THE MULTIPLE HOLOMORPH OF SPLIT METACYCLIC $p$-GROUPS

CINDY (SIN YI) TSANG

Abstract. Given any group $G$, the normalizer $\text{Hol}(G)$ of the subgroup of left translations in the group of all permutations on $G$ is called the holomorph, and the normalizer $\text{NHol}(G)$ of $\text{Hol}(G)$ in turn is called the multiple holomorph. The quotient $T(G) = \text{NHol}(G)/\text{Hol}(G)$ has been computed for various families of groups $G$ in the literature. In this paper, we shall supplement the existing results by considering finite split metacyclic $p$-groups $G$ with $p$ an odd prime. Our work gives new examples of groups $G$ for which $T(G)$ is not a 2-group.

Contents

1. Introduction 1
2. Characterization of equivariant antihomomorphisms 4
3. Isomorphism classes of normal regular subgroups 14
4. Counting residue classes of admissible triplets 17
5. Elements in the multiple holomorph 22
Acknowledgments 26
References 26

1. INTRODUCTION

Let $G$ be a group and write $\text{Perm}(G)$ for the group of all permutations on $G$. Recall that a subgroup $N$ of $\text{Perm}(G)$ is called regular if the map

$$N \longrightarrow G; \quad \eta \mapsto \eta(1_G)$$

is bijective. For example, the images of the left and right regular representations of $G$, respectively defined by

$$\begin{align*}
\lambda : G &\longrightarrow \text{Perm}(G); \quad \lambda(\sigma) = (\tau \mapsto \sigma\tau), \\
\rho : G &\longrightarrow \text{Perm}(G); \quad \rho(\sigma) = (\tau \mapsto \tau\sigma^{-1}),
\end{align*}$$

Date: April 12, 2022.
are regular subgroups of $\text{Perm}(G)$. The \textit{holomorph of $G$} is defined to be
\[ \text{Hol}(G) = \rho(G) \rtimes \text{Aut}(G). \]
Let $\text{Norm}(\cdot)$ denote normalizer in $\text{Perm}(G)$. Then, it is easy to check that
\[ \text{Norm}(\lambda(G)) = \text{Hol}(G) = \text{Norm}(\rho(G)). \]
The \textit{multiple holomorph of $G$} in turn is defined to be
\[ \text{NHol}(G) = \text{Norm}(\text{Hol}(G)). \]
We are interested in the quotient group
\[ T(G) = \text{NHol}(G)/\text{Hol}(G). \]
The study of $T(G)$ was initiated by G. A. Miller in [9]. The motivation was that $T(G)$ acts regularly via conjugation on the set of regular subgroups $N$ of $\text{Perm}(G)$ with $N \cong G$ and $\text{Norm}(N) = \text{Hol}(G)$. A proof of this simple fact may be found in [7, Section 1] or [10, Section 2], for example. The structure of $T(G)$ was determined for all finite abelian groups $G$ in [9] and later for all finitely generated abelian groups $G$ in [8]. Notice that these two papers were published in 1908 and 1951.

Research on the group $T(G)$ was revitalized by T. Kohl’s paper [7] in 2015, and since then the structure of $T(G)$ has been investigated for other families of groups $G$; see [2–4, 10–12]. Interestingly, in a lot of the known cases $T(G)$ turns out to be a 2-group, or even an elementary abelian 2-group. But there are exceptions and the first such example was given by A. Caranti in [4]. He showed that $T(G)$ is not a 2-group for certain $p$-groups $G$ of nilpotency class 2 with $p$ odd. The present author extended this result slightly to $p$-groups $G$ of nilpotency class at most $p - 1$ in [11]. She also gave examples of groups of the form $G = A \rtimes C$, where $A$ is abelian and $C$ is cyclic of order coprime to the exponent of $A$, such that $T(G)$ is not a 2-group. We shall say a bit more about how to construct elements of odd order in $T(G)$ later in Section 5.

The group $T(G)$ acts regularly on and so has the same cardinality as the set of regular subgroups $N$ of $\text{Perm}(G)$ with $N \cong G$ and $\text{Norm}(N) = \text{Hol}(G)$. 
These \( N \) turn out to be precisely the normal regular subgroups \( N \) of \( \text{Hol}(G) \) with \( N \cong G \) when \( G \) is finite. Again a proof of this simple fact may be found in [7, Section 1] or [10, Section 2]. It is easy to see that any regular subgroup \( N \) of \( \text{Hol}(G) \), not necessarily isomorphic to \( G \), must be of the shape

\[
N_{\Gamma} = \{ \rho(\sigma)\Gamma(\sigma) : \sigma \in G \} \text{ for some } \Gamma \in \text{Map}(G, \text{Aut}(G)).
\]

For \( N_{\Gamma} \) to be a subgroup, in which case regularity is guaranteed, of course \( \Gamma \) needs to satisfy certain properties. For \( N_{\Gamma} \) to be a normal subgroup, we have the following nice criterion:

**Proposition 1.1.** For any \( \Gamma \in \text{Map}(G, \text{Aut}(G)) \), the set \( N_{\Gamma} \) above is a normal (regular) subgroup of \( \text{Hol}(G) \) if and only if

\[
\Gamma(\sigma\tau) = \Gamma(\tau)\Gamma(\sigma) \text{ and } \Gamma(\varphi(\sigma)) = \varphi\Gamma(\sigma)\varphi^{-1}
\]

hold for all \( \sigma, \tau \in G \) and \( \varphi \in \text{Aut}(G) \).

**Proof.** See [3, Theorem 5.2]. Note that \( \gamma \) is used there instead of \( \Gamma \), and we changed the notation because \( \gamma \) is to denote something else in Section 2. \( \square \)

**Remark 1.2.** Note that \( \rho(G) \) are \( \lambda(G) \) are both normal regular subgroups of \( \text{Hol}(G) \). They correspond to the maps from \( G \) to \( \text{Aut}(G) \) defined by

\[
\Gamma_{\rho}(\sigma) = \text{Id}_G \text{ and } \Gamma_{\lambda}(\sigma) = \text{conj}(\sigma^{-1}) \text{ for all } \sigma \in G,
\]

respectively, where \( \text{conj}(\cdot) = \rho(\cdot)\lambda(\cdot) \) denotes the inner automorphisms.

Letting \( \text{Aut}(G) \) act on \( G \) canonically and on itself by conjugation, we may restate Proposition 1.1 as follows: the set \( N_{\Gamma} \) is a normal subgroup of \( \text{Hol}(G) \) if and only if \( \Gamma \) is an \( \text{Aut}(G) \)-equivariant antihomomorphism. We now deduce from the above discussion that:

**Corollary 1.3.** For any finite group \( G \), the order of \( T(G) \) is the number of \( \text{Aut}(G) \)-equivariant antihomomorphisms \( \Gamma \) from \( G \) to \( \text{Aut}(G) \) with \( N_{\Gamma} \cong G \).

The purpose of this paper is to study \( T(G) \), via these \( \text{Aut}(G) \)-equivariant antihomomorphisms \( \Gamma \), when \( G \) is a finite split metacyclic \( p \)-group with \( p \) an odd prime. We may assume that \( G \) is non-abelian, because we already know from [9] that \( T(G) \) is trivial for all abelian groups \( G \) of odd order.
Assumption. In the rest of this paper, the symbol $G$ denotes a finite non-abelian split metacyclic $p$-group with $p$ an odd prime. Then, by [6] we know that $G$ has a (unique) presentation of the form

$$(1.1) \quad G = \langle x, y : x^{p^{m}} = 1, y^{p^{n}} = 1, yxy^{-1} = x^{1+p^{m-r}} \rangle,$$

where $m \geq 2$, $n \geq 1$, and $1 \leq r \leq \min\{n, m-1\}$.

Our main result is the following:

**Theorem 1.4.** The order of the quotient $T(G)$ is equal to

$$
\begin{cases}
2p^{m-r+\min\{r,n-r\}} & \text{when } m \leq n \text{ with } m-r < r, \\
(p-1)p^{r-1+\min\{r,n-r\}} & \text{when } m \leq n \text{ with } r \leq m-r, \\
(p-1)p^{r-1} & \text{when } n \leq m-r.
\end{cases}
$$

We are unable to determine the exact order of $T(G)$ when $m-r < n < m$ because the relevant congruence conditions are too complicated in this case; see the end of Section 2. Note that our Theorem 1.4 exhibits another family of groups $G$ for which the order of $T(G)$ is not a power of 2. It also explains why $T(G)$ has order 18 for the group $G$ in [11, Example 3.7], which is (1.1) with $(p,m,n,r) = (3,3,3,2)$; observe that this group $G$ has nilpotency class $p = 3$ and so was not covered by work of [4] or [11].

Here is an outline of this paper. In Sections 2 and 3, respectively, we first give an arithmetic characterization of the Aut($G$)-equivariant antihomomorphisms $\Gamma$ from $G$ to Aut($G$), and determine the isomorphism class of $N_\Gamma$. In Section 4, we prove Theorem 1.4 by counting the number of solutions to certain congruence conditions. Finally in Section 5, we shall discuss the actual elements lying in $T(G)$ and compare them with work of [4] and [12].

2. Characterization of equivariant antihomomorphisms

In this section, we shall give an arithmetic characterization of the Aut($G$)-equivariant antihomomorphisms $\Gamma$ from $G$ to Aut($G$).

