The Classification of Finite Metahamiltonian p-Groups *

Xingui Fang
School of Mathematics Science, Peking University
Beijing, 100087 PR China
Lijian An†
Department of Mathematics, Shanxi Normal University
Linfen, Shanxi, 041004 PR China

Abstract

A finite non-abelian group G is called metahamiltonian if every subgroup of G is either abelian or normal in G. If G is non-nilpotent, then the structure of G has been determined. If G is nilpotent, then the structure of G is determined by the structure of its Sylow subgroups. However, the classification of finite metahamiltonian p-groups is an unsolved problem. In this paper, finite metahamiltonian p-groups are completely classified up to isomorphism.

Keywords minimal non-abelian groups, Hamiltonian groups, metahamiltonian groups, $\mathcal{A}_2$-groups *2000 Mathematics subject classification:* 20D15.

1 Introduction

To determine a finite group by using its subgroup structure is an important theme in the group theory. Let G be a finite non-abelian p-group. If every proper subgroup of G is abelian then G is called *minimal non-abelian*, which was classified by Redei [19]. If every subgroup of G is normal in G then G is called *Hamiltonian*, which was classified by Dedekind [9]. The classifications of minimal non-abelian p-groups and Hamiltonian groups are two classical results in the theory of finite p-groups.

As a generalization of minimal non-abelian group, many authors investigate finite p-groups with many abelian subgroups. Among these works, the classification of $\mathcal{A}_2$-groups is the most important one. A finite non-abelian p-group G is called an $\mathcal{A}_2$-*group* if G is not minimal non-abelian and all of its subgroups of index p are either abelian or minimal non-abelian. Many scholars studied and classified $\mathcal{A}_2$-groups, see [6, 7, 10, 11, 20, 26]. Resent years, several important classes of p-groups which contain $\mathcal{A}_2$-group are determined. For example, Xu et al. [21] classified finite p-groups all of whose non-abelian proper subgroups are generated by two elements. An et al. [1, 2, 16, 17, 18] classified finite p-groups with a minimal non-abelian subgroup of index p. Zhang et al. [27] classified finite p-groups all of its subgroups of index p^3 are abelian.

*This work was supported by NSFC (No. 11471198 & 10171006).
†Corresponding author. e-mail: anlj@sxnu.edu.cn

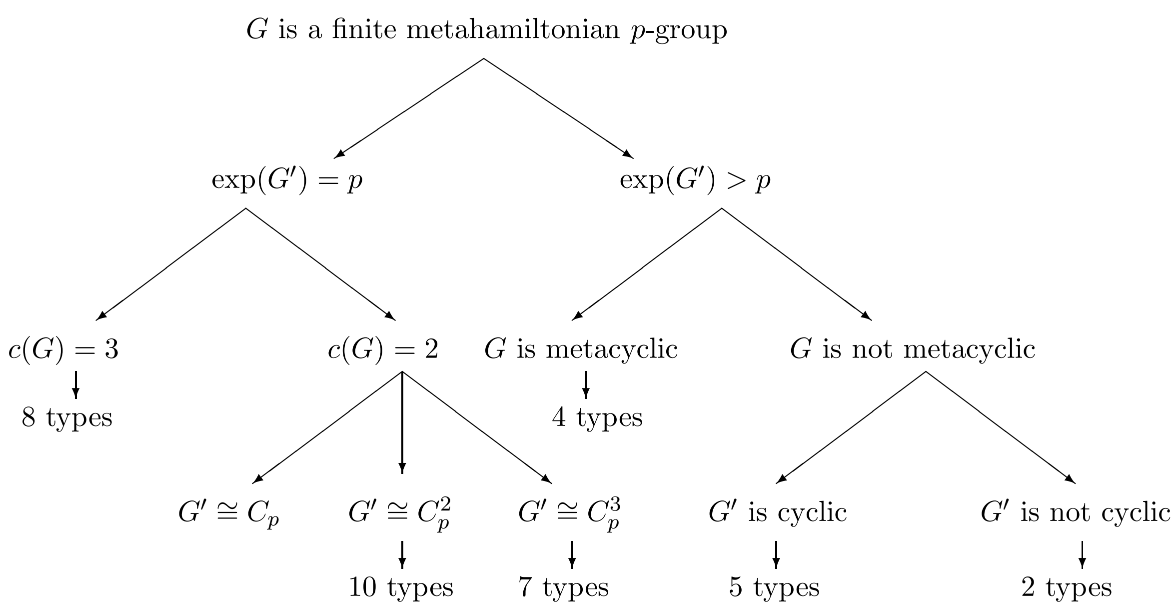
As a generalization of Hamilton groups, many authors investigate finite p-groups with many normal subgroups. For example, Passman [15] classified finite p-groups all of whose non-normal subgroups are cyclic. Zhang et al. [23, 24, 25] classified finite p-groups all of whose non-normal subgroups have orders $\leq p^3$.

A non-abelian group G is called *metahamiltonian* if every proper subgroup of G is either abelian or normal in G. Obviously, $\mathcal{A}_2$-groups are metahamiltonian. Groups in [15, 23] are also metahamiltonian. Thus the class of metahamiltonian p-groups is much larger than that of minimal non-abelian p-groups and Hamilton p-groups. The classification of metahamiltonian p-groups is an old problem. The present paper is devoted to the classification.

By the way, Nagrebeckii [13] determined the structure of finite non-nilpotent metahamiltonian groups. Obviously, a nilpotent group is metahamiltonian if and only if all its Sylow subgroups are metahamiltonian. Hence finite metahamiltonian groups are completely determined.

This paper is divided into four sections. Section 2 is a preliminary. In section 3, we classify finite metahamiltonian p-groups whose derived group is of exponent p, and the case of exponent $> p$ is dealt with in section 4.

The sketch of the classification of metahamiltonian p-groups is as follows.



2 Preliminaries

Let G be a finite p-group. For a positive integer t, G is said to be an *$\mathcal{A}_t$-group* if the greatest index of non-abelian subgroups is p^{t-1}. So $\mathcal{A}_1$-groups are just the minimal non-abelian p-groups.

Let G be a finite p-group. We define

$$\Lambda_m(G) = \{a \in G \mid a^{p^m} = 1\}, \qquad V_m(G) = \{a^{p^m} \mid a \in G\},$$
$$\Omega_m(G) = \langle \Lambda_m(G) \rangle = \langle a \in G \mid a^{p^m} = 1 \rangle, \text{ and } \mho_m(G) = \langle V_m(G) \rangle = \langle a^{p^m} \mid a \in G \rangle.$$

G is called *p-abelian* if $(ab)^p = a^p b^p$ for all $a, b \in G$. We use $c(G)$ and $d(G)$ to denote the nilpotency class and minimal number of generators, respectively.

We use C_n and C_n^m to denote the cyclic group and the direct product of m cyclic groups of order n, respectively. We use $M_p(m,n)$ to denote groups

$$\langle a, b \mid a^{p^m} = b^{p^n} = 1, a^b = a^{1+p^{m-1}} \rangle, \text{ where } m \geq 2,$$

and use $M_p(m,n,1)$ to denote groups

$$\langle a, b, c \mid a^{p^m} = b^{p^n} = c^p = 1, [a,b] = c, [c,a] = [c,b] = 1 \rangle,$$

where $m + n \geq 3$ for $p = 2$ and $m \geq n$. We can give a presentation of minimal non-abelian p-groups as follows:

Theorem 2.1. (See [19]) *Let G be a minimal non-abelian p-group. Then G is Q_8, $M_p(m,n)$, or $M_p(m,n,1)$.*

A finite p-group G is called *metacyclic* if it has a cyclic normal subgroup N such that G/N is also cyclic.

In 1973 King [12] classified metacyclic p-groups. In 1988 Newman and Xu (see [14, 22]) found new presentations for these groups. Theorem 2.2 is quoted from [22].

Theorem 2.2. (1) *Any metacyclic p-group G, p odd, has the following presentation:*

$$G = \langle a, b \mid a^{p^{r+s+u}} = 1,\ b^{p^{r+s+t}} = a^{p^{r+s}},\ a^b = a^{1+p^r} \rangle$$

where $r,\ s,\ t,\ u$ are non-negative integers with $r \geq 1$ and $u \leq r$. Different values of the parameters $r,\ s,\ t$ and u with the above conditions give non-isomorphic metacyclic p-groups. It is denoted to $< r, s, t, u >_p$ in this paper.

(2) *Let G be a metacyclic 2-group. Then G has one of the following three kinds of presentations:*

(I) *G has a cyclic maximal subgroup. Hence G is dihedral, semi-dihedral, generalized quaternion, or an ordinary metacyclic group presented by*

$$G = \langle a, b \mid a^{2^n} = 1, b^2 = 1, a^b = a^{1+2^{n-1}} \rangle.$$

(II) *Ordinary metacyclic 2-groups:*

$$G = \langle a, b \mid a^{2^{r+s+u}} = 1,\ b^{2^{r+s+t}} = a^{2^{r+s}}, a^b = a^{1+2^r} \rangle,$$

where r, s, t, u *are non-negative integers with* $r \geq 2$ *and* $u \leq r$. *It is denoted to be* $< r, s, t, u >_2$ *in this paper.*

(III) *Exceptional metacyclic 2-groups:*

$$G = \langle a, b \mid a^{2^{r+s+v+t'+u}} = 1,\ b^{2^{r+s+t}} = a^{2^{r+s+v+t'}}, a^b = a^{-1+2^{r+v}} \rangle,$$

where r, s, v, t, t', u *are non-negative integers with* $r \geq 2$, $t' \leq r$, $u \leq 1$, $tt' = sv = tv = 0$, *and if* $t' \geq r - 1$ *then* $u = 0$. *Groups of different types or of the same type but with different values of parameters are not isomorphic to each other. It is denoted to be* $< r, s, v, t, t', u >_2$ *in this paper.*

Lemma 2.3. (See [8]) *Suppose that* G *is a finite* p*-group. Then* G *is metacyclic if and only if* $G/\Phi(G')G_3$ *is metacyclic.*

Lemma 2.4. (See [5, Lemma J(i)]) *Let* G *be a metacyclic* p*-group. Then* G *is an* $\mathcal{A}_n$*-group if and only if* $|G'| = p^n$.

In [4], the properties of metahamiltonian p-groups are given as follows:

Theorem 2.5. *Let* G *be a metahamiltonian* p*-group. Then* $c(G) \leq 3$. *In particular,* G *is metabelian.*

Theorem 2.6. *Let* G *be a finite* p*-group.* G *is metahamiltonian if and only if* G' *is contained in every non-abelian subgroup of* G.

Theorem 2.7. *Suppose that* G *is a finite metahamilton* p*-group. If* $d(G) = 2$ *and* $\exp(G') > p$, *then* G *is metacyclic.*

Theorem 2.8. *Suppose that* G *is a finite metahamiltonian* p*-group having an elementary abelian derived group. If* $c(G) = 3$, *then* G *is an* $\mathcal{A}_2$*-group.*

Corollary 2.9. *Suppose that* G *is a finite metahamiltonian* p*-group having an elementary abelian derived group. If* $c(G) = 3$, *then* $d(G) = 2$ *and* p *is odd.*

3 Finite metahamiltonian p-groups whose derived group is of exponent p

In this section, we determine finite metahamiltonian p-groups whose derived group is of exponent p. In order to avoid tedious calculations, we provide a proof which relies on some results obtained in other papers. These papers are [2, 3, 17, 26].

Theorem 3.1. *Suppose that* G *is a finite metahamiltonian* p*-group with* $\exp(G') = p$. *Then* G *is one of the following non-isomorphic groups:*

(A) *groups with* $|G'| = p$.

(B) $c(G) = 3$. *In this case,* p *is odd,* $d(G) = 2$ *and* $G \in \mathcal{A}_2$.

(B1) $\langle a_1, b \mid a_1^p = a_2^p = a_3^p = b^{p^m} = 1, [a_1, b] = a_2, [a_2, b] = a_3, [a_3, b] = 1, [a_i, a_j] = 1\rangle$, *where* $p \geq 5$ *for* $m = 1$, $p \geq 3$ *and* $1 \leq i, j \leq 3$;

(B2) $\langle a_1, b \mid a_1^p = a_2^p = b^{p^{m+1}} = 1, [a_1, b] = a_2, [a_2, b] = b^{p^m}, [a_1, a_2] = 1\rangle$, *where* $p \geq 3$;

(B3) $\langle a_1, b \mid a_1^{p^2} = a_2^p = b^{p^m} = 1, [a_1, b] = a_2, [a_2, b] = a_1^{\nu p}, [a_1, a_2] = 1\rangle$, *where* $p \geq 3$ *and* $\nu = 1$ *or a fixed quadratic non-residue modulo* p;

(B4) $\langle a_1, a_2, b \mid a_1^9 = a_2^3 = 1, b^3 = a_1^3, [a_1, b] = a_2, [a_2, b] = a_1^{-3}, [a_2, a_1] = 1\rangle$.

(B5) $\langle a, b \mid a^{p^2} = b^{p^2} = c^p = 1, [a, b] = c, [c, a] = b^{\nu p}, [c, b] = a^p\rangle$, *where* $p \geq 5$, ν *is a fixed square non-residue modulo* p;

(B6) $\langle a, b \mid a^{p^2} = b^{p^2} = c^p = 1, [a, b] = c, [c, a] = a^{-p}b^{-lp}, [c, b] = a^{-p}\rangle$, *where* $p \geq 5$, $4l = \rho^{2r+1} - 1$, $r = 1, 2, \ldots, \frac{1}{2}(p-1)$, ρ *is the smallest positive integer which is a primitive root modulo* p;

(B7) $\langle a, b \mid a^9 = b^9 = c^3 = 1, [a, b] = c, [c, a] = b^{-3}, [c, b] = a^3\rangle$;

(B8) $\langle a, b \mid a^9 = b^9 = c^3 = 1, [a, b] = c, [c, a] = b^{-3}, [c, b] = a^{-3}\rangle$.

(C) $c(G) = 2$ *and* $G' \cong C_p^2$.

(C1) $K \times A$, *where* $K = \langle a_1, a_2, b \mid a_1^4 = a_2^4 = 1, b^2 = a_1^2, [a_1, a_2] = 1, [a_1, b] = a_2^2, [a_2, b] = a_1^2\rangle$ *and* A *is abelian such that* $\exp(A) \leq 2$;

(C2) $K \times A$, *where* $K = \langle a_1, a_2, b, d \mid a_1^4 = a_2^4 = 1, b^2 = a_1^2, d^2 = a_2^2, [a_1, a_2] = 1, [a_1, b] = a_2^2, [a_2, b] = a_1^2, [a_1, d] = a_1^2, [a_2, d] = a_1^2 a_2^2, [b, d] = 1\rangle$ *and* A *is abelian such that* $\exp(A) \leq 2$.

(C3) $K \times A$, *where* $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3}} = 1, [a_1, a_2] = a_1^{p^{m_1}}, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = 1\rangle$, $m_1 > 1$ *for* $p = 2$, $m_1 \geq m_2 \geq m_3$, *and* A *is abelian such that* $\exp(A) \leq p^{m_2}$;

(C4) $K \times A$, *where* $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3}} = 1, [a_1, a_2] = 1, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = a_1^{\nu p^{m_1}}\rangle$, $p > 2$, ν *is a fixed square non-residue modulo* p, $m_1 - 1 = m_2 \geq m_3$ *or* $m_1 = m_2 \geq m_3$, *and* A *is abelian such that* $\exp(A) \leq p^{m_2}$;

(C5) $K \times A$, *where* $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3}} = 1, [a_1, a_2] = 1, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = a_1^{kp^{m_1}} a_2^{-p^{m_2}}\rangle$, $1 + 4k \notin (F_p)^2$ *for* $p > 2$, $k = 1$ *for* $p = 2$, $m_1 = m_2 \geq m_3$ *and* A *is abelian such that* $\exp(A) \leq p^{m_2}$;

(C6) $K \times A$, *where* $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3}} = 1, [a_1, a_2] = 1, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = a_1^{p^{m_1}}\rangle$, $m_1 - 1 = m_2 \geq m_3$ *and* A *is abelian such that* $\exp(A) \leq p^{m_2}$;

(C7) $K \times A$, *where* $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = 1\rangle$, $m_1 \geq m_2 = m_3 + 1$ *and* A *is abelian such that* $\exp(A) \leq p^{m_3}$;

(C8) $K \times A$, *where* $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_2^{\nu p^{m_2}}, [a_2, a_3] = 1\rangle$, $p > 2$, ν *is a fixed square non-residue modulo* p, $m_1 \geq m_2 = m_3 + 1$ *or* $m_1 > m_2 = m_3$ *and* A *is abelian such that* $\exp(A) \leq p^{m_3}$;

(C9) $K \times A$, *where* $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_2^{kp^{m_2}} a_3^{-p^{m_3}}, [a_2, a_3] = 1\rangle$, $1 + 4k \notin (F_p)^2$ *for* $p > 2$, $k = 1$ *for* $p = 2$, $m_1 > m_2 = m_3$ *and* A *is abelian such that* $\exp(A) \leq p^{m_3}$;

(C10) $K \times A$, *where* $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2}} = a_3^{p^{m_3+1}} = 1, [a_1, a_2] = a_3^{p^{m_3}}, [a_1, a_3] = a_1^{p^{m_1}}, [a_2, a_3] = 1\rangle$, $m_1 \geq m_2 = m_3 + 1$ *and* A *is abelian such that* $\exp(A) \leq p^{m_3}$.

(D) $c(G) = 2$ *and* $G' \cong C_p^3$.

(D1) $K \times A$, *where* $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_2, a_3] = a_1^{p^{m_1}}, [a_1, a_3] = a_2^{\eta p^{m_2}}, [a_1, a_2] = a_3^{p^{m_3}}, [a_3^p, a_1] = [a_3^p, a_2] = 1\rangle$, *where* p *is odd,* $m_1 = m_2 + 1 = m_3 + 1$ *and* η *is a fixed square non-residue modulo* p, *and* A *is abelian with* $\exp(A) \leq p^{m_3}$;

(D2) $K \times A$, *where* $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_2, a_3] = a_1^{p^{m_1}}, [a_1, a_3] = a_2^{lp^{m_2}} a_3^{-p^{m_2}}, [a_1, a_2] = a_3^{p^{m_3}}, [a_3^p, a_1] = [a_3^p, a_2] = 1\rangle$, *where* p *is odd,* $m_1 = m_2 + 1 = m_3 + 1$ *and* $1 + 4l \notin (F_p)^2$, *and* A *is abelian with* $\exp(A) \leq p^{m_3}$;

(D3) $K \times A$, *where* $K = \langle a_1, a_2, a_3 \mid a_1^{2^{m_1+1}} = a_2^{2^{m_2+1}} = a_3^{2^{m_3+1}} = 1, [a_2, a_3] = a_1^{2^{m_1}}, [a_3, a_1] = a_2^{2^{m_2}}, [a_1, a_2] = a_2^{2^{m_2}} a_3^{2^{m_3}}, [a_3^2, a_1] = [a_3^2, a_2] = 1\rangle$, *where* $m_1 = m_2 + 1 = m_3 + 1$, *and* A *is abelian with* $\exp(A) \leq 2^{m_3}$;

(D4) $K \times A$, *where* $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_2, a_3] = a_1^{p^{m_1}}, [a_1, a_3] = a_2^{\eta p^{m_2}}, [a_1, a_2] = a_3^{p^{m_3}}, [a_3^p, a_1] = [a_3^p, a_2] = 1\rangle$, *where* p *is odd,* $m_1 = m_2 = m_3 + 1$ *and* η *is a fixed square non-residue modulo* p, *and* A *is abelian with* $\exp(A) \leq p^{m_3}$;

(D5) $K \times A$, *where* $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3+1}} = 1, [a_2, a_3] = a_1^{p^{m_1}}, [a_1, a_3] = a_1^{p^{m_1}} a_2^{lp^{m_2}}, [a_1, a_2] = a_3^{p^{m_3}}, [a_3^p, a_1] = [a_3^p, a_2] = 1\rangle$, *where* p *is odd,* $m_1 = m_2 = m_3 + 1$ *and* $1 + 4l \notin (F_p)^2$, *and* A *is abelian with* $\exp(A) \leq p^{m_3}$;

(D6) $K \times A$, *where* $K = \langle a_1, a_2, a_3 \mid a_1^{2^{m_1+1}} = a_2^{2^{m_2+1}} = a_3^{2^{m_3+1}} = 1, [a_2, a_3] = a_1^{2^{m_1}} a_2^{2^{m_2}}, [a_3, a_1] = a_2^{2^{m_2}}, [a_1, a_2] = a_3^{2^{m_3}}, [a_3^2, a_1] = [a_3^2, a_2] = 1\rangle$, *where* $m_1 = m_2 = m_3 + 1$, *and* A *is abelian with* $\exp(A) \leq 2^{m_3}$;

(D7) $K\times A$, *where* $K=\langle a,b,c \mid a^4=b^4=c^4=1,[b,c]=a^2b^2,[c,a]=b^2c^2,[a,b]=c^2,[c^2,a]=[c^2,b]=1\rangle$, *and* A *is abelian with* $\exp(A)\le 2$.

Proof By Theorem 2.5, $c(G)\le 3$. If $c(G)=3$, then, by Theorem 2.8, $G\in\mathcal{A}_2$. Checking groups listed in [4, Lemma 2.4], we get groups (B1)–(B8). In the following, we may assume that $c(G)=2$. Let N be a minimal non-abelian subgroup of G. By Theorem 2.6, $G'\le N$. Since $G'\le Z(G)$, $G'\le \Omega_1(Z(N))=\Omega_1(\Phi(N))$. It follows from Theorem 2.1 that $G'\le C_p^3$. If $G'\cong C_p$, then G is of Type (A) in the theorem. If $G'\cong C_p^2$, then, by the following Lemma 3.2, G is a group of Type (C1)–(C10) in the theorem. For the case of $G'\cong C_p^3$, Lemma 3.3 gives groups of Type (D1)–(D5) in the theorem. Finally, it is omitted to check that such groups are non-isomorphic metahamiltonian p-groups. □

Lemma 3.2. *Suppose that G is a metahamilton p-group. If $G'\cong C_p^2$ and $c(G)=2$, then G is a group of Type* (C1)–(C10) *as defined in Theorem* 3.1.

Proof Let the type of G/G' be $(p^{m_1},p^{m_2},\dots,p^{m_r})$, where $m_1\ge m_2\ge\cdots\ge m_r$. Let

$$G/G'=\langle a_1G'\rangle\times\langle a_2G'\rangle\times\cdots\times\langle a_rG'\rangle,\text{ where } o(a_iG')=p^{m_i},\ i=1,2,\dots,r.$$

Then $G=\langle a_1,a_2,\dots,a_r\rangle$.

If $m_1=1$, then G/G' is elementary abelian. By Theorem 2.6, $G'\le\langle x,y\rangle$ for every non-commutative pair $x,y\in G$ and hence $\langle x,y\rangle$ is minimal non-abelian with order p^4. Such groups were classified in [3]. By checking the results in [3], we get the groups (C3)–(C5) where $m_1=m_2=m_3=1$ and (C1)–(C2). In the following, we may assume that $m_1>1$.

Let i be the minimal integer such that $a_i\notin Z(G)$. That is, there exists $j>i$ such that $[a_i,a_j]\ne 1$. If $i\ne 1$, then $a_1\in Z(G)$. Replacing a_1 with a_1a_j, we get $a_1\notin Z(G)$. If $i=1$, then we also have $a_1\notin Z(G)$.

Let j be the minimal integer such that $[a_1,a_j]\ne 1$. If $j\ne 2$, then $[a_1,a_2]=1$. Replacing a_2 with a_2a_j, we get $[a_1,a_2]\ne 1$. If $j=2$, then we also have $[a_1,a_2]\ne 1$.

Let k be the minimal integer such that $[a_k,a_l]\notin\langle[a_1,a_2]\rangle$. If $k>2$, then, for all integer s, we have

$$[a_1,a_s]\in\langle[a_1,a_2]\rangle \text{ and } [a_2,a_s]\in\langle[a_1,a_2]\rangle.$$

(1) If $[a_1,a_l]=1$, then, replacing a_2 with a_2a_l, we have $[a_2,a_k]\notin\langle[a_1,a_2]\rangle$. (2) If $[a_1,a_l]=[a_1,a_2]^\alpha$ where $(\alpha,p)=1$, then, letting $[a_1,a_k]=[a_1,a_2]^\beta$ and replacing a_2 with $a_2a_ka_l^{\alpha^{-1}\beta}$, we have $[a_2,a_l]\notin\langle[a_1,a_2]\rangle$. Hence we may assume that $k\le 2$.

Let l be the minimal integer such that $[a_k,a_l]\notin\langle[a_1,a_2]\rangle$. If $l\ne 3$, then $[a_1,a_3]\in\langle[a_1,a_2]\rangle$ and $[a_2,a_3]\in\langle[a_1,a_2]\rangle$. Replacing a_3 with a_3a_l, we have $[a_k,a_3]\notin\langle[a_1,a_2]\rangle$. Hence we may assume that $l=3$.

Let $K = \langle a_1, a_2, a_3\rangle$. Then $|K'| = |G'| = p^2$. Such groups K were determined in [2]. By checking [2, Table 4], K is one of the groups (C3)–(C10) in Theorem 3.1. If $r = 3$, then $G = K$. In the following we may assume that $r \geq 4$.

Case 1: K is one of the groups of Type (C3)–(C6) in Theorem 3.1.

In this case, $G' = \langle a_1^{p^{m_1}}, a_2^{p^{m_2}}\rangle$ and $[a_1, a_3] = a_2^{p^{m_2}}$. Assume that $a_4^{p^{m_4}} = a_1^{\alpha p^{m_1}} a_2^{\beta p^{m_2}}$. Replacing a_4 with $a_4 a_1^{-\alpha p^{m_1 - m_4}}$, we have $a_4^{p^{m_4}} = a_2^{\beta p^{m_2}}$ since $m_1 > 1$.

If $p > 2$ or $m_2 > 1$, then, replacing a_4 with $a_4 a_2^{-\beta p^{m_2 - m_4}}$, we have $a_4^{p^{m_4}} = 1$. If $p = 2$ and $m_2 = 1$, then we claim that there exists an $x \in \{a_4, a_4 a_2\}$ such that $x^2 \in \langle a_1^{2^{m_1}}\rangle$. Otherwise, $a_4^2 = a_2^2$. Since $[a_4, a_2] = (a_4 a_2)^2 \notin \langle a_1^{2^{m_1}}\rangle$, $\langle a_4, a_2\rangle$ is not abelian. It follows from Theorem 2.6 that $a_1^{2^{m_1}} \in \langle a_4, a_2\rangle$. Hence $[a_4, a_2] = a_1^{2^{m_1}} a_2^2$. Thus $\langle a_4 a_2, a_2 a_1^{2^{m_1 - 1}}\rangle$ is neither abelian nor normal in G, a contradiction. Replacing a_4 with x or $x a_1^{2^{m_1 - 1}}$, we have $a_4^2 = 1$.

Hence we may assume that $a_4^{p^{m_4}} = 1$. We claim that $[a_1, a_4] \in \langle a_2^{p^{m_2}}\rangle$. Otherwise, we may assume that $[a_1, a_4] = a_1^{\gamma p^{m_1}} a_2^{\alpha p^{m_2}}$ where $(\gamma, p) = 1$. By calculation, $\langle a_1, a_4 a_3^{-\alpha}\rangle$ is neither abelian nor normal in G, a contradiction. Hence $[a_1, a_4] \in \langle a_2^{p^{m_2}}\rangle$.

Let $L = \langle a_1, a_2, a_4\rangle$. If $[a_1, a_4] \neq 1$, then, by suitable replacement, we may assume that $[a_1, a_4] = a_2^{p^{m_2}}$. In this case, we claim that $L' = G'$. If not, then $L' = \langle a_2^{p^{m_2}}\rangle$. Since $G' \not\leq \langle a_2, a_4\rangle$, $[a_2, a_4] = 1$ by Theorem 2.6. Since $K' = G'$, $K' = \langle a_2^{p^{m_2}}, [a_2, a_3]\rangle$. Hence we may assume that $[a_2, a_3] = a_1^{sp^{m_1}} a_2^{tp^{m_2}}$ where $(s, p) = 1$. If $(t, p) = 1$, then $\langle a_1^{sp^{m_1 - m_2}} a_2^t, a_3 a_4^{-1}\rangle$ is neither abelian nor normal in G, a contradiction. If $t = 0$ and $m_1 > m_2$, then $\langle a_1 a_2, a_3 a_4^{-1}\rangle$ is neither abelian nor normal in G, a contradiction. If $t = 0$ and $m_1 = m_2$, then $\langle a_1 a_2, a_3 a_4^{s-1}\rangle$ is neither abelian nor normal in G, also a contradiction.

By a similar argument as above, for $4 \leq i \leq r$, we may assume that $a_i^{p^{m_i}} = 1$ and $[a_1, a_i] = 1$ or $a_2^{p^{m_2}}$. Moreover, we have:

$$(*)\quad \text{If } [a_1, a_i] = a_2^{p^{m_2}}, \text{ then } L' = G' \text{ where } L = \langle a_1, a_2, a_i\rangle.$$

For $3 \leq i < j \leq r$, $[a_i, a_j] = 1$ by Theorem 2.6.

Let j be the maximal integer such that $[a_1, a_j] = a_2^{p^{m_2}}$. Then $[a_1, a_k] = 1$ for $j < k \leq r$. For $3 \leq k < j$, if $[a_1, a_k] = a_2^{p^{m_2}}$, then $[a_1, a_k a_j^{-1}] = 1$. Replacing a_k with $a_k a_j^{-1}$ if necessary, we get $[a_1, a_k] = 1$.

Let $J = \langle a_1, a_2, a_j\rangle$. Then J is one of the groups of Type (C3)–(C6) in Theorem 3.1 since $J' = \langle a_1^{p^{m_1}}, a_2^{p^{m_2}}\rangle$. We claim that $[a_2, a_k] = 1$ for $3 \leq k \leq r$ and $k \neq j$. If not, then we will reduce contradictions on two subcases respectively.

Subcase 1: J is the group of Type (C3) in Theorem 3.1.

In this subcase, $[a_2, a_j] = 1$. We may assume that $[a_2, a_k] = a_2^{\gamma p^{m_2}} a_1^{\beta p^{m_1}}$ where $(\beta, p) = 1$. If $(\gamma, p) = 1$, then $\langle a_1^{\beta p^{m_1 - m_2}} a_2^{\gamma}, a_k\rangle$ is neither abelian nor normal in G, a contradiction. If $\alpha = 0$ and $m_1 > m_2$, then $\langle a_1 a_2, a_k\rangle$ is neither abelian nor normal in G, a contradiction. If $\alpha = 0$ and $m_1 = m_2$, then $\langle a_1 a_2, a_k a_j^{\beta}\rangle$ is neither abelian nor normal in G, also a contradiction.

Subcase 2: J is one of the groups of Type (C4)–(C7) in Theorem 3.1.

In this subcase, $[a_1, a_2] = 1$ and $G' = \langle [a_2, a_j], a_2^{p^{m_2}} \rangle$. Hence we may assume that $[a_2, a_k] = a_2^{\gamma p^{m_2}} [a_2, a_j]^\beta$ where $(\beta, p) = 1$. Let $x = a_k^{-\beta^{-1}} a_j$. Then $[a_1, x] = a_2^{p^{m_2}}$ and $[a_2, x] = a_2^{-\beta^{-1}\gamma p^{m_2}}$. If $(\gamma, p) = 1$, then $\langle a_2, a_k a_j^{-\beta} \rangle$ is neither abelian nor normal in G, a contradiction. If $\alpha = 0$, then $\langle a_1, a_2, x\rangle' = \langle a_2^{p^{m_2}} \rangle$. This contradicts (*).

In this case, $G = J \times A$ where $A = \langle a_3 \rangle \times \cdots \times \langle a_{j-1} \rangle \times \langle a_{j+1} \rangle \times \cdots \times \langle a_r \rangle$. Hence we get the groups (C3)–(C7) in Theorem 3.1.

Case 2: K is one of the groups of Type (C7)–(C10) in Theorem 3.1.

In this case, $G' = \langle a_s^{p^{m_s}}, a_3^{p^{m_3}} \rangle$ where $s = 1$ or 2, $[a_1, a_2] = a_3^{p^{m_3}}$ and $[a_2, a_3] = 1$. Assume that $a_4^{p^{m_4}} = a_s^{\alpha p^{m_s}} a_3^{\beta p^{m_3}}$.

If $p > 2$ or $m_3 > 1$, then, replacing a_4 with $a_4 a_s^{-\alpha p^{m_s - m_4}} a_3^{-\beta p^{m_3 - m_4}}$, we have $a_4^{p^{m_4}} = 1$. If $p = 2$, $m_3 = 1$ and $m_s > 1$, then, we claim that there exists an $x \in \{a_4, a_4 a_3\}$ such that $x^2 \in \langle a_s^{2^{m_s}} \rangle$. Otherwise, $a_4^2 = a_s^{\alpha 2^{m_s}} a_3^2$. Replacing a_4 with $a_4 a_s^{-\alpha p^{m_s - m_4}}$, we have $a_4^2 = a_3^2$. Since $[a_4, a_3] = (a_4 a_3)^2 \notin \langle a_s^{2^{m_s}} \rangle$, $\langle a_4, a_3 \rangle$ is non-abelian. It follows from Theorem 2.6 that $G' \le \langle a_4, a_3 \rangle$. Hence $[a_4, a_3] = a_s^{2^{m_s}} a_3^2$. By calculation, $\langle a_4 a_3, a_3 a_s^{2^{m_s - 1}} \rangle$ is neither abelian nor normal in G, a contradiction. Replacing a_4 with x or $x a_s^{2^{m_s - 1}}$, we have $a_4^2 = 1$. If $p = 2$ and $m_s = m_3 = 1$, then $s = 2$ since $m_1 > 1$. Hence K is a group of Type (C9). In this case, $[a_1, a_3] = a_2^2 a_3^2$. we claim that there exists an involution in $\{a_4, a_4 a_2, a_4 a_3, a_4 a_2 a_3\}$. Otherwise, since $a_4^2 \neq 1$, we have

$$a_4^2 = a_2^2,\ a_3^2 \text{ or } a_2^2 a_3^2.$$

If $a_4^2 = a_3^2$, then, by replacing a_2, a_3 with $a_3, a_2 a_3$ respectively, it is reduced to $a_4^2 = a_2^2$. If $a_4^2 = a_2^2 a_3^2$, then, by replacing a_2, a_3 with $a_2 a_3, a_2$ respectively, it is also reduced to $a_4^2 = a_2^2$. Hence we may assume that $a_4^2 = a_2^2$. Since $(a_4 a_2)^2 = [a_4, a_2] \neq 1$, $L = \langle a_4, a_2 \rangle$ is not abelian. It follows from Theorem 2.6 that $G' \le L$. Hence we may assume that $[a_4, a_2] = a_3^2 a_2^{2\alpha}$. If $[a_4, a_2] = a_3^2 a_2^2$, then $\langle a_1 a_4, a_2 \rangle$ is neither abelian nor normal in G, a contradiction. If $[a_4, a_2] = a_3^2$, then $(a_4 a_2)^2 = a_3^2$. Since $(a_4 a_2 a_3)^2 \neq 1$, $[a_4 a_2, a_3] = [a_4, a_3] = (a_4 a_2 a_3)^2 \neq 1$. Since $M = \langle a_4 a_2, a_3 \rangle$ is not abelian, $G' \le \langle a_4 a_2, a_3 \rangle$ by Theorem 2.6. Hence we may assume that $[a_4, a_3] = [a_4 a_2, a_3] = a_2^2 a_3^{2\alpha}$. Since $(a_4 a_3)^2 \neq 1$, $[a_4, a_3] \neq a_2^2 a_3^3$. Hence $[a_4, a_3] = a_2^2$. In this case, $\langle a_1 a_4 a_2, a_3 \rangle$ is neither abelian nor normal in G, a contradiction.

By the above argument, we may assume that $a_4^{p^{m_4}} = 1$. Let $\{s, t\} = \{1, 2\}$. Since $G' \not\le \langle a_t, a_4 \rangle$, $[a_t, a_4] = 1$ by Theorem 2.6. By the definition relations of (C7)–(C10), $m_t > m_3$. It follows from Theorem 2.6 that $[a_t a_3, a_4] = 1$ since $G' \not\le \langle a_t a_3, a_4 \rangle$. Hence $[a_3, a_4] = 1$. We claim that $[a_s, a_4] \in \langle a_3^{p^{m_3}} \rangle$. Otherwise, we may assume that $[a_s, a_4] = a_s^{\alpha p^{m_s}} a_3^{\beta p^{m_3}}$ where $(\alpha, p) = 1$. By calculation, $\langle a_s, a_t^\beta a_4^{s-t} \rangle$ is neither abelian or normal in G, a contradiction. Hence we may assume that $[a_s, a_4] = a_3^{\beta p^{m_3}}$.

We claim that $[a_s, a_4] = 1$. If not, then, $(\beta, p) = 1$ and we may assume that $[a_s, a_4] = a_3^{p^{m_3}}$ by suitable replacement. We will reduce contradictions on three subcases respectively.

Subcase 1: $s = 2, t = 1$ and $m_2 > m_3$.

In this subcase, K is one of the groups of Type (C7)–(C8). By the definition relations of Type (C7)–(C8), $[a_1, a_3] = a_2^{\eta p^{m_2}}$ where $\eta = 1$ or ν. By calculation, $\langle a_1 a_4, a_2 a_3 \rangle$ is neither abelian or normal in G, a contradiction.

Subcase 2: $s = 2, t = 1$ and $m_2 = m_3$.

In this subcase, K is one of the groups of Type (C8)–(C9). If K is one of the groups of Type (C8), then $[a_1, a_3] = a_2^{\nu p^{m_2}}$. By calculation, $\langle a_1 a_4^{1-\nu}, a_2 a_3 \rangle$ is neither abelian or normal in G, a contradiction. If K is one of the groups of Type (C9), then $[a_1, a_3] = a_2^{kp^{m_2}} a_3^{-p^{m_3}}$ where $(k, p) = 1$. By calculation, $\langle a_1 a_4, a_2^k a_3^{-1} \rangle$ is neither abelian or normal in G, a contradiction.

subcase 3: $s = 1, t = 2$.

In this subcase, K is a group of Type (C10). By the definition relations of Type (C10), $[a_1, a_3] = a_1^{p^{m_3}}$. By calculation, $\langle a_1, a_2 a_3 a_4^{-1} \rangle$ is neither abelian or normal in G, also a contradiction.

Hence $[a_s, a_4] = 1$. By a similar argument, for $4 \leq i \leq r$, we may assume that $a_i^{p^{m_i}} = 1$. Moreover, $[a_1, a_i] = [a_2, a_i] = [a_3, a_i] = 1$. For $4 \leq i < j \leq r$, $[a_i, a_j] = 1$ by Theorem 2.6. In this case, $G = K \times A$ where $A = \langle a_4 \rangle \times \langle a_5 \rangle \times \cdots \times \langle a_r \rangle$. Hence we get the groups of Type (C7)–(C10) in Theorem 3.1. □

Lemma 3.3. *Suppose that G is a metahamilton p-group. If $G' \cong C_p^3$ and $c(G) = 2$, then G is a group of Type* (D1)–(D7) *as defined in Theorem* 3.1.

Proof Let the type of G/G' be $(p^{m_1}, p^{m_2}, \ldots, p^{m_r})$, where $m_1 \geq m_2 \geq \cdots \geq m_r$, $G/G' = \langle a_1 G' \rangle \times \langle a_2 G' \rangle \times \cdots \times \langle a_r G' \rangle$, where $o(a_i G') = p^{m_i}$, $i = 1, 2, \ldots, r$. Then $G = \langle a_1, a_2, \ldots, a_r \rangle$. If $[a_i, a_j] \neq 1$, then $G' = \langle a_i^{p^{m_i}}, a_j^{p^{m_j}}, [a_i, a_j] \rangle$ by Theorem 2.6. Hence we have:

$$\textbf{(*)} \quad \text{If } a_i^{p^{m_i}} = 1, \text{ then } a_i \in Z(G).$$

Let i be the minimal integer such that $a_i^{p^{m_i}} \neq 1$. If $i \neq 1$, then

$$a_1^{p^{m_1}} = \cdots = a_{i-1}^{p^{m_{i-1}}} = 1$$

and hence $a_1, \ldots a_{i-1} \in Z(G)$ by (*). We claim that $m_i = m_1$. If not, then $(a_1 a_j)^{p^{m_1}} = 1$ for $j \geq i$. It follows that $a_1 a_j \in Z(G)$ by (*) and hence $a_j \in Z(G)$ for $j \geq i$. This contradicts $|G'| = p^3$. Hence we may assume that $a_1^{p^{m_1}} \neq 1$.

Let j be the minimal integer such that $a_j^{p^{m_j}} \notin \langle a_1^{p^{m_1}} \rangle$. If $j \neq 2$, then we may assume that $a_k^{p^{m_k}} = a_1^{\alpha_k p^{m_1}}$ for $2 \leq k \leq j-1$. By Theorem 2.6, $[a_k, a_1] = 1$. Replacing a_k with $a_k a_1^{-\alpha_k p^{m_1 - m_k}}$, we get $a_k^{p^{m_k}} = 1$. By (*), $a_k \in Z(G)$ for $2 \leq k \leq j-1$. We claim that $m_j = m_2$. If not, then $(a_2 a_k)^{p^{m_2}} = 1$ for $k \geq j$. It follows that $a_2 a_k \in Z(G)$ by (*) and hence $a_k \in Z(G)$ for $k \geq j$. This contradicts $|G'| = p^3$. Hence we may assume that $a_2^{p^{m_2}} \notin \langle a_1^{p^{m_1}} \rangle$.

Let k be the minimal integer such that $a_k^{p^{m_k}} \notin \langle a_1^{p^{m_1}}, a_2^{p^{m_2}} \rangle$. If $k \neq 3$, then we may assume that $a_w^{p^{m_w}} = a_1^{\alpha_w p^{m_1}} a_2^{\beta_w p^{m_2}}$ for $3 \leq w \leq k-1$. We claim that $m_k = m_3$. If not, then $m_3 > m_k$. Without loss of generality, we may assume that $m_{k-1} > m_k$. Replacing a_w with $a_w a_1^{-\alpha_w p^{m_1 - m_w}} a_2^{\beta_w p^{m_2 - m_w}}$, we get $a_w^{p^{m_w}} = 1$. By (*), $a_w \in Z(G)$ for $3 \leq w \leq k-1$. For $w \geq k$, since $(a_3 a_w)^{p^{m_3}} = 1$, $a_3 a_w \in Z(G)$ by (*). It follows that $a_w \in Z(G)$ for $w \geq k$. This contradicts $|G'| = p^3$. Hence we may assume that $a_3^{p^{m_3}} \notin \langle a_1^{p^{m_1}}, a_2^{p^{p^{m_3}}} \rangle$.

If $r = 3$, then, by [17, Theorem 8.1], G is a group of Type (D1)–(D7) in Theorem 3.1. In the following we may assume that $r \geq 4$.

We claim that there are suitable a_1, a_2, a_3 such that the following condition:

(**) For all $x \in G'$, there exists $b \in \langle a_1, a_2, a_3 \rangle$ such that $x = b^{p^{m_3}}$.

If (**) holds, then for $i > 3$, there exists $b_i \in \langle a_1, a_2, a_3 \rangle$ such that $a_i^{p^{m_i}} = b_i^{p^{m_3}}$. By Theorem 2.6, $[a_i, b_i] = 1$. Replacing a_i with $a_i b_i^{-p^{m_3 - m_i}}$, we get $a_i^{p^{m_i}} = 1$. By (*), $a_i \in Z(G)$. Hence we get the groups (D1)–(D7) in Theorem 3.1.

In the following, we prove that we may choose suitable a_1, a_2, a_3 satisfying the condition (**). If $p > 2$ or $m_2 > 1$, then (**) holds. Hence, we only need to deal with the case where $p = 2$ and $m_2 = 1$.

Case 1. $m_1 > 1$.

If $[a_2, a_3] \neq 1$, then we may assume that $[a_2, a_3] = a_2^{2i} a_3^{2j} a_1^{2^{m_1}}$ by Theorem 2.6. If $[a_2, a_3] = a_2^2 a_3^{2j} a_1^{2^{m_1}}$, then $\langle a_2 a_1^{2^{m_1 - 1}}, a_3 \rangle$ is neither abelian nor normal in G, a contradiction. If $[a_2, a_3] = a_2^3 a_1^{2^{m_1}} = (a_3 a_1^{2^{m_1-1}})^2$, then $\langle a_3 a_1^{2^{m_1-1}}, a_3 \rangle$ is neither abelian nor normal in G, a contradiction. Hence $[a_2, a_3] = a_1^{2^{m_1}}$. In this case, it is easy to check that $G' = V_1(\langle a_1, a_2, a_3 \rangle)$. Hence (**) holds.

Case 2. $m_1 = 1$.

By an argument similar to the beginning of the proof of Theorem 3.1, we may choose suitable a_1, a_2, a_3 such that the commutative group of $K = \langle a_1, a_2, a_3 \rangle$ is of order at least 4.

If there are two elements in $\{1, a_1, a_2, a_3, a_1 a_2, a_1 a_3, a_2 a_3, a_1 a_2 a_3\}$ such that the squares are equal to each other, then, by Theorem 2.6, they are commutative. It follows that there is an involution in $\{a_1, a_2, a_3, a_1 a_2, a_1 a_3, a_2 a_3, a_1 a_2 a_3\}$. By (*), this involution is in the center of K, which contradicts $|K'| \geq 4$. Hence

$$G' = V_1(K) = \{1, a_1^2, a_2^2, a_3^2, (a_1 a_2)^2, (a_1 a_3)^2, (a_2 a_3)^2, (a_1 a_2 a_3)^2\}.$$

That is, (**) holds. □

4 Finite metahamiltonian p-groups whose derived group is of exponent $> p$

Theorem 4.1. *Suppose that G is a finite metahamiltonian p-group with $\exp(G') > p$. Then G is isomorphic to one of the following non-isomorphic groups:*

(E) *G is metacyclic.*

(E1) $\langle a, b \mid a^{p^{r+s+u}} = 1,\ b^{p^{r+s+t}} = a^{p^{r+s}},\ a^b = a^{1+p^r}\rangle$, *where* $r \geq 1$, $u \leq r$, $r+1 \geq s+u \geq 2$, *and if* $p = 2$ *then* $r \geq 2$;

(E2) $\langle a, b \mid a^{2^3} = b^{2^m} = 1, a^b = a^{-1}\rangle$, *where* $m \geq 1$;

(E3) $\langle a, b \mid a^{2^3} = 1, b^{2^m} = a^4, a^b = a^{-1}\rangle$, *where* $m \geq 1$;

(E4) $\langle a, b \mid a^{2^3} = b^{2^m} = 1, a^b = a^3\rangle$, *where* $m \geq 1$.

(F) *G is not metacyclic and G' is cyclic and* $|G'| \geq p^2$.

(F1) $K \times A$, *where* $K = \langle a, b \mid a^{p^{r+s+u}} = 1, b^{p^{r+s}} = 1, a^b = a^{1+p^r}\rangle$, $u \leq r$, $r+1 > s+u \geq 2$, *and* $A \neq 1$ *is abelian such that* $\exp(A) \leq p^{(r+1)-(s+u)}$;

(F2) $K \times A$, *where* $K = \langle a, b \mid a^{p^{r+t+u}} = 1, b^{p^r} = 1, a^b = a^{1+p^{r+t}}\rangle$, $t \geq 1$, $r \geq u \geq 2$, *and* $A \neq 1$ *is abelian such that* $\exp(A) \leq p^{t+(r+1)-u}$;

(F3) $K \times A$, *where* $K = \langle a, b \mid a^{p^{r+s}} = 1, b^{p^{r+s+t}} = 1, a^b = a^{1+p^r}\rangle$, $t \geq 1$, $r+1 > s \geq 2$, *and* $A \neq 1$ *is abelian such that* $\exp(A) \leq p^{(r+1)-s}$;

(F4) $K \times A$, *where* $K = \langle a, b \mid a^{p^{r+s+u}} = 1, b^{p^{r+s+t}} = a^{p^{r+s}}, a^b = a^{1+p^r}\rangle$, $stu \neq 0$, $r+1 > s+u \geq 2$, *and* $A \neq 1$ *is abelian such that* $\exp(A) \leq p^{(r+1)-(s+u)}$;

(F5) $(K \rtimes B) \times A$, *where* $K = \langle a, b \mid a^{p^{r+t+u}} = 1, b^{p^r} = 1, a^b = a^{1+p^{r+t}}\rangle$, $B = \langle b_1\rangle \times \langle b_2\rangle \times \cdots \times \langle b_f\rangle$ *such that* $o(b_i) = p^{r_i}$, $[a, b_i] = a^{p^{r+t_i}}$, $[b, b_i] = 1$, $\max\{t, u-2\} < t_1 < t_2 < \cdots < t_f < t+u$, $r+t > r_1+t_1 > r_2+t_2 > \cdots > r_f+t_f \geq t+u \geq t+2$, *and* A *is abelian such that* $\exp(A) \leq p^{t+(r+1)-u}$.

(G) *the type of G' is* (p^α, p) *where* $\alpha \geq 2$.

(G1) $\langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1+m_2}} = a_2^{p^{m_2+1}} = a_3^p = 1,\ [a_1, a_2] = a_1^{p^{m_1}},\ [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = 1\rangle$, *where* $p > 2$ *and* $m_1 > m_2 \geq 1$;

(G2) $K \times A$, *where* $K = \langle a_1, a_2, a_3 \mid a_1^{p^{m_1+1+k}} = a_2^{p^{m_2+1}} = a_3^{p^{m_3}} = 1, [a_1, a_2] = a_1^{p^{m_1}}, [a_1, a_3] = a_2^{p^{m_2}}, [a_2, a_3] = 1\rangle$, $m_1 \geq m_2 \geq m_3$, $1 \leq k \leq \min\{m_1 - m_3, m_2 - m_3 + 1, m_2 - 1\}$ *and* A *is abelian such that* $\exp(A) \leq p^{m_2-k}$.

Proof If G is metacyclic, then, by Lemma 4.2, G is a group of Type (E1)–(E4) in the theorem. In the following, we may assume that G is not metacyclic. If G' is cyclic, then, by Lemma 4.5, G is a group of Type (F1)–(F5) in the theorem. If G' is not cyclic, then, by Lemma 4.6, G is a group of Type (G1)–(G2) in theorem. Finally, it is omitted to check that such groups are non-isomorphic metahamiltonian p-groups. □

Lemma 4.2. *Suppose that G is a metacyclic p-group and $|G'| \geq p^2$. If G is metahamiltonian, then G is a group of Type* (E1)–(E4) *as defined in Theorem* 4.1.

Proof Case 1: $p > 2$ or G is an ordinary metacyclic 2-group. That is,

$$G = \langle a, b \mid a^{p^{r+s+u}} = 1, b^{p^{r+s+t}} = a^{p^{r+s}}, a^b = a^{1+p^r} \rangle,$$

where $r \geq 1$, $u \leq r$, and if $p = 2$ then $r \geq 2$.

Since $|G'| \geq p^2$, we have $s + u \geq 2$. We only need to prove that $r + 1 \geq s + u$. Otherwise, $r + 1 < s + u$. By calculation,

$$[a^{p^{r+1}}, b] = a^{-p^{r+1}}(a^{p^{r+1}})^b = a^{p^{2r+1}} \neq 1.$$

Hence $\langle a^{p^{r+1}}, b \rangle$ is neither abelian nor normal in G, a contradiction. Thus $r+1 \geq s+u$ and G is a group of Type (E1) in Theorem 4.1.

Case 2: $p = 2$ and G is not an ordinary metacyclic 2-group.

Let $o(a) = 2^n$ and $H = \langle a^{2^{n-2}}, b \rangle$. Since $H' = \langle a^{2^{n-1}} \rangle$, H is not abelian. It follows that $H \trianglelefteq G$. By Theorem 2.6, $a^2 \in H$. Hence $n \leq 3$ and $|G'| = 4$. By Lemma 2.4, $G \in \mathcal{A}_2$. By [4, Lemma 2.4], we get groups of (E2)–(E4) in Theorem 4.1. $\square$

We need the following two lemmas on number theory. Proofs are omitted.

Lemma 4.3. *Suppose that $U = U(p^n)$ is the multiplicative group containing of all the invertible elements of $\mathbb{Z}/p^n\mathbb{Z}$, where p is an odd prime and n is a positive integer. That is,*

$$U = \{x \in \mathbb{Z}/p^n\mathbb{Z} \mid (x, p) = 1\}.$$

Let $S(U) \in \mathrm{Syl}_p(U)$. Then

$$S(U) = \{x \in U \mid x \equiv 1 \pmod{p}\},$$

and $S(U)$ is cyclic with order p^{n-1}. $S_i(U)$ where $0 \leq i < n$, the unique subgroup of $S(U)$ of order p^i, is

$$S_i(U) = \{x \in U \mid x \equiv 1 \pmod{p^{n-i}}\}.$$

Lemma 4.4. *Suppose that $U = U(2^n)$ is the multiplicative group containing of all invertible elements of $\mathbb{Z}/2^n\mathbb{Z}$, where $n \geq 2$ is a positive integer. Then*

$$\begin{aligned} U &= \langle -1 \rangle \times \langle 1 + 2^2 \rangle (\cong C_2 \times C_{2^{n-2}}) \\ &= \{\varepsilon + i2^m \mid \varepsilon = \pm 1, 2 \leq m \leq n, 1 \leq i \leq 2^{n-m} \text{ and } i \text{ is odd}\} \end{aligned}$$

For $m < n$, the order of $\varepsilon + i2^m$ is 2^{n-m} and $\langle \varepsilon + i2^m \rangle = \langle \varepsilon + j2^m \rangle$ for all odd j.

Lemma 4.5. *Suppose that G is a metahamilton p-group and G is not metacyclic. If $|G'| \geq p^2$ and G' is cyclic, then G is a group of Type* (F1)–(F5) *in Theorem* 4.1.

Proof By Theorem 2.7, $d(G) > 2$. Let $G' = \langle c \rangle$, the type of G/G' be $(p^{m_1}, p^{m_2}, \ldots, p^{m_w})$ where $m_1 \geq m_2 \geq \cdots \geq m_w$. Let

$$G/G' = \langle a_1G' \rangle \times \langle a_2G' \rangle \times \cdots \times \langle a_wG' \rangle \text{ where } o(a_iG') = p^{m_i},\ i = 1, 2, \ldots, w.$$

Then $G = \langle a_1, a_2, \dots, a_w \rangle$.

Let i be the minimal integer such that $a_i \notin C_G(G/\mho_1(G'))$. Then there exists $j > i$ such that $G' = \langle [a_i, a_j] \rangle$. If $i \neq 1$, then $a_1 \in C_G(G/\mho_1(G'))$. Replacing a_1 with $a_1 a_j$, we have $G' = \langle [a_1, a_i] \rangle$.

Let j be the minimal integer such that $G' = \langle [a_1, a_j] \rangle$. If $j \neq 2$, then $[a_1, a_2] \in \mho_1(G')$. Replacing a_2 with $a_2 a_j$, we have $G' = \langle [a_1, a_2] \rangle$.

Let $K = \langle a_1, a_2 \rangle$. By Theorem 2.7, K is metacyclic. Hence K is one of the groups in Theorem 4.2. That is, K is one of the groups (E1)–(E4) in Theorem 4.1.

Step 1: We claim that K is one of the groups of Type (E1) in Theorem 4.1.

If not, then we may assume that $K = \langle a, b \rangle$ satisfying the relations of Type (E2)–(E4) in Theorem 4.1. That is,

$$a^{2^3} = 1, b^{2^m} \in \mho_1(K') = \langle a^4 \rangle \text{ and } [a, b] \equiv a^2 \pmod{\mho_1(K')}.$$

Obviously, $G' = K' = \langle a^2 \rangle$ and $m_3 = m_4 = \cdots = m_w = 1$.

Case 1: $a_3^2 \in \mho_1(K')$ and $[a_3, b] \in \mho_1(K')$.

If $[a_3, b] = a^4$, then $\langle a_3, b \rangle$ is neither abelian nor normal in G, a contradiction. If $[a_3, b] = 1$, then $\langle a_3 a^2, b \rangle$ is neither abelian nor normal in G, a contradiction.

Case 2: $a_3^2 \in \mho_1(K')$ and $[a_3, b] \equiv a^2 \pmod{\mho_1(K')}$.

If $[a_3, a] \equiv a^2 \pmod{\mho_1(K')}$, then $(a_3 a)^2 \in \mho_1(K')$ and $[a_3 a, b] \in \mho_1(K')$. Replacing a_3 with $a_3 a$, it is reduced to Case 1. Hence we may assume that $[a_3, a] \in \mho_1(K')$. Since $[a_3, a^2] = [a_3, a]^2 = 1$, $[a_3, G'] = 1$. By calculation, $1 = [a_3^2, b] = [a_3, b]^2 [a_3, b, a_3] = [a_3, b]^2$. Hence $[a_3, b] \in \mho_1(K')$, a contradiction.

Case 3: $a_3^2 \equiv a^2 \pmod{\mho_1(K')}$.

If $[a_3, a] \in \mho_1(K')$, then, replacing a_3 with $a_3 a$, it is reduced to Case 1 or Case 2. Hence we may assume that $[a_3, a] \equiv a^2 \pmod{\mho_1(K')}$. Since $a_3^2 \equiv a^2 \pmod{\mho_1(K')}$, $[a_3^2, b] = [a^2, b] = a^4$. It follows that $[a_3, b] \equiv a^2 \pmod{\mho_1(K')}$. Since $(a_3 a)^2 \equiv a^2 \pmod{\mho_1(K')}$, similar reason as above gives that $[a_3 a, b] \equiv a^2 \pmod{\mho_1(K')}$. Hence $[a, b] \in \mho_1(K')$, a contradiction.

Step 2: By suitable replacement, we may assume $a_i^{p^{m_i}} = 1$, where $3 \le i \le w$. Moreover, $[a_i, a_j] = 1$ for all $3 \le i, j \le w$.

By Step 1, $K \cong \langle r, s, t, u \rangle_p$ where $r \geq 1$, $u \leq r$, $r + 1 \geq s + u$, and if $p = 2$ then $r \geq 2$. Assume that

$$K = \langle a, b \mid a^{p^{r+s+u}} = 1, b^{p^{r+s+t}} = a^{p^{r+s}}, a^b = a^{1+p^r} \rangle.$$

Let $L = \langle a, a_i \rangle$ and $x_i \in L$ such that $L = \langle a, x_i \rangle$ and $\langle x_i \rangle \cap \langle a \rangle$ has minimal order. We claim that $x_i^{p^{m_i}} = 1$. Otherwise, we may assume that

$$\langle x_i \rangle \cap \langle a \rangle = \langle a^{p^\alpha} \rangle \text{ and } \langle [x_i, a] \rangle = \langle a^{p^\beta} \rangle \text{ where } \alpha \geq r \text{ and } \beta \geq r.$$

Then there exist integers y and z such that $(yz,p)=1$, $x_i^{p^{m_i}}=a^{yp^{\alpha}}$ and $[x_i,a]=a^{zp^{\beta}}$. By calculation,

$$\begin{aligned}(x_i a^{-yp^{\alpha-m_i}})^{p^{m_i}} &= x_i^{p^{m_i}}[x_i,a^{yp^{\alpha-m_i}}]^{\binom{p^{m_i}}{2}}[x_i,a^{yp^{\alpha-m_i}},x_i]^{\binom{p^{m_i}}{3}}a^{-yp^{\alpha}}\\ &= a^{yzp^{\alpha+\beta-m_i}\binom{p^{m_i}}{2}}[a^{yzp^{\alpha+\beta-m_i}\binom{p^{m_i}}{3}},x_i]\end{aligned}$$

Noting that $\beta\geq r\geq 2$ for $p=2$, we have $(x_i a^{-yp^{\alpha-m_i}})^{p^{m_i}}\in\langle a^{p^{\alpha+1}}\rangle$, which is contrary to the choice of x_i. Replacing a_i with x_i, we have $a_i^{p^{m_i}}=1$ where $3\leq i\leq w$.

For $3\leq i,j\leq w$, we claim that $[a_i,a_j]=1$. Otherwise, Theorem 2.6 gives that $G'\leq\langle a_i,a_j\rangle$. It is easy to see that $\langle a_i,a_j\rangle$ is not metacyclic. This contradicts Theorem 2.7.

Step 3: K is one of the following groups:

(A) $\langle a,b\mid a^{p^{r+s+u}}=1, b^{p^{r+s}}=1, a^b=a^{1+p^r}\rangle$, where $r\geq 2$ for $p=2$ and $r+1\geq s+u\geq 2$;

(B) $\langle a,b\mid a^{p^{r+t+u}}=1, b^{p^{r}}=1, a^b=a^{1+p^{r+t}}\rangle$, where $t\geq 1$ and $r\geq u\geq 2$;

(C) $\langle a,b\mid a^{p^{r+s}}=1, b^{p^{r+s+t}}=1, a^b=a^{1+p^r}\rangle$, where $r\geq 2$ for $p=2$, $t\geq 1$ and $r+1\geq s\geq 2$;

(D) $\langle a,b\mid a^{p^{r+s+u}}=1, b^{p^{r+s+t}}=a^{p^{r+s}}, a^b=a^{1+p^r}\rangle$, where $r\geq 2$, $stu\neq 0$ and $r+1\geq s+u\geq 2$.

Assume that $K=\langle a,b\mid a^{p^{r+s+u}}=1, b^{p^{r+s+t}}=a^{p^{r+s}}, a^b=a^{1+p^r}\rangle$. If $t=0$, then we have $(ba^{-1})^{p^{r+s}}=1$ for $p>2$ and $(ba^{2^u-2^{r-1}-1})^{2^{r+s}}=1$ for $p=2$. Replacing b with ba^{-1} or $ba^{2^u-2^{r-1}-1}$ respectively, we get a group of Type (A). In the following we may assume that $t\geq 1$. If $s=0$, then $(a^{-1}b^{p^t})^{p^r}=1$. Replacing a and b with b and $a^{-1}b^{p^t}$, respectively, we get a group of Type (B). If $u=0$, then we get a group of Type (C). If $su\neq 0$, then we get a group of Type (D).

Step 4: Determine G in which K is a direct factor. That is, $G=K\times A$. Since $K'=G'$, A is abelian.

Case 1: K is a group of Type (A) in Step 3.

Let $d\in A$ and $o(d)=p^e$. By calculation,

$$[a^{p^{s+u-1}}d,b]=a^{p^{r+s+u-1}}\neq 1.$$

It follows that

$$a^{p^r}\in\langle(a^{p^{s+u-1}}d)^{p^e}\rangle=\langle a^{p^{e+s+u-1}}\rangle.$$

Hence $e+s+u-1\leq r$. By the arbitrariness of d, we get $\exp(A)\leq p^{(r+1)-(s+u)}$. Since G is not metacyclic, $A\neq 1$. It follows that $r+1>s+u$. Hence we get a group of Type (F1) in Theorem 4.1.

Case 2: K is a group of Type (B) in Step 3.

Let $d \in A$ and $o(d) = p^e$. By calculation,

$$[a^{p^{u-1}}d, b] = a^{p^{r+t+u-1}} \neq 1.$$

It follows that

$$a^{p^{r+t}} \in \langle (a^{p^{u-1}}d)^{p^e} \rangle = \langle a^{p^{e+u-1}} \rangle.$$

Hence $e + u - 1 \leq r + t$. By the arbitrariness of d, we get $\exp(A) \leq p^{t+(r+1)-u}$. Hence G is a group of Type (F2) in Theorem 4.1.

Case 3: K is a group of Type (C) or (D) in Step 3.

Let $d \in A$ and $o(d) = p^e$. By calculation,

$$[a^{p^{s+u-1}}d, b] = a^{p^{r+s+u-1}} \neq 1.$$

It follows that

$$a^{p^r} \in \langle (a^{p^{s+u-1}}d)^{p^e} \rangle = \langle a^{p^{e+s+u-1}} \rangle.$$

Hence $e+s+u-1 \leq r$. By that arbitrariness of d, we get $\exp(A) \leq p^{(r+1)-(s+u)}$. Since G is not metacyclic, $A \neq 1$. It follows that $r + 1 > s + u$. Hence we get a group of Type (F3) or (F4) in Theorem 4.1.

Step 5: Determine G in which K is not a direct factor.

Let $G = H \times A$, where $K < H$ and A is as large as possible for K. Since $K' = G'$, A is abelian. By Step 2, we may assume that $H = K \rtimes B$ where $B = \langle b_1 \rangle \times \langle b_2 \rangle \times \cdots \times \langle b_f \rangle$ such that $o(b_i) = p^{r_i}$, $o(bG') \geq r_1 \geq r_2 \geq \cdots \geq r_f$.

We claim that K is neither a group of Type (C) nor (D) in Step 3. Otherwise, by calculation, $\langle ab^{-p^t} \rangle \cap \langle a \rangle = 1$. Since $G' \not\leq \langle ab^{-p^t}, b_i \rangle$, Theorem 2.6 gives that $[ab^{-p^t}, b_i] = 1$. Similar reason gives that $[b, b_i] = 1$. Hence $H = K \times B$, which is contrary to the choice of H.

If K is a group of Type (A) in Step 3, then we claim that $s = 0$. Otherwise, by calculation, $\langle ab \rangle \cap \langle a \rangle \leq \langle a^{p^{r+1}} \rangle$. Since $G' \not\leq \langle ab, b_i \rangle$, Theorem 2.6 gives that $[ab, b_i] = 1$. Similar reason gives that $[b, b_i] = 1$. Hence $H = K \times B$, which is contrary to the choice of H.

By the above argument, we may assume that

$$K = \langle a, b \mid a^{p^{r+t+u}} = 1, b^{p^r} = 1, a^b = a^{1+p^{r+t}} \rangle,$$

where $t \geq 0$ and $r \geq u \geq 2$. Since $G' \not\leq \langle b, b_i \rangle$, Theorem 2.6 gives that $[b, b_i] = 1$.

Let j be the minimal positive integer such that $[a, b_i]$ has maximal order. We may assume that $j = 1$, replacing b_1 with $b_1 b_j$ when it is necessary. Similarly, we may assume that $\langle [a, b_1] \rangle \geq \langle [a, b_2] \rangle \geq \cdots \geq \langle [a, b_f] \rangle$.

Assume that $[a,b_i]=a^{\gamma_i p^{r+t_i}}$ where $(\gamma_i,p)=1$. Then $t\le t_1\le t_2\le\cdots\le t_f$. Note that $a^b=a^{1+\gamma_i p^{r+t_i}}$. By Lemma 4.3 and 4.4, there exists positive integer w such that

$$(1+\gamma_i p^{r+t_i})^j\equiv 1+p^{r+t_i} \pmod{p^{r+t+u}}.$$

Replacing b_i with b_i^w, we have $[a,b_i]=a^{p^{r+t_i}}$.

Case 1: $t_1>t$.

If $t_2=t_1$, then $b_1b_2^{-1}$ is a direct factor of H, a contradiction. So $t_1<t_2$. Similarly, we have

$$t<t_1<t_2<\cdots<t_f.$$

If $(b_1b^{-p^{t_1-t}})^{p^{r_1}}=1$, then $b_1b^{-p^{t_1-t}}$ is a direct factor of H, a contradiction. Hence $(b_1b^{-p^{t_1-t}})^{p^{r_1}}\ne 1$. It follows that $b^{p^{r_1+t_1-t}}\ne 1$. Hence $r_1+t_1-t<r$. Thus

$$r-r_1>t_1-t>0.$$

Similarly, we have

$$r_i+t_i>r_{i+1}+t_{i+1}.$$

By Lemma 4.3 and 4.4, in the multiplicative group consisting of all invertible elements of $\mathbb{Z}/p^{r+t+u}\mathbb{Z}$, the order of $1+p^{r+t_f}$ is p^{t+u-t_f}. Since $[a,b_f^{p^{r_f}}]=1$, we have

$$a^{b_f^{p^{r_f}}}=a^{(1+p^{r+t_f})^{p^{r_f}}}=a.$$

It follows that $r_f\ge t+u-t_f$. Thus

$$t_f+r_f\ge t+u.$$

By calculation,

$$\langle ba^{p^{t-t_1+u-1}}\rangle\cap\langle a\rangle=\langle (ba^{p^{t-t_1+u-1}})^{p^r}\rangle=\langle a^{p^{r+t-t_1+u-1}}\rangle.$$

Let $N=\langle ba^{p^{t-t_1+u-1}},b_1\rangle$. Since $[ba^{p^{t-t_1+u-1}},b_1]=a^{p^{r+t+u-1}}\ne 1$, N is not abelian. By Theorem 2.6, $G'\le N$. It follows that $r+t-t_1+u-1\le r+t$. Thus

$$t_1\ge u-1.$$

Finally, by an argument similar to Step 4, we have $\exp(A)\le p^{t+(r+1)-u}$. Hence we get a group of Type (F5) in Theorem 4.1. In this case, $\exp(A)\le p^r$.

Case 2: $t_1=t$.

Suppose that h is the maximal positive integer such that $t_h=t$. Let $r'=r_h$, $t'=t+(r-r_h)$ and $\tilde K=\langle a,b_h\rangle$. Then

$$\tilde K=\langle a,b_h \mid a^{p^{r'+t'+u}}=1, b_h^{p^{r'}}=1, a^{b_h}=a^{1+p^{r'+t'}}\rangle.$$

If $h<f$, then we let $f'=f-h$. For $1\le i\le f'$, let

$$b'_i = b_{h+i},\ t'_i = t_{h+i},\ \tilde{B} = \langle b'_1\rangle \times \dots \langle b'_{f'}\rangle,\ \tilde{H} = \tilde{K} \rtimes \tilde{B}, \text{ and}$$
$$\tilde{A} = A \times \langle bb_h^{-1}\rangle \times \langle b_1 b_h^{-1}\rangle \dots \langle b_{h-1} b_h^{-1}\rangle.$$

Then $G = \tilde{H} \times \tilde{A}$, where $\tilde{A}$ is as large as possible. Notice that $t'_1 > t'$. By a similar argument to Case 1, we get a group of Type (F5) in Theorem 4.1.

If $h = f$, then we also have $G = \tilde{H} \times \tilde{A}$. The difference in this case from the case $h < f$ is $\tilde{H} = \tilde{K}$. By an argument similar to Step 4, we have $\exp(A) \le p^{t'+(r'+1)-u}$. Hence we get a group of Type (F2) in Theorem 4.1. □

Lemma 4.6. *Suppose that G is a finite metahamilton p-group. If $\exp(G') > p$ and G' is not cyclic, then G is a group of Type (G1)–(G2) in Theorem 4.1.*

Proof Let $H \le G$ such that $d(H) = 2$ and $\exp(H') > p$. By Theorem 2.7, H is metacyclic. By Theorem 2.6, $G' < H$ and hence G' is metacyclic.

Let $N = \mho_1(G')$ and $\bar{G} = G/N$. Then $\bar{G}' \cong C_p^2$. By Theorem 2.7, $d(G) > 2$ and hence $d(\bar{G}) > 2$. By Corollary 2.9, $c(\bar{G}) = 2$. Hence $\bar{G}$ is a group in Theorem 3.2. That is, $\bar{G}$ is a group of Type (C1)–(C10) in Theorem 3.1.

Suppose that $\bar{G}$ is a group of Type (C1) in Theorem 3.1. That is, $\bar{G} = \bar{K} \times \bar{A}$, where

$$\bar{K} = \langle \bar{a}_1, \bar{a}_2, \bar{b} \mid \bar{a}_1^4 = \bar{a}_2^4 = 1, \bar{b}^2 = \bar{a}_1^2, [\bar{a}_1, \bar{a}_2] = 1, [\bar{a}_1, \bar{b}] = \bar{a}_2^2, [\bar{a}_2, \bar{b}] = \bar{a}_1^2\rangle$$

and $\bar{A}$ is abelian such that $\exp(\bar{A}) \le 2$. Then

$$G' = \langle [a_1, b], [a_2, b], \mho_1(G')\rangle = \langle a_1^2, a_2^2\rangle \text{ and } \mho_1(G') = \langle a_1^4, a_2^4\rangle.$$

Let M be a maximal subgroup of $\mho_1(G')$ such that $M \trianglelefteq G$. Then we may assume that

$$M = \langle e, \mho_2(G')\rangle,\ [a_1, a_2] \equiv e^i \pmod M,$$
$$b^2 \equiv a_1^2 e^j \pmod M \text{ and } [a_1, b] \equiv a_2^2 e^k \pmod M.$$

It follows from $[a_1, a_2] \equiv e^i \pmod M$ that $[a_1^2, a_2] \equiv [a_1, a_2^2] \equiv 1 \pmod M$. It follows from $b^2 \equiv a_1^2 e^j \pmod M$ that $[a_1^2, b] \equiv [a_1, b^2] \equiv 1 \pmod M$. On the other hand, it follows from $[a_1, b] \equiv a_2^2 e^k \pmod M$ that $[a_1^2, b] \equiv [a_1, b]^2 [a_1, b, a_1] \equiv a_2^4 \pmod M$. It follows that $a_2^4 \in M$ and hence $M = \langle a_1^8, a_2^4\rangle$.

Let $L = \langle a_1 M, bM\rangle$. Since $\exp(L') = 2$, Theorem 2.8 gives that $c(L) = 2$. It follows that $[a_2^2, b] \equiv 1 \pmod M$. On the other hand, $[a_2^2, b] \equiv [a_2, b]^2 [a_2, b, a_2] \equiv a_1^4 \pmod M$. It follows that $a_1^4 \in M$. Hence $M = \mho_1(G)$, a contradiction.

Similar reasoning gives that $\bar{G}$ is not a group of Type (C2) in Theorem 3.1.

Suppose that $\bar{G}$ is a group of Type (C4) in Theorem 3.1. That is, $\bar{G} = \bar{K} \times \bar{A}$, where

$$\bar{K} = \langle \bar{a}_1, \bar{a}_2, \bar{a}_3 \mid \bar{a}_1^{p^{m_1+1}} = \bar{a}_2^{p^{m_2+1}} = \bar{a}_3^{p^{m_3}} = 1, [\bar{a}_1, \bar{a}_2] = 1, [\bar{a}_1, \bar{a}_3] = \bar{a}_2^{p^{m_2}},$$
$$[\bar{a}_2, \bar{a}_3] = \bar{a}_1^{\nu p^{m_1}}\rangle,\ p > 2,\ \nu \text{ is a fixed square non-residue modulo } p,$$
$$m_1 - 1 = m_2 \ge m_3 \text{ or } m_1 = m_2 \ge m_3, \text{ and } \bar{A} \text{ is abelian such that } \exp(\bar{A}) \le p^{m_2}.$$

Then $G' = \langle [a_1,a_3],[a_2,a_3],\mho_1(G')\rangle = \langle [a_1,a_3],[a_2,a_3]\rangle = \langle a_1^{p^{m_1}}, a_2^{p^{m_2}}\rangle$. Since $\langle \bar{a}_1,\bar{a}_3\rangle$ and $\langle \bar{a}_2,\bar{a}_3\rangle$ are not metacyclic, $\langle a_1,a_2\rangle$ and $\langle a_1,a_3\rangle$ are not metacyclic. By Theorem 2.7, $[a_1,a_2]^p = 1$ and $[a_1,a_3]^p = 1$. Moreover, $\exp(G') = p$, a contradiction.

Similar reasoning gives that $\bar{G}$ is not a group of Type (C5)–(C10) in Theorem 3.1.

By the above argument, $\bar{G}$ is a group of Type (C3) in Theorem 3.1. That is, $\bar{G} = \bar{K}\times\bar{A}$, where

$$\bar{K} = \langle \bar{a}_1,\bar{a}_2,\bar{a}_3 \mid \bar{a}_1^{p^{m_1+1}} = \bar{a}_2^{p^{m_2+1}} = \bar{a}_3^{p^{m_3}} = 1, [\bar{a}_1,\bar{a}_2] = \bar{a}_1^{p^{m_1}}, [\bar{a}_1,\bar{a}_3] = \bar{a}_2^{p^{m_2}}, [\bar{a}_2,\bar{a}_3] = 1\rangle,\ m_1 > 1 \text{ for } p = 2,$$
$$m_1 \geq m_2 \geq m_3 \text{ and } \bar{A} \text{ is abelian such that } \exp(\bar{A}) \leq p^{m_2}.$$

Then $G' = \langle a_1^{p^{m_1}}, a_2^{p^{m_2}}\rangle$.

Since $G' \not\leq \langle a_2,a_3\rangle$, $[a_2,a_3] = 1$. Since $\langle \bar{a}_1,\bar{a}_3\rangle$ is not metacyclic, $\langle a_1,a_3\rangle$ is not metacyclic. By Theorem 2.7, $[a_1,a_3]^p = 1$. Let $[a_1,a_3] = a_2^{p^{m_2}}d$ where $d \in \mho_1(G')$. Then $a_2^{p^{m_2+1}}d^p = 1$. It follows that $a_2^{p^{m_2+1}} \in \mho_2(G')$. Hence

$$o(a_1) > p^{m_1+1},\ N = \mho_1(G') = \langle a_1^{p^{m_1+1}}, a_2^{p^{m_2+1}}\rangle = \langle a_1^{p^{m_1+1}}\rangle \text{ and } a_2^{p^{m_2+1}} \in \langle a_1^{p^{m_1+2}}\rangle.$$

Since $G' \not\leq \langle a_2, a_3a_1^{p^{m_1}}\rangle$, $[a_2, a_3a_1^{p^{m_1}}] = 1$ and hence $[a_1^{p^{m_1}}, a_2] = a_1^{p^{2m_1}} = 1$. Assume that the order of a_1 is p^{m_1+1+k} where $k \geq 1$. Then $m_1 > k$.

Let $\bar{A} = \langle \bar{a}_4\rangle \times \langle \bar{a}_5\rangle \times \cdots \times \langle \bar{a}_f\rangle$ and the type of $\bar{A}$ be $(p^{m_4}, p^{m_5}, \dots, p^{m_f})$. For $4 \leq i \leq f$ and $1 \leq j \leq f$, since $G' \not\leq \langle a_i, a_j\rangle$, $[a_i,a_j] = 1$ and hence $a_i \in Z(G)$. Assume that $a_i^{p^{m_i}} = a_1^{sp^{m_1+1}}$. Then $(a_ia_1^{-sp^{m_1+1-m_i}})^{p^{m_i}} = 1$. Let $b_i = a_ia_1^{-sp^{m_1+1-m_i}}$, $A = \langle b_4\rangle \times \langle b_5\rangle \times \cdots \times \langle b_f\rangle$ and $K = \langle a_1,a_2,a_3\rangle$. Then $G = K \times A$.

Assume that $[a_1,a_2] = a_1^{p^{m_1}}a_1^{up^{m_1+1}}$. Then $a_1^{a_2} = a_1^{1+(1+up)p^{m_1}}$. By Lemma 4.3 and Lemma 4.4, there exists a positive integer w such that $(1+(1+up)p^{m_1})^j = 1 + p^{m_1}$. Replacing a_2 and a_3 with a_2^w and a_3^w respectively, we have $[a_1,a_2] = a^{p^{m_1}}$.

By Lemma 4.3 and Lemma 4.4, in the multiplicative group consisting of all invertible elements of $\mathbb{Z}/p^{m_1+1+k}\mathbb{Z}$, the order of $1+p^{m_1}$ is p^{k+1}. Since $a_1^{(1+p^{m_1})^{p^{m_2+1}}} = a