ is ‘bad’.

**Lemma 3.17.** Case (b) cannot occur.

**Proof.** Assume that $h \in Z_m^I$ such that for all finite $F \subseteq I$, $h|_F$ is ‘bad’; that is, for every finite subset $F$ of $I$, the set

$$\Gamma^h_F = \{(x|_F, \phi'(x)) \mid x \in X \text{ and } \varepsilon(x|_F) = h|_F\}$$

is not a subset of a $\ast$-preserving map defined on the $\ast$-substructure generated by $\varepsilon^{-1}(h|_F)$. Define $\tilde{Y} := X \cup \langle h \rangle (Z(G))'$.

Then by Theorem 3.13, $\tilde{Y}$ is a closed substructure of $\tilde{G}^I$ and $\phi'$ can be extended to a continuous homomorphism $\phi''$ on $\tilde{Y}$. Consequently, $\phi''$ depends only on some finite $F \subseteq I$; that is, for $x, x' \in Y$ with $x|_F = x'|_F$, we have $\phi''(x) = \phi''(x')$. Since $\varepsilon(h|_F) = \varepsilon(h)|_F$ and since $\varepsilon^{-1}(h) \subseteq Y$, we have

$$\Gamma^h_F = \{(x|_F, \phi'(x)) \mid x \in X \text{ and } \varepsilon(x|_F) = h|_F\}$$

$$\subseteq \{(x|_F, \phi''(x)) \mid x \in Y \text{ and } \varepsilon(x|_F) = h|_F\}$$

$$= \{(x|_F, \phi''(x)) \mid x \in \langle a \rangle \langle h \rangle\}.$$ 

But this latter set is the projection of the graph of a $\ast$-homomorphism on a total $\ast$-algebra, and so is the graph of a $\ast$-homomorphism on $\langle a \rangle$ which extends $\Gamma^h_F$, contrary to assumption. This contradiction shows that Case (b) cannot occur.

Thus, we are left with Case (a). Let $F$ be a finite subset of $I$ such that every member $h$ of $Z_m^I$ is good. Let $Y$ be the $\ast$-closure of $X|_F$ in $G^F$.

**Lemma 3.18.** $\tilde{Y}$ is a closed substructure of $\tilde{G}^F$. 

PROOF. As $\tilde{G}^F$ is finite, every subset is closed. By assumption, $Y$ is closed under $\ast$. As $Z_m^I \cup (Z_p^I \times (Z(G))^I) \subseteq X$, $Z_m^I \cup (Z_p^I \times (Z(G))^I) \subseteq X|_F$; thus, $Y$ is closed under $+$ and $\circ$. As $X$ is closed under $\ast$ and contains $Z(G)^I$, it is clear that $Y$ is closed under $\ast$. For closure under $\ast$, let $ab$, $a'b \in X|_F$. Then $\alpha(a'b) = a'\alpha(b) \in X|_F$ and $aa'b \in Y$. Thus, $\alpha(aa'b) = aa'\alpha(b) = ab \ast \alpha(a'b) \in Y$. Inductively, we see that $Y$ is closed under $\ast$.

Next, we want to define a homomorphism $\psi : \tilde{Y} \to \tilde{G}$ whose graph extends the union of the $\Gamma^F_P$ and is a homomorphism. Since $F$ is finite, $\psi$ is automatically continuous.

**Theorem 3.19.** $\text{INJ}$ holds in $\mathbb{S}_p \mathbb{P}(\tilde{G})$.

**Proof.** By Corollary 3.15, we can extend $\psi$ to a continuous homomorphism $\phi_F : G^F \to G$. Now define $\phi$ so that for $\underline{x} \in G^I$, $\phi(\underline{x}) := \phi_F(\underline{x}|_F)$. Then $\phi$ is a continuous homomorphism extending $\phi'$.

**Theorem 3.20.** The structure $\tilde{G}$ yields a strong duality semidirect over $Z_m$ on $\mathbb{S}_p \mathbb{P}(G)$, where $G = Z_{p^r} \rtimes Z_m$ with $(m, p) = 1$.

**Proof.** By Theorem 3.5, condition $\text{CLO}$ holds. By Theorem 3.19, condition $\text{INJ}$ holds. By Corollary 3.14, condition $\text{STR}$ holds.

**Theorem 3.21.** Groups having all Sylow subgroups cyclic are dualizable.

**Proof.** By Theorem 2.1, all these groups $G$ can be represented as a semidirect product of cyclic groups $G = Z_m \rtimes Z_n$ where $(m, n) = 1$. If $m = \prod p_i^{n_i}$, then $Z_m = \prod Z_{p_i^{n_i}}$, where $(p_i, n) = 1$. As by Theorem 3.20 there is a strong duality for the groups $Z_{p_i^{n_i}} \rtimes Z_m$, Theorem 2.3 implies that $G$ is dualizable.

In a companion article [4] we prove that no finite group containing a non-abelian nilpotent subgroup is dualizable. That is, in order for a finite group to be dualizable, it must have abelian Sylow subgroups. From Olshanskii [3] we know that these are exactly the finite groups generating residually small varieties. We conjecture that every finite group with abelian Sylow subgroups is dualizable. We have only rudimentary results in this direction; for instance, we know that the alternating group $A_5$ is dualizable.
References


Department of Mathematics  
Department of Algebra and Number Theory  
University of Manitoba  
ELTE  
Winnipeg, Manitoba R3T 2N2  
Budapest  
Canada  
Hungary  
e-mail: qbush@cc.umanitoba.ca  
e-mail: csaba@cs.elte.hu