For any $z \in \mathbb{Z}$ and $\ell \in \mathbb{N}_{\geq 0}$, let us define

$$S(z, \ell) = 1 + z + \cdots + z^{\ell-1},$$
with the empty sum representing 0. For any \(i, j \in \mathbb{Z}\), we then have
\[
(x^i y^j)^\ell = x^{iS((1+p^{m-r})^j,\ell)} y^{j\ell}.
\]

Below, we record two useful facts, both of which require that \(p\) is odd.

**Lemma 2.1.** Let \(z, \ell, s, t\) be non-negative integers with \(s < t\).

(a) The integer \(z\) satisfies \(z^{p^s} \equiv 1 \pmod{p^t}\) if and only if \(z \equiv 1 \pmod{p^{t-s}}\).

(b) The exact powers of \(p\) dividing \(\ell\) and \(S(z, \ell)\) are equal if \(z \equiv 1 \pmod{p}\).

*Proof.* Part (a) is standard and part (b) is [12, Lemma 2.1]. \qed

Now, it is necessary to understand the structure of \(\text{Aut}(G)\), which has been computed in [1]. We note in passing that the automorphism group of a split metacyclic 2-group is also known by [5].

**Proposition 2.2.** The automorphism group of \(G\) has order
\[
(p - 1)p^{m-1} \cdot p^\min\{m,n\} \cdot p^\min\{m-r,n\} \cdot p^{n-r},
\]
and is a product of four cyclic subgroups, namely
\[
\text{Aut}(G) = \langle \beta \rangle \langle \gamma \rangle \langle \alpha \rangle \langle \delta \rangle,
\]
where \(\alpha, \beta, \gamma, \delta\), respectively, are automorphisms of orders
\[
(p - 1)p^{m-1} \cdot p^\min\{m,n\} \cdot p^\min\{m-r,n\} \cdot p^{n-r},
\]
and are explicitly defined as follows:

- \(\alpha(x) = x^u\) and \(\alpha(y) = y\), where \(u\) generates the units modulo \(p^m\);
- \(\beta(x) = x\) and \(\beta(y) = x^{p^\max\{m-n,0\}} y\);
- \(\gamma(x) = xy^{p^\max\{n-m+r,0\}}\) and \(\gamma(y) = y\);
- \(\delta(x) = x\) and \(\delta(y) = y^{1+p^r}\).

Moreover, we have the following relations:

\[
\begin{align*}
(2.1) \quad &\alpha \delta = \delta \alpha, \quad \alpha \beta \alpha^{-1} = \beta^u, \quad \delta \beta \delta^{-1} = \beta^{(1+p^r)^{-1}}, \quad \delta \gamma \delta^{-1} = \gamma^{1+p^r}, \\
(2.2) \quad &\alpha \gamma \alpha^{-1} = \alpha_{a_0}^u \gamma^{u^{-1}} \quad \text{with} \quad \alpha_{a_0}^u \gamma = \gamma \alpha_{a_0}^u,
\end{align*}
\]
where \(a_0\) is any natural number satisfying the congruence
\[
u^{a_0} \equiv uS((1+p^{m-r})^{p^\max\{n-m+r,0\}}, u^{-1}) \pmod{p^m},
\]
and the \((\cdot)^{-1}\) in the exponents are to be interpreted modulo \(p^{\min\{m,n\}}\).

**Proof.** See [1, Sections 3 and 4] and its corrigendum. \(\square\)

Proposition 2.2 implies that elements of \(\text{Aut}(G)\) may be written as

\[
\beta^b\gamma^c\alpha^a\delta^d,
\]

where \((a, b, c, d) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}\) is uniquely determined modulo \((p-1)p^{m-1}\mathbb{Z} \times p^{\min\{m,n\}}\mathbb{Z} \times p^{\min\{m-r,n\}}\mathbb{Z} \times p^{n-r}\mathbb{Z}.

Since an antihomomorphism \(\Gamma\) from \(G\) to \(\text{Aut}(G)\) is uniquely determined by the values of \(\Gamma(x)\) and \(\Gamma(y)\), it is also clear that:

**Lemma 2.3.** For any \(\psi_x, \psi_y \in \text{Aut}(G)\), the assignments

\[
\Gamma(x) = \psi_x \text{ and } \Gamma(y) = \psi_y
\]

extend to an antihomomorphism \(\Gamma\) from \(G\) to \(\text{Aut}(G)\) if and only if

\[
\psi_x^{p^m} = \text{Id}_G, \quad \psi_y^{p^n} = \text{Id}_G, \quad \psi_y^{-1}\psi_x\psi_y = \psi_x^{1+p^{m-r}}.
\]

Moreover, in this case \(\Gamma\) is \(\text{Aut}(G)\)-equivariant exactly when

\[
(2.3) \quad \Gamma(\varphi(x)) = \varphi\Gamma(x)\varphi^{-1} \text{ and } \Gamma(\varphi(y)) = \varphi\Gamma(y)\varphi^{-1}
\]

are both satisfied for \(\varphi\) ranging over the generators \(\alpha, \beta, \gamma, \delta\).

The problem is then reduced to determining which of the \(\psi_x, \psi_y \in \text{Aut}(G)\) satisfy the conditions in Lemma 2.3. But \(\psi_x\) and \(\psi_y\) are each determined by four parameters, one for each of the generators \(\alpha, \beta, \gamma, \delta\), so approaching this directly could lead to some very complicated calculations. To overcome this issue, we shall first significantly narrow down the possibilities for \(\psi_x, \psi_y\), and show that they only require one and two parameters, respectively.

**Proposition 2.4.** Every \(\text{Aut}(G)\)-equivariant antihomomorphism \(\Gamma\) from \(G\) to \(\text{Aut}(G)\) satisfies the containments

(a) \(\Gamma(y) \in \langle \alpha^{(p-1)p^{m-r-1}} \rangle \times \langle \delta^{p^{\max\{n-2r,0\}}} \rangle;\)

(b) \(\Gamma(x) \in \langle \beta^{p^{\min\{m,n\}-r}} \rangle.\)
Proof of (a). Write \( \Gamma(y) = \beta^a \gamma^c \alpha^d \delta^d \) with \( a, b, c, d \in \mathbb{N} \). Observe that
\[
\Gamma(y)^{1+p^r} = \Gamma(y^{1+p^r}) = \Gamma(\delta(y)) = \delta \Gamma(y) \delta^{-1}.
\]
Assuming that \( \beta^b = \gamma^c = \text{Id}_G \), by (2.1) this simplifies to
\[
\alpha^{ap^r} \delta^{dp^r} = \text{Id}_G,
\]
and so
\[
\begin{cases}
  a \equiv 0 \pmod{(p-1)p^{m-r-1)}, \\
  d \equiv 0 \pmod{p^{\max\{n-2r,0\}}}
\end{cases}
\]
It remains to show that indeed \( \beta^b = \gamma^c = \text{Id}_G \). We shall use the relation
\[
\Gamma(y) = \Gamma(\alpha(y)) = \alpha \Gamma(y) \alpha^{-1}.
\]
Using (2.1) and (2.2), we may rewrite the above as
\[
\beta^{b(u-1)} \gamma^{c(u-1)-1} \alpha^{ca_0} = \text{Id}_G.
\]
Note that \( u-1 \) and \( u^{-1}-1 \) are coprime to \( p \) by Lemma 2.1(a). Since \( \beta \) and \( \gamma \) have orders a power of \( p \), we see that \( \beta^b = \gamma^c = \text{Id}_G \), as desired. \( \square \)

Proof of (b). Write \( \Gamma(x) = \beta^b \gamma^c \alpha^a \delta^d \) with \( a, b, c, d \in \mathbb{N} \). Observe that
\[
\Gamma(x) = \Gamma(\delta(x)) = \delta \Gamma(x) \delta^{-1}.
\]
Assuming that \( \gamma^c = \alpha^a = \delta^d = \text{Id}_G \), by (2.1) this simplifies to
\[
\beta^{bp^r} = \text{Id}_G,
\]
and so \( b \equiv 0 \pmod{p^{\min\{m,n\}-r}} \).

Hence, it remains to show that indeed \( \gamma^c = \alpha^a = \delta^d = \text{Id}_G \).

For \( m \leq n \), we have \( \beta(y) = xy \), whence
\[
\Gamma(y) \Gamma(x) = \Gamma(\beta(y)) = \beta \Gamma(y) \beta^{-1}, \quad \text{and so} \quad \Gamma(x) = \Gamma(y)^{-1} \beta \Gamma(y) \beta^{-1}.
\]
Since \( \Gamma(y) \) lies in \( \langle \alpha \rangle \times \langle \delta \rangle \) by (a), from (2.1) we see that \( \langle \beta \rangle \) is normalized by \( \Gamma(y) \), so then \( \Gamma(x) \) is a power of \( \beta \). Thus, we have \( \gamma^c = \alpha^a = \delta^d = \text{Id}_G \).

For \( m > n \), we shall first use the relation
\[
\Gamma(x) = \Gamma(\beta(x)) = \beta \Gamma(x) \beta^{-1}.
\]
Using (2.1), we may rewrite the above as
\[
\gamma^c = \beta \gamma^c \beta^{-u^a(1+p^r)-d}.
\]
In particular, we have the equality
\[ \gamma^c(x) = (\beta \gamma^c \beta^{-u^{a(1+p^r)}-d})(x) = (\beta \gamma^c)(x). \]

By comparing the \( \langle x \rangle \)-components, we see that
\[ x = x^{1+p^{m-r}S(1+p^{m-r},cp^{\max\{n-m+r,0\}})}, \]
and so \( c \equiv 0 \pmod{p^{\min\{m-r,n\}}} \) in view of Lemma 2.1(b). This shows that \( \gamma^c = \text{Id}_G \), and so in fact \( \Gamma(x) \) lies in the subgroup \( \langle \beta \rangle \rtimes (\langle \alpha \rangle \times \langle \delta \rangle) \). Next, we consider the relations
\[ \Gamma(x)^{p^m} = \text{Id}_G \text{ and } \Gamma(x)^u = \Gamma(x^u) = \Gamma(\alpha(x)) = \alpha \Gamma(x) \alpha^{-1}. \]

By projecting them onto \( \langle \alpha \rangle \times \langle \delta \rangle \), we obtain
\[ \alpha^{ap^m} \delta^{dp^m} = \text{Id}_G \text{ and } \alpha^{a(u-1)} \delta^{d(u-1)} = \text{Id}_G. \]

Again, we know from Lemma 2.1(a) that \( u - 1 \) is coprime to \( p \). The second equation then yields \( \delta^d = \text{Id}_G \) because \( \delta \) has order a power of \( p \). From these two equalities, respectively, we also see that
\[ a \equiv 0 \pmod{p - 1} \text{ and } a \equiv 0 \pmod{p^{m-1}}. \]

It follows that \( \alpha^a = \text{Id}_G \) as well, and this proves the claim. \( \square \)

In view of Proposition 2.4, let us introduce some notation. Put
\[ \tilde{\alpha} = \alpha^{(p-1)p^{m-r}-1}, \tilde{\beta} = \beta^{p^{\min\{m,n\}-r}}, \tilde{\delta} = \delta^{p^{\max\{n-2r,0\}}}, \]
and observe that their orders in \( \text{Aut}(G) \) are given by
\[ (2.4) \quad |\tilde{\alpha}| = p^r, \quad |\tilde{\beta}| = p^r, \quad |\tilde{\delta}| = p^{\min\{r,n-r\}}. \]

Further define the integers
\[ \tilde{u} = u^{(p-1)p^{m-r}-1}, \quad \tilde{v} = (1+p^r)^{p^{\max\{n-2r,0\}}}. \]

Then, it follows from the definition that
\[ \tilde{\alpha}(x) = x^{\tilde{u}}, \quad \tilde{\beta}(y) = x^{p^{m-r}y}, \quad \tilde{\delta}(y) = y^{\tilde{v}}, \]
and by Lemma 2.1(a), we have
\[ (2.5) \quad p^{m-r} \parallel \tilde{u} - 1, \quad p^{\max\{r,n-r\}} \parallel \tilde{v} - 1. \]
For convenience, we also make the following definition.

**Definition 2.5.** For any \( a, b, d \in \mathbb{Z} \), define

\[
\Gamma_{a,b,d}(x) = \tilde{\beta}^b \quad \text{and} \quad \Gamma_{a,b,d}(y) = \tilde{\alpha}^a \tilde{\delta}^d.
\]

The triplet \((a, b, d)\) is called *pre-admissible* if \(\Gamma_{a,b,d}\) extends to an antihomomorphism from \(G\) to \(\text{Aut}(G)\), and *admissible* if \(\Gamma_{a,b,d}\) is \(\text{Aut}(G)\)-equivariant in addition.

**Remark 2.6.** Recall Remark 1.2. It is not hard to see that

\[
\Gamma_\rho = \Gamma_{0,0,0} \quad \text{and} \quad \Gamma_\lambda = \Gamma_{a_\lambda,1,0},
\]

where \(a_\lambda \in \mathbb{N}\) is such that \(\tilde{u}^{a_\lambda} \equiv (1 + p^{m-r})^{-1} \pmod{p^m}\).

The \(\text{Aut}(G)\)-equivariant antihomomorphisms \(\Gamma\) from \(G\) to \(\text{Aut}(G)\) are thus precisely the maps \(\Gamma_{a,b,d}\) for \((a, b, d)\) ranging over all admissible triplets. We shall now characterize admissibility in terms of congruence conditions.

**Proposition 2.7.** A triplet \((a, b, d)\) is pre-admissible if and only if

\[
b\tilde{u}^{-a} \equiv b(1 + p^{m-r}) \pmod{p^r}.
\]

**Proof.** By Lemma 2.3, a triplet \((a, b, d)\) is pre-admissible if and only if

\[
(\tilde{\beta}^b)^{p^n} = \text{Id}_G, \quad (\tilde{\alpha}^a \tilde{\delta}^d)^{p^n} = \text{Id}_G, \quad (\tilde{\alpha}^a \tilde{\delta}^d)^{-1} \tilde{\beta}^b (\tilde{\alpha}^a \tilde{\delta}^d) = \tilde{\beta}^b(1 + p^{m-r}).
\]

Note that the first two equalities always hold by (2.4). For the last equality, using (2.1) we may rewrite the left hand side as

\[
(\tilde{\alpha}^a \tilde{\delta}^d)^{-1} \tilde{\beta}^b (\tilde{\alpha}^a \tilde{\delta}^d) = \tilde{\delta}^{-d} \tilde{\alpha}^{-a} \tilde{\beta}^b \tilde{\alpha}^a \tilde{\delta}^d = \tilde{\beta}^{b\tilde{u}^{-a} \tilde{v}^d}.
\]

Since \(\tilde{\beta}\) has order \(p^r\) and \(\tilde{v} \equiv 1 \pmod{p^r}\), we see that the claim holds.

To decide whether a pre-admissible triplet \((a, b, d)\) is in fact admissible, we need to check the two equations in (2.3) for \(\varphi\) ranging over \(\alpha, \beta, \gamma, \delta\). There are eight relations in total, but it turns that out five of them always hold.

**Proposition 2.8.** For any pre-admissible triplet \((a, b, d)\), the antihomomorphism \(\Gamma = \Gamma_{a,b,d}\) satisfies the relations

\[
\Gamma(\varphi(x)) = \varphi\Gamma(x)\varphi^{-1} \quad \text{for} \quad \varphi \in \{\alpha, \beta, \delta\},
\]
\[ \Gamma(\varphi(y)) = \varphi \Gamma(y) \varphi^{-1} \text{ for } \varphi \in \{\alpha, \delta\}. \]

**Proof.** Using (2.1), it is straightforward to check that
\[ \Gamma(\alpha(x)) = \Gamma(x)^u = \tilde{\beta}^b = \alpha \tilde{\beta}^b \alpha^{-1} = \alpha \Gamma(x) \alpha^{-1}, \]
\[ \Gamma(\beta(x)) = \Gamma(x) = \tilde{\beta}^b = \beta \tilde{\beta}^b \beta^{-1} = \beta \Gamma(x) \beta^{-1}, \]
\[ \Gamma(\alpha(y)) = \Gamma(y) = \tilde{\alpha}^a \tilde{\delta}^d = \alpha \tilde{\alpha}^a \tilde{\delta}^d \alpha^{-1} = \alpha \Gamma(y) \alpha^{-1}. \]

Together with (2.4), it is also easy to see that
\[ \Gamma(\delta(x)) = \Gamma(x) = \tilde{\beta}^b = \tilde{\beta}^{b(1+p^r)}^{-1} = \delta \tilde{\beta}^b \delta^{-1} = \delta \Gamma(x) \delta^{-1}, \]
\[ \Gamma(\delta(y)) = \Gamma(y)^{1+p^r} = \tilde{\alpha}^{a(1+p^r)} \tilde{\delta}^{d(1+p^r)} = \tilde{\alpha}^a \tilde{\delta}^d = \delta \tilde{\alpha}^a \tilde{\delta}^d \delta^{-1} = \delta \Gamma(y) \delta^{-1}. \]

Thus, indeed the five stated relations are satisfied. \(\Box\)

For the remaining three relations, two of them are fairly easy to deal with, while \(\Gamma(\gamma(x)) = \gamma \Gamma(x) \gamma^{-1}\) is complicated in general. But as we shall show, the congruences in Proposition 2.9(c) below may be simplified when \(m \leq n\) or \(n \leq m - r\); this is why we restricted to these two cases in Theorem 1.4.

**Proposition 2.9.** Let \((a, b, d)\) be a pre-admissible triplet and put \(\Gamma = \Gamma_{a,b,d} \).

(a) The relation \(\Gamma(\beta(y)) = \beta \Gamma(y) \beta^{-1}\) holds if and only if
\[ \tilde{u}^{-a} \tilde{v}^d \equiv 1 + bp^{m-r} \pmod{p^{\min\{m,n\}}}. \]

(b) The relation \(\Gamma(\gamma(y)) = \gamma \Gamma(y) \gamma^{-1}\) holds if and only if
\[ a_0(\tilde{u}^{-a} - 1) \equiv 0 \pmod{p^{m-1}}, \]
\[ (2.6) \quad \tilde{u}^{-a} \tilde{v}^d \equiv 1 \pmod{p^{\min\{m-r,n\}}}, \]

where \(a_0\) is defined as in Proposition 2.2.

(c) The relation \(\Gamma(\gamma(x)) = \gamma \Gamma(x) \gamma^{-1}\) holds if and only if
\[ \tilde{u}^{aq}(1 + bp^{m-r} S(1 + p^{m-r}, q)) \equiv 1 \pmod{p^m}, \]
\[ \tilde{u}^{aq} bp^{m-r} \equiv S((1 + p^{m-r})^q, bp^{m-r}) \pmod{p^m}, \]
\[ \tilde{v}^{dq} \equiv 1 \pmod{p^n}, \]

where we define \(q = p^{\max\{n-m+r,0\}}\).
Proof of (a). The relation $\Gamma(\beta(y)) = \beta \Gamma(y) \beta^{-1}$ is equivalent to

$$\Gamma(x)^{p^{\max\{m-n,0\}}} \beta = \Gamma(y)^{-1} \beta \Gamma(y),$$

that is $\beta^{bp^{m-r}} \beta = (\tilde{\alpha}^a \tilde{\delta}^d)^{-1} \beta (\tilde{\alpha}^a \tilde{\delta}^d)$. But by (2.1), we may rewrite the right hand side as

$$(\tilde{\alpha}^a \tilde{\delta}^d)^{-1} \beta (\tilde{\alpha}^a \tilde{\delta}^d) = \tilde{\delta}^{-d} \tilde{\alpha}^{-a} \beta \tilde{\alpha}^a \tilde{\delta}^d = \beta \tilde{u}^{-a} \tilde{v}^d,$$

and the claim is now clear. \qed

Proof of (b). The relation $\Gamma(\gamma(y)) = \gamma \Gamma(y) \gamma^{-1}$ is equivalent to

$$\gamma = \Gamma(y) \gamma \Gamma(y)^{-1},$$

that is $\gamma = (\tilde{\alpha}^a \tilde{\delta}^d) \gamma (\tilde{\alpha}^a \tilde{\delta}^d)^{-1}$.

First, using induction, we deduce from (2.2) that

$$\alpha^\ell \gamma \alpha^{-\ell} = \alpha a_0 S(u^{-1},\ell) \gamma u^{-\ell} = \alpha a_0 (u^{-\ell}-1)/(u^{-1}-1) \gamma u^{-\ell}$$

for all $\ell \in \mathbb{N}_{\geq 0}$.

Together with (2.1), we then see that

$$(\tilde{\alpha}^a \tilde{\delta}^d) \gamma (\tilde{\alpha}^a \tilde{\delta}^d)^{-1} = \tilde{\alpha}^a \gamma \tilde{\delta}^d \tilde{\alpha}^{-a} = \alpha a_0 \gamma \tilde{v}^d (\tilde{u}^{-a}-1)/(u^{-1}-1) \gamma \tilde{u}^{-a} \tilde{v}^d.$$

Thus, the relation $\Gamma(\gamma(y)) = \gamma \Gamma(y) \gamma^{-1}$ holds exactly when

$$\alpha a_0 \gamma \tilde{v}^d (\tilde{u}^{-a}-1)/(u^{-1}-1) = \text{Id}_G$$

and $\gamma \tilde{u}^{-a} \tilde{v}^d = \gamma$.

Note that $u a_0 \equiv 1 \pmod{p}$ by definition, so $p-1$ divides $a_0$. Since $u^{-1}-1$ and $\tilde{v}$ are coprime to $p$, we see that the first equation is equivalent to (2.6). The second equation is clearly equivalent to (2.7), whence the claim. \qed

Proof of (c). The relation $\Gamma(\gamma(x)) = \gamma \Gamma(x) \gamma^{-1}$ is equivalent to

$$\Gamma(y)^q \Gamma(x) \gamma = \gamma \Gamma(x),$$

that is $\tilde{\alpha}^{aq} \tilde{\delta}^{dq} \tilde{b}^b \gamma = \gamma \tilde{b}^b$,

where $q = p^{\max\{n-m+r,0\}}$. A direct computation yields

$$(\tilde{\alpha}^{aq} \tilde{\delta}^{dq} \tilde{b}^b \gamma)(x) = x^{\tilde{u}^{aq}(1+bp^{m-r}S(1+p^{m-r}.q))} y^{\tilde{v}^{dq}},$$

$$(\tilde{\alpha}^{aq} \tilde{\delta}^{dq} \tilde{b}^b \gamma)(y) = x^{\tilde{u}^{aq}bp^{m-r}} y^{\tilde{v}^{dq}},$$

$$(\gamma \tilde{b}^b)(x) = xy^q,$$

$$(\gamma \tilde{b}^b)(y) = x^{S(1+p^{m-r}q,bp^{m-r})} y^{1+bp^{m-r}q},$$

and $y^{1+bp^{m-r}q} = y$. The claim now follows by comparing the exponents. \qed
To summarize, we have shown that a triplet \((a, b, d)\) is admissible exactly when the congruence conditions in Propositions 2.7 and 2.9 are all satisfied. Notice that (2.7) follows from the condition in Proposition 2.9(a) and so may be omitted. Let us further simplify the conditions, as follows.

**Lemma 2.10.** Every admissible triplet \((a, b, d)\) satisfies
\[
b \equiv 0 \text{ or } 1 \pmod{p^\max\{2r-m,0\}}.
\]

**Proof.** Recall that \(\tilde{v} \equiv 1 \pmod{p^r}\). From the conditions in Propositions 2.7 and 2.9(a), we then deduce that
\[
0 \equiv b(\tilde{u}^a(1 + p^{m-r}) - 1) \pmod{p^r}
\]
\[
\equiv b(\tilde{u}^a(1 + bp^{m-r}) + \tilde{u}^a(1 - b)p^{m-r} - 1) \pmod{p^r}
\]
\[
\equiv b(\tilde{v}^d + \tilde{u}^a(1 - b)p^{m-r} - 1) \pmod{p^r}
\]
\[
\equiv \tilde{u}^a b(1 - b)p^{m-r} \pmod{p^r}.
\]
Since \(\tilde{u}\) is coprime to \(p\), this implies that
\[
b(1 - b) \equiv 0 \pmod{p^\max\{2r-m,0\}}.
\]
The claim now follows since \(b\) and \(1 - b\) cannot both be divisible by \(p\). \(\square\)

Since \(\tilde{v} \equiv 1 \pmod{p^r}\), given the two conditions in Proposition 2.9(a) and Lemma 2.10, we may deduce that
\[
b \tilde{u}^{-a} \equiv b(1 + bp^{m-r}) \equiv b(1 + p^{m-r}) \pmod{p^r},
\]
which is the condition in Proposition 2.7. Hence, a triplet \((a, b, d)\) is admissible if and only if the conditions in (2.6), Propositions 2.9(a),(c), and Lemma 2.10 are all satisfied. We now specialize to the cases \(m \leq n\) and \(n \leq m - r\).

**Corollary 2.11.** If \(m \leq n\), then \((a, b, d)\) is admissible exactly when
\[
\tilde{u}^{-a} \tilde{v}^d \equiv 1 + bp^{m-r} \pmod{p^m},
\]
\[
b \equiv 0 \text{ or } 1 \pmod{p^\max\{2r-m,0\}}.
\]

**Proof.** Suppose that \(m \leq n\) and let \(q = p^{n-m+r}\). Since \(p^r \mid q\), we have
\[
(1 + p^{m-r})q \equiv 1 \pmod{p^m}
\]
by Lemma 2.1(a). It then follows from the definition that
\[ u^{a_0} \equiv uS((1 + p^{m-r})^q, u^{-1}) \equiv uS(1, u^{-1}) \equiv 1 \pmod{p^m}, \]
which implies \( a_0 \equiv 0 \pmod{p^{m-1}} \). This means that (2.6) always holds and so may be omitted. Again by Lemma 2.1, and also (2.5), we have
\[ \tilde{u}^q \equiv 1 \pmod{p^m}, \quad \tilde{v}^d \equiv 1 \pmod{p^n}, \quad S(1 + p^{m-r}, q) \equiv 0 \pmod{p^r}. \]
We then see that the conditions in Proposition 2.9(c) hold and thus may be omitted as well. Hence, we are left with the conditions in Proposition 2.9(a) and Lemma 2.10, as claimed. \( \square \)

**Lemma 2.12.** If \( r \leq m - r \), then for any \( z \in \mathbb{Z} \) and \( \ell \in \mathbb{N}_{\geq 0} \), we have
\[ (1 + zp^{m-r})^\ell \equiv 1 + \ell zp^{m-r} \pmod{p^m}, \]
which in particular implies that
\[ S(1 + zp^{m-r}, \ell) \equiv \ell + \frac{1}{2} \ell(\ell - 1)zp^{m-r} \pmod{p^m}. \]

**Proof.** This follows from the binomial theorem, for example. \( \square \)

**Corollary 2.13.** If \( n \leq m - r \), then \((a, b, d)\) is admissible exactly when
\[ \tilde{u}^a(1 + bp^{m-r}) \equiv 1 \pmod{p^m}, \]
\[ \tilde{v}^d \equiv 1 \pmod{p^n}. \]

**Proof.** Suppose that \( n \leq m - r \). We have
\[ u^{a_0} \equiv uS(1 + p^{m-r}, u^{-1}) \equiv uS(1, u^{-1}) \equiv 1 \pmod{p^{m-r}} \]
by definition, and this implies that \( a_0 \equiv 0 \pmod{p^{m-r-1}} \). Since \( r \leq m - r \), together with (2.5), we see that (2.6) always holds and so may be omitted. Note also that the condition in Lemma 2.10 is vacuous. Now, by plugging in \( q = 1 \), the congruences in Proposition 2.9(c) become
\[ \tilde{u}^a(1 + bp^{m-r}) \equiv 1 \pmod{p^m}, \]
\[ \tilde{u}^a bp^{m-r} \equiv S(1 + p^{m-r}, bp^{m-r}) \pmod{p^m}, \]
\[ \tilde{v}^d \equiv 1 \pmod{p^n}. \]
By Lemma 2.12, the second congruence may be rewritten as

$$\tilde{u}^a b \equiv b + \frac{1}{2} b(bp^{m-r} - 1)p^{m-r} \equiv b \pmod{p^r},$$

which follows from the first congruence and so may be omitted. Notice that the condition in Proposition 2.9(a) may be omitted as well because it follows from the first and third congruences above. Thus, we are only left with the two stated congruences, as claimed.

We have left out the case $m - r < n < m$ here because we do not see any simple way of dealing with the congruences in Proposition 2.9(c).

3. ISOMORPHISM CLASSES OF NORMAL REGULAR SUBGROUPS

In Section 2, we described the Aut($G$)-equivariant antihomomorphisms $\Gamma$ from $G$ to Aut($G$) in terms of suitable congruence conditions. To compute the order of $T(G)$, however, by Corollary 1.3 we only want to count those $\Gamma$ whose associated normal regular subgroup $N_\Gamma$ is isomorphic to $G$.

In this section, let us fix an admissible triplet $(a, b, d)$, and by definition

$$N_{\Gamma_{a,b,d}} = \{\rho(x^i)\rho(y^j)\tilde{\alpha}^a \tilde{\delta}^d \tilde{\beta}^b : i, j \in \mathbb{Z}\}.$$  

We shall show that $N_{\Gamma_{a,b,d}}$ is also a split metacyclic $p$-group, isomorphic to a semidirect product of $\mathbb{Z}/p^m\mathbb{Z}$ and $\mathbb{Z}/p^n\mathbb{Z}$, but it need not be non-abelian. We shall determine the isomorphism class of $N_{\Gamma_{a,b,d}}$ by exhibiting a presentation. As an application, we give a criterion for $N_{\Gamma_{a,b,d}}$ to be isomorphic to $G$.

Taking $(i, j) = (1, 0), (0, 1)$, respectively, we obtain the elements

$$\Phi_x = \rho(x)\tilde{\beta}^b$$

$$\Phi_y = \rho(y)\tilde{\alpha}^a \tilde{\delta}^d.$$

Note that for any $\ell \in \mathbb{N}$, we have

$$\Phi_x^\ell = \rho(x)\tilde{\beta}^b(x)\cdots \tilde{\beta}^b(\ell - 1)(x))\tilde{\beta}^{b\ell} = \rho(x^\ell)\tilde{\beta}^{b\ell},$$

$$\Phi_y^\ell = \rho(y(\tilde{\alpha}^a \tilde{\delta}^d)(y)\cdots (\tilde{\alpha}(\ell - 1) \tilde{\delta}(\ell - 1))(y))\tilde{\alpha}^{a\ell} \tilde{\delta}^{d\ell} = \rho(y^S(\tilde{\nu}, \ell))\tilde{\alpha}^{a\ell} \tilde{\delta}^{d\ell}.$$

From this, it is clear that $\langle \Phi_x \rangle$ and $\langle \Phi_y \rangle$ intersect trivially. Since $N_{\Gamma_{a,b,d}}$ has the same order $p^{m+n}$ as $G$, the next lemma shows that $N_{\Gamma_{a,b,d}}$ is also a split metacyclic $p$-group and is given by the semidirect product $\langle \Phi_x \rangle \rtimes \langle \Phi_y \rangle$. 
Lemma 3.1. The elements $\Phi_x$ and $\Phi_y$, respectively, have orders $p^m$ and $p^n$. Moreover, they satisfy the relation $\Phi_y \Phi_x \Phi_y^{-1} = \Phi_x \Phi y^a(1+(1-b)p^{m-r}) \cdot \Phi$. 

Proof. The first claim follows from (3.1), (2.4), and Lemma 2.1(b). To prove the relation, we compute that 

$$\Phi_y \Phi_x \Phi_y^{-1} = \rho(y) \alpha^a \delta^d \cdot \rho(x) \beta^b \cdot \rho(y) \alpha^a \delta^d)^{-1}$$

$$= \rho(y) \rho((\alpha^a \delta^d)(x)) \cdot \alpha^a \delta^d \beta^b \delta^{-d} \alpha^{-a} \cdot \rho(y^{-1})$$

$$= \rho(y x \alpha^a) \beta^b \alpha^a \delta^d \rho(y^{-1})$$

where we used (2.1) in the last equality. But $\tilde{\upsilon} \equiv 1 \pmod{p^r}$, and we know that $\tilde{\beta}$ has order $p^r$. We then see that 

$$\Phi_y \Phi_x \Phi_y^{-1} = \rho(y x \alpha^a) \beta^b \alpha^a \delta^d \rho(y^{-1}) \beta^b \alpha^a$$

Recall that $bp^{m-r} \equiv \epsilon p^{m-r} \pmod{p^r}$ with $\epsilon \in \{0, 1\}$ by Lemma 2.10, and so 

$$b(1 - b)p^{m-r} \equiv \epsilon(1 - \epsilon)p^{m-r} \equiv 0 \pmod{p^r}.$$ 

Since $\tilde{\beta}$ has order $p^r$, we see that indeed 

$$\Phi_y \Phi_x \Phi_y^{-1} = \rho(x \alpha^a(1+(1-b)p^{m-r})) \beta^b \alpha^a(1+(1-b)p^{m-r}))$$

$$= \Phi_x \alpha^a(1+(1-b)p^{m-r})),$$ 

where the second equality follows from (3.1). 

To determine whether $N_{\Gamma_{a,b,d}}$ is isomorphic to $G$, first note that 

$$p^{m-r+s_{a,b,d}} \parallel u^a(1 + (1 - b)p^{m-r}) - 1$$

by (2.5), and there exists $j_{a,b,d} \in \mathbb{N}$ coprime to $p$ such that 

$$\Phi_y \Phi_x \Phi_y^{-1} = \Phi_x \alpha^a(1+(1-b)p^{m-r})) \mid \Phi_y^{j_{a,b,d}} \equiv 1 + p^{m-r+s_{a,b,d}} \pmod{p^m}$$

by Lemma 2.1(a). Setting $\Phi' = \Phi_y^{j_{a,b,d}}$, we then obtain:
Corollary 3.2. The group $N_{\Gamma_{a,b,d}}$ admits the presentation

$$N_{\Gamma_{a,b,d}} = \langle \Phi_x, \Phi_y' : \Phi_x^m = 1, (\Phi_y')^n = 1, (\Phi_y')\Phi_x(\Phi_y')^{-1} = \Phi_x^{1+p^{m-r+s_{a,b,d}}} \rangle,$$

which is isomorphic to $G$ if and only if $s_{a,b,d} = 0$, that is

(3.3) $\tilde{u}^a(1 + (1 - b)p^{m-r}) \not\equiv 1 \pmod{p^{m-r+1}}$.

Proof. The first claim is clear from Lemma 3.1, and the second claim follows from [6], which tells us that the presentation (1.1) is unique.

The above presentation of $N_{\Gamma_{a,b,d}}$ may be also be used to explicitly describe the element in $T(G)$ which $N_{\Gamma_{a,b,d}}$ corresponds to when $N_{\Gamma_{a,b,d}}$ is isomorphic to $G$. Note that when $s_{a,b,d} = 0$, we have a well-defined isomorphism

$$\lambda(G) \rightarrow N_{\Gamma_{a,b,d}}; \begin{cases} \lambda(x) \mapsto \Phi_x, \\ \lambda(y) \mapsto \Phi_y^{j_{a,b,d}}. \end{cases}$$

Then, as shown in the proof of [10, Lemma 2.1], this implies that

(3.4) $N_{\Gamma_{a,b,d}} = \pi_{a,b,d}\lambda(G)\pi_{a,b,d}^{-1}$,

where $\pi_{a,b,d}$ is the bijection defined by

$$\pi_{a,b,d} : G \rightarrow G; \quad \pi_{a,b,d}(x^iy^j) = (\Phi_x^i\Phi_y^{ja,b,d})^{-1}(1).$$

In particular, the element in $T(G)$ which $N_{\Gamma_{a,b,d}}$ gives rise to is $\pi_{a,b,d}\text{Hol}(G)$. Note that $\pi_{a,b,d}$ depends on the choice of $j_{a,b,d}$, which is only unique modulo $p^r$. But say $\pi_{a,b,d}'$ is the bijection arising from a different choice $j'_{a,b,d}$. Then, we have $j_{a,b,d}^{-1}j'_{a,b,d} \equiv 1 \pmod{p^r}$, so there exists $\varphi \in \text{Aut}(G)$ which is a power of $\delta$ such that $\varphi(x) = x$ and $\varphi(y) = y^{j_{a,b,d}^{-1}j'_{a,b,d}}$. We see that

$$\pi_{a,b,d}' = \pi_{a,b,d} \circ \varphi \quad \text{and so} \quad \pi_{a,b,d}' \equiv \pi_{a,b,d} \pmod{\text{Aut}(G)}.$$

Thus, the element $\pi_{a,b,d}\text{Hol}(G)$ in $T(G)$, which is what we care about, does not depend on the choice of $j_{a,b,d}$. Let us end this section by computing the explicit action of $\pi_{a,b,d}$.

Proposition 3.3. If $s_{a,b,d} = 0$, then with a fixed choice of $j_{a,b,d}$, we have

$$\pi_{a,b,d}(x^iy^j) = x^{-i(1+bp^{m-r}S(k,S(\tilde{v}^d,j_0)))k-S(\tilde{v}^d,j_0)}y^{-S(\tilde{v}^d,j_0)},$$
where we define $k = 1 + p^{m-r}$ and $j_0 = j_{a,b,d}$.

**Proof.** From (3.1), we see that

$$
\pi_{a,b,d}(x^iy^j) = (\rho(x^i)\tilde{\beta}^{bi} \rho(y^S(\tilde{v}^{d},j_0)))\tilde{\alpha}^{a,j_0}j_0 \tilde{\delta}^{d,j_0})(1)
$$

$$
= (\rho(x^i)\tilde{\beta}^{bi})(y^{-S(\tilde{v}^{d},j_0)})
$$

$$
= (x^{bp^{m-r}i}y)^{-S(\tilde{v}^{d},j_0)}x^{-i}
$$

$$
= y^{-S(\tilde{v}^{d},j_0)}x^{-bp^{m-r}iS(k,S(\tilde{v}^{d},j_0)))x^{-i},
$$

which simplifies to the desired expression. \[\square\]

**Remark 3.4.** Recall Remarks 1.2 and 2.6. Notice that we may take $j_{0,0,0} = 1$ and $j_{a,1,0} = -1 + p^n$. With these choices, we have

$$
\pi_{0,0,0}(x^iy^j) = x^{-ik-j}y^{-j} = (x^iy^j)^{-1},
$$

$$
\pi_{a,1,0}(x^iy^j) = x^{-i(1+p^{m-r}S(k,(-1+p^n))j)}k^iy^j = x^{-i}y^j,
$$

where $k = 1 + p^{m-r}$ as in Proposition 3.3, and the last equality holds since

$$
1 + p^{m-r}S(k,(-1+p^n)j) = 1 + (k - 1)S(k,(-1+p^n)j) = k^{(-1+p^n)j}.
$$

It is then easy to check that

$$
\rho(x^iy^j) = \pi_{0,0,0}\lambda(x^iy^j)\pi_{0,0,0}^{-1},
$$

$$
\lambda(x^{-i}y^j) = \pi_{a,1,0}\lambda(x^iy^j)\pi_{a,1,0}^{-1}.
$$

This verifies (3.4) in these two special cases.

4. **Counting residue classes of admissible triplets**

In this section, we shall prove Theorem 1.4. First, by Proposition 2.4, we know that the Aut(G)-equivariant antihomomorphisms $\Gamma$ from $G$ to Aut(G) are exactly the $\Gamma_{a,b,d}$ for $(a, b, d)$ ranging over all admissible triplets. Clearly, the definition of $\Gamma_{a,b,d}$ is uniquely determined by the class of $(a, b, d)$ modulo

$$
\mathbb{M} = p^r\mathbb{Z} \times p^r\mathbb{Z} \times p^{\min\{r,n-r\}}\mathbb{Z}
$$

because of (2.4). With Corollaries 1.3 and 3.2, we then deduce that

$$
|T(G)| = \#\{\text{admissible } (a,b,d) \text{ mod } \mathbb{M} \text{ such that (3.3) holds}\}.$$
In the next two subsections, we shall compute this number using Corollaries 2.11 and 2.13, respectively, in the cases that \(m \leq n\) and \(n \leq m - r\). We shall in fact first count the number of admissible triplets \((a, b, d)\) modulo \(\mathbb{M}\), and then explain how imposing the extra restriction \((3.3)\) affects the argument.

Let us first make a change of variables. For any \(a \in \mathbb{Z}\), by \((2.5)\) and Lemma 2.1(a), there exists \(\mu_a \in \mathbb{Z}\) such that

\[
\tilde{u}^a \equiv 1 + \mu_a p^{m-r} \pmod{p^m}, \tag{4.1}
\]

and \(\tilde{u} \pmod{p^m}\) has multiplicative order \(p^r\). We then see that

\[
\mathbb{Z}/p^r\mathbb{Z} \longrightarrow \mathbb{Z}/p^r\mathbb{Z}; \quad a + p^r\mathbb{Z} \mapsto \mu_a + p^r\mathbb{Z}
\]

is a well-defined bijection. With this notation, we have

\[
\tilde{u}^a(1 + (1-b)p^{m-r}) \equiv 1 + (1 + \mu_a - b)p^{m-r} \pmod{p^{m-r+1}}.
\]

This implies that \((3.3)\) holds if and only if

\[
1 + \mu_a - b \not\equiv 0 \pmod{p}, \tag{4.2}
\]

which is much easier to work with.

4.1. The case \(m \leq n\). In this subsection, assume that \(m \leq n\). Recall from Corollary 2.11 that a triplet \((a, b, d)\) is admissible if and only if

\[
\tilde{u}^{-a}\tilde{v}^d \equiv 1 + bp^{m-r} \pmod{p^m} \tag{4.3}
\]

\[
b \equiv 0 \text{ or } 1 \pmod{p^{\max\{2r-m,0\}}} \tag{4.4}
\]

are satisfied. Our strategy is to first choose \(b\) satisfying \((4.4)\), and then pick \(a\) such that \((4.3)\) has a solution in \(d\).

**Proposition 4.1.** The number of admissible triplets modulo \(\mathbb{M}\) is equal to

\[
\begin{cases} 
2p^{m-r+\min\{r,n-r\}} & \text{if } m - r < r, \\
p^{r+\min\{r,n-r\}} & \text{if } r \leq m - r.
\end{cases}
\]

**Proof.** Let us first use \((4.1)\) to rewrite \((4.3)\) as

\[
\tilde{v}^d \equiv 1 + (\mu_a + b)p^{m-r} + \mu_a bp^{2(m-r)} \pmod{p^m}.
\]
We then see that (4.3) has a solution in \(d\) if and only if
\[
(\mu_a + b)p^{m-r} + \mu_a bp^{2(m-r)} \equiv 0 \pmod{p^{\min\{m,\max\{r,n-r\}\}}}
\]
because \(p^{\max\{r,n-r\}} \parallel \tilde{\nu} - 1\) by (2.5). The above is equivalent to
\[
\mu_a \equiv -b(1 + bp^{m-r})^{-1} \pmod{p^{\min\{r,\max\{r,n-r\}-(m-r)\}}}.
\]
This means that once \(b\) is fixed, we have
\[
p^{r-\min\{r,\max\{r,n-r\}-(m-r)\}} = p^{\max\{m-\max\{r,n-r\},0\}}
\]
choices for \(\mu_a\) and thus \(a\) modulo \(p^r\). Note that \(\tilde{\nu} \mod p^m\) has multiplicative order \(p^{\max\{m-\max\{r,n-r\},0\}}\) by Lemma 2.1(a). Hence, once both \(b\) and \(\mu_a\) have been chosen, we have
\[
p^{\min\{r,n-r\}-\max\{m-\max\{r,n-r\},0\}} = p^{\min\{r,n-m\}}
\]
choices for \(d\) modulo \(p^{\min\{r,n-r\}}\mathbb{Z}\). Since there are
\[
\begin{cases}
2p^{m-r} & \text{if } m - r < r \\
p^r & \text{if } r \leq m - r
\end{cases}
\]
choices for \(b\) modulo \(p^r\) which satisfy (4.4), and
\[
p^{\max\{m-\max\{r,n-r\},0\}} \cdot p^{\min\{r,n-m\}} = p^{\min\{r,n-r\}},
\]
the total number of admissible triplets \((a, b, d)\) modulo \(\mathbb{M}\) is as claimed. \(\square\)

The case \(r \leq m - r\) may actually proven via a different and much simpler argument, as follows.

**Proposition 4.2.** The number of admissible triplets modulo \(\mathbb{M}\) is equal to
\[
p^{r+\min\{r,n-r\}} \quad \text{if } r \leq m - r.
\]

**Proof.** Notice that by (2.5), the left hand side of (4.3) is always congruent to 1 modulo \(p^{m-r}\). This means that given any choices of \(a\) and \(d\), there exists \(b\), which is unique modulo \(p^r\), for which (4.3) holds. If \(r \leq m - r\), then (4.4) is vacuous, so there is no other restriction on \(b\), whence we have
\[
p^r \cdot 1 \cdot p^{\min\{r,n-r\}}
\]
admissible triplets \((a, b, d)\) modulo \(\mathbb{M}\), as claimed. □

We now take condition (3.3) into account. We consider the three cases:

(1) \(m - r < r\);
(2) \(r \leq m - r\) and \(m < n\);
(3) \(r \leq m - r\) and \(m = n\).

On the one hand, cases (1) and (2) may be treated using the proof of Proposition 4.1, except that the number of the choices for \(b\) modulo \(p^r\) might need to be adjusted to make sure that (3.3) is satisfied. On the other hand, case (3) may similarly be dealt with using the proof of Proposition 4.2, except we must pick \(a\) and \(d\) suitably so that (3.3) holds.

**Proof of Theorem 1.4 when \(m \leq n\): Cases (1) and (2).** Observe that

\[
m - r + 1 \leq r \leq \max\{r, n - r\}
\]

\[
m - r + 1 \leq n - r = \max\{r, n - r\}
\]

in cases (1) and (2), respectively. We then see from (2.5) that

\[
\tilde{v} \equiv 1 \pmod{p^{m-r+1}}.
\]

Hence, the condition (4.3) implies

\[
1 \equiv 1 + (\mu_a + b)p^{m-r} \pmod{p^{m-r+1}}, \text{ namely } \mu_a \equiv -b \pmod{p}.
\]

So by (4.2), an admissible triplet \((a, b, d)\) satisfies (3.3) exactly when

\[
1 - 2b \not\equiv 0 \pmod{p}.
\]

In case (1), this is satisfied by every admissible triplet \((a, b, d)\) by (4.4), and so we deduce from Proposition 4.1 that

\[
|T(G)| = 2p^{m-r} \cdot p^{{\min}\{r, n-r\}}.
\]

In case (2), the condition (4.4) is vacuous, and requiring \(1 - 2b \not\equiv 0 \pmod{p}\) means that instead of \(p^r\), we only have \((p - 1)p^{r-1}\) choices for \(b\) modulo \(p^r\). The same argument in Proposition 4.1 then gives us

\[
|T(G)| = (p - 1)p^{r-1} \cdot p^{{\min}\{r, n-r\}}.
\]
This proves the theorem when \( m \leq n \) in cases (1) and (2). \( \square \)

**Proof of Theorem 1.4 when \( m \leq n \): Case (3).** Let us make a change of variables for \( d \) analogous to (4.1). Note that \( \max\{r, n - r\} = m - r \) in this case.

For any \( d \in \mathbb{Z} \), by (2.5) and Lemma 2.1(a), there exists \( \nu_d \in \mathbb{Z} \) such that

\[
\tilde{v}^d \equiv 1 + \nu_d p^{m-r} \pmod{p^m},
\]

and \( \tilde{v} \pmod{p^m} \) has multiplicative order \( p^r \). It follows that

\[
\mathbb{Z}/p^r\mathbb{Z} \longrightarrow \mathbb{Z}/p^r\mathbb{Z}; \quad d + p^r\mathbb{Z} 
\rightarrow \nu_d + p^r\mathbb{Z}
\]

is a well-defined bijection. Observe that then (4.3) implies

\[
bp^{m-r} \equiv (\nu_d - \mu_a)p^{m-r} \pmod{p^{m-r+1}}, \text{ namely } b \equiv \nu_d - \mu_a \pmod{p}.
\]

So by (4.2), an admissible triplet \((a, b, d)\) satisfies (3.3) if and only if

\[
1 + 2\mu_a - \nu_d \not\equiv 0 \pmod{p}.
\]

This means that we cannot pick both \( a \) and \( d \) arbitrarily anymore. Instead, once we pick \( a \), we only have \((p - 1)p^{r-1}\) choices for \( d \) modulo \( p^r \). From the same argument in Proposition 4.2, we then see that

\[
|T(G)| = p^r \cdot 1 \cdot (p - 1)p^{r-1}.
\]

This proves the theorem when \( m \leq n \) in case (3). \( \square \)

4.2. **The case** \( n \leq m - r \). In this subsection, assume that \( n \leq m - r \). From Corollary 2.13, we know that a triplet \((a, b, d)\) is admissible if and only if

\[
\tilde{u}^a(1 + bp^{m-r}) \equiv 1 \pmod{p^m} \tag{4.5}
\]

\[
\tilde{v}^d \equiv 1 \pmod{p^n} \tag{4.6}
\]

are satisfied. Hence, we simply have to pick \((a, b)\) and \( d \) such that (4.5) and (4.6) are satisfied, respectively.

**Proposition 4.3.** The number of admissible triplet modulo \( \mathfrak{M} \) is equal to \( p^r \).

**Proof.** By (2.5) and Lemma 2.1(a), we know that

\[
|\tilde{u} \pmod{p^m}| = p^r \text{ and } |\tilde{v} \pmod{p^n}| = p^{\min\{r, n-r\}}.
\]
The latter implies that there is only one choice, namely the zero element, for $d \bmod p^\min\{r,n-r\} \mathbb{Z}$ such that (4.6) holds. The former implies that $b$ may be chosen arbitrarily, and then $a \bmod p^r$ is uniquely determined by (4.5). Thus, indeed we have $1 \cdot p^r \cdot 1$ admissible triplets $(a,b,d)$ modulo $\mathbb{M}$. 

Proof of Theorem 1.4 when $n \leq m - r$. The argument is very similar to that on p. 20. The condition (4.5) implies that

$$1 + (\mu_a + b)p^{m-r} \equiv 1 \pmod{p^{m-r+1}},$$

namely $\mu_a \equiv -b \pmod{p}$. So by (4.2), an admissible triplet $(a,b,d)$ satisfies (3.3) exactly when

$$1 - 2b \not\equiv 0 \pmod{p}.$$ 

This means that instead of $p^r$, we only have $(p - 1)p^{r-1}$ choices for $b \bmod p^r$. By the same argument in Proposition 4.3, we then obtain

$$|T(G)| = (p - 1)p^{r-1}.$$ 

This proves the theorem when $n \leq m - r$. 

□

5. Elements in the multiple holomorph

In [4] and [12], two different methods of constructing elements in the multiple holomorph were given. In this section, let us recall these constructions, and compare them with the $\pi_{a,b,d}$ calculated in Proposition 3.3. It shall also be helpful to recall the definition of $\mathbb{M}$ in Section 4.

First, consider a finite $p$-group $P$. For any $\ell \in \mathbb{Z}$ coprime to $p$, the map

$$\pi_\ell : P \longrightarrow P; \quad \pi_\ell(\sigma) = \sigma^\ell$$

is a bijection. Of course $\pi_\ell$ need not lie in $\text{NHol}(P)$, and so $\pi_\ell\text{Hol}(P)$ might not be an element of $T(P)$ in general. Nonetheless, in [4, Proposition 3.1], it was shown that if $P$ has nilpotency class 2, then

$$\{\pi_\ell\text{Hol}(P) : \ell \in \mathbb{Z} \text{ coprime to } p\} \simeq (\mathbb{Z}/p^e\mathbb{Z})^\times$$

is a cyclic subgroup of $T(P)$ whose order is given by

$$(p - 1)p^{e-1}, \text{ where } \exp(P/Z(P)) = p^e$$
is the exponent of $P/Z(P)$ and $Z(P)$ denotes the center of $P$.

**Lemma 5.1.** We have $Z(G) = \langle x^p, y^p \rangle$ and so $\exp(G/Z(G)) = p^r$.

**Proof.** For any $i, j \in \mathbb{Z}$, we have

$$ (x^iy^j)x(x^iy^j)^{-1}x^{-1} = x^{(1+p^{m-r}j)i}, $$

$$ (x^iy^j)y(x^iy^j)^{-1}y^{-1} = x^{-p^{m-r}i}. $$

Since $1 + p^{m-r} \mod p^m$ has order $p^r$ by Lemma 2.1(a), we see that $x^iy^j$ lies in the center of $G$ if and only if $i, j \equiv 0 \pmod{p^r}$, whence the claims. \qed

**Lemma 5.2.** If $r \leq m - r$, then $G$ has nilpotency class 2.

**Proof.** For any $i_1, i_2, j_1, j_2 \in \mathbb{Z}$, we have

$$ (x^{i_1}y^{j_1})(x^{i_2}y^{j_2})(x^{i_1}y^{j_1})^{-1}(x^{i_2}y^{j_2})^{-1} = x^{i_1(1-(1+p^{m-r}j_2)}-i_2(1-(1+p^{m-r}j_1)). $$

Clearly the exponent is divisible by $p^{m-r}$. We then see from Lemma 5.1 that every commutator lies in $Z(G)$ if $r \leq m - r$, and this implies the claim. \qed

Lemmas 5.1 and 5.2, together with [4], then show that the power maps $\pi_\ell$ define a cyclic subgroup of order $(p - 1)p^{r-1}$ in $T(G)$ when $r \leq m - r$. Note that by Theorem 1.4, this means that

$$ T(G) = \{\pi_\ell \text{Hol}(G) : \ell \in \mathbb{Z} \text{ coprime to } p\} $$

when $n \leq m - r$. Let us now show that these $\pi_\ell$ correspond precisely to the admissible triplets $(a, b, 0)$, namely those with $d \equiv 0 \pmod{p^{\min\{r, n-r\}}}$ (satisfying (3.3) so that $N_{G_{a,b,0}}$ is isomorphic to $G$), in the cases $m \leq n$ with $r \leq m - r$, or $n \leq m - r$.

**Proposition 5.3.** If $m \leq n$ with $r \leq m - r$, or $n \leq m - r$, then the number of admissible triplets $(a, b, 0)$ modulo $M$ satisfying (3.3) is equal to $(p - 1)p^{r-1}$, and all such $(a, b, 0)$ satisfies

$$ \pi_{a,b,0} \equiv \pi_{-a,b,0} \pmod{\text{Aut}(G)}, $$

where $j_{a,b,0}$ is defined as in (3.2).
Proof. Suppose that \( m \leq n \) with \( r \leq m - r \), or \( n \leq m - r \). The first claim essentially follows from the proof of Theorem 1.4: with the restriction (3.3) we only have \((p - 1)p^{r-1}\) choices for \(b\) modulo \(p^r\), and once \(b\) is chosen \(a\) modulo \(p^r\) is uniquely determined by (4.3) or (4.5).

For any admissible triplet \((a, b, 0)\) satisfying (3.3), let us write \(j_{a,b} = j_{a,b,0}\) and \(\ell_{a,b} = -j_{a,b,0}\). On the one hand, observe that
\[
\pi_{\ell_{a,b}}(x^i y^j) = x^{i S((1+p^{m-r})j_{a,b},\ell_{a,b})} y^{j_{a,b}} = x^{i S(1+jp^{m-r},\ell_{a,b})} y^{j_{a,b}} = x^{i(\ell_{a,b}+\frac{j}{2}\ell_{a,b}(\ell_{a,b}-1)jp^{m-r})} y^{j_{a,b}}
\]
by Lemma 2.12. On the other hand, since \(j_{a,b}\) is coprime to \(p\), there exists \(\varphi\) which is a power of \(\alpha\) such that \(\varphi(x) = x^{-\ell_{a,b}}\) and \(\varphi(y) = y\). By Proposition 3.3 and Lemma 2.12, together with \(r \leq m - r\), we then see that
\[
(\varphi \circ \pi_{a,b,0})(x^i y^j) = \varphi(x^{-i(1+jp^{m-r}S(1+p^{m-r}j_{a,b}))}) y^{-j_{a,b}} = \varphi(x^{-i(1+j_{a,b}jbp^{m-r})(1+\ell_{a,b}jp^{m-r})}) y^{j_{a,b}} = \varphi(x^{-i(1+\ell_{a,b}jp^{m-r}(1-b))}) y^{j_{a,b}} = x^{i(\ell_{a,b}+\ell_{a,b}(1-b)jp^{m-r})} y^{j_{a,b}}.
\]
Recall the notation in (4.1). Then, from (4.3) or (4.5), we deduce that
\[
(1 + \mu_a p^{m-r})(1 + bp^{m-r}) \equiv 1 \pmod{p^m}, \text{ namely } \mu_a \equiv -b \pmod{p^r}.
\]
Also, by Lemma 2.12 and \(r \leq m - r\), we see that
\[
(\tilde{u}^a(1 + (1 - b)p^{m-r}))^{j_{a,b}} \equiv (1 + j_{a,b} \mu_a p^{m-r})(1 + j_{a,b}(1 - b)p^{m-r}) \pmod{p^m}
\equiv 1 + j_{a,b}(1 + \mu_a - b)p^{m-r} \pmod{p^m}
\equiv 1 + j_{a,b}(1 - 2b)p^{m-r} \pmod{p^m}.
\]
By the definition (3.2), this implies that
\[
j_{a,b}(1 - 2b)p^{m-r} \equiv p^{m-r} \pmod{p^m}.
\]
It then follows that
\[
2\ell_{a,b}^2(1 - b)p^{m-r} \equiv \ell_{a,b}^2(1 - 2b)p^{m-r} + \ell_{a,b}^2p^{m-r} \pmod{p^m} \\
\equiv -\ell_{a,b}p^{m-r} + \ell_{a,b}^2p^{m-r} \pmod{p^m} \\
\equiv \ell_{a,b}(\ell_{a,b} - 1)p^{m-r} \pmod{p^m}.
\]
We have thus shown that \( \varphi \circ \pi_{a,b,0} = \pi_{a,b} \), whence the claim. \( \square \)

Next, consider a group which is a semidirect product \( Q = A \rtimes \langle y \rangle \), where \( A \) is any group and \( y \) is the generator of order \( p^n \) in \( G \). For any \( v \in \mathbb{Z} \) with \( v \equiv 1 \pmod{p} \), in [12] the present author showed that we have a bijection defined by
\[
\pi'_v : Q \to Q; \quad \pi'_v((a, y^j)) = (a, y^{S(v,j)}) \text{ for all } a \in A \text{ and } j \in \mathbb{N}_{\geq 0}.
\]
Again \( \pi'_v \) might not lie in \( \text{NHol}(Q) \). But in [12], it was proven that \( \pi'_v \) lies in \( \text{NHol}(Q) \) and the order of \( \pi'_v \text{Hol}(Q) \) in \( T(Q) \) is a power of \( p \), under suitable hypotheses, one of which is that the exponent of \( A \) is coprime to \( p \). For our group \( G \) in (1.1), where \( A \) is the cyclic group of order \( p^m \), this hypothesis is of course never satisfied. Nevertheless, up to the inversion map
\[
\iota : G \to G; \quad \iota(x^iy^j) = (x^iy^j)^{-1},
\]
some of the bijections \( \pi_{a,b,d} \) do arise in this way when \( m \leq n \).

**Proposition 5.4.** If \( m \leq n \), then the number of admissible triplets \((a, 0, d)\) modulo \( M \) with \( \tilde{v}^d \equiv 1 \pmod{p^m} \) is equal to \( p^\min\{r,n-m\} \), and all such \((a, 0, d)\) satisfy (3.3) as well as the congruence
\[
\iota \circ \pi_{a,0,d} \equiv \pi'_{\tilde{v}^d} \pmod{\text{Aut}(G)}.
\]

**Proof.** Suppose that \( m \leq n \). Note that \( \tilde{v}^d \equiv 1 \pmod{p^m} \) is equivalent to
\[
d \equiv 0 \pmod{p^{\max\{m-\max\{r,n-r\},0\}}}
\]
by (2.5) and Lemma 2.1(a). Hence, we have
\[
p^{\min\{r,n-r\}-\max\{m-\max\{r,n-r\},0\}} = p^{\min\{r,n-m\}}
\]
choices for $d$ modulo $p^\min\{r,n-r\}$. A triplet $(a,0,d)$ with $\bar{v}^d \equiv 1 \pmod{p^n}$ is admissible exactly when $\bar{u}^a \equiv 1 \pmod{p^n}$ by Corollary 2.11. Thus, by (2.5), there is only one choice for $a$ modulo $p^r$, namely the zero element, and this proves the first claim.

For any admissible triplet $(a,0,d)$ with $\bar{v}^d \equiv 1 \pmod{p^m}$, we have

$$\bar{u}^a(1+(1-0)p^{m-r}) \equiv 1(1+p^{m-r}) \equiv 1+p^{m-r} \pmod{p^m}$$

and so (3.3) always holds. This also implies that we may take $j_{a,0,d} = 1$ for the $j_{a,0,d}$ defined in (3.2). With this choice, by Proposition 3.3, we have

$$(\iota \circ \pi_{a,0,d})(x^iy^j) = \left(x^{-i(1+p^{m-r})-S(\bar{v}^d,j)}y^{-S(\bar{v}^d,j)}\right)^{-1}$$

$$= y^{S(\bar{v}^d,j)}x^{i(1+p^{m-r})-S(\bar{v}^d,j)}y^{-S(\bar{v}^d,j)}y^{S(\bar{v}^d,j)}$$

$$= x^iy^{S(\bar{v}^d,j)}$$

$$= \pi'_{\bar{v}^d}(x^iy^j).$$

This completes the proof. □

ACKNOWLEDGMENTS

This research was supported by the Fundamental Research Funds for the Central Universities (Award No.: 19lpgy247). The author thanks the referee for helpful comments.

REFERENCES

[1] J. N. S. Bidwell and M. J. Curran, The automorphism group of a split metacyclic $p$-group, Arch. Math. (Basel) 87 (2006), no. 6, 488–497; corrigendum, ibid. 92 (2009), no. 1, 14–18.
[2] A. Caranti and F. Dalla Volta, The multiple holomorph of a finitely generated abelian group, J. Algebra 481 (2017), 327–347.
[3] A. Caranti and F. Dalla Volta, Groups that have the same holomorph as a finite perfect group, J. Algebra 507 (2018), 81–102.
[4] A. Caranti, Multiple holomorphs of finite $p$-groups of class two, J. Algebra 516 (2018), 352–372.
[5] M. J. Curran, The automorphism group of a split metacyclic 2-group, Arch. Math. 89 (2007), 10–23.
[6] B. W. King, Presentations of metacyclic groups, Bull. Austral. Math. Soc. 8 (1973), 103–131.
[7] T. Kohl, Multiple holomorphs of dihedral and quaternionic groups, Comm. Algebra 43 (2015), no. 10, 4290–4304.
[8] W. H. Mills, Multiple holomorphs of finitely generated abelian groups, Trans. Amer. Math. Soc. 71 (1951), 379–392.
[9] G. A. Miller, On the multiple holomorphs of a group, Math. Ann. 66 (1908), no. 1, 133–142.
[10] C. Tsang, *On the multiple holomorph of a finite almost simple group*, New York J. Math. 25 (2019), 949–963.

[11] C. Tsang, *On the multiple holomorph of groups of squarefree or odd prime power order*, J. Algebra 544 (2020), 1–25.

[12] C. Tsang, *The multiple holomorph of a semidirect product of groups having coprime exponents*, Arch. Math. (Basel) 115 (2020), no. 1, 13–21.

**Department of Mathematics, Ochanomizu University, Tokyo, Japan**

*Email address:* tsang.sin.yi@ocha.ac.jp

*URL:* http://sites.google.com/site/cindysinyitsang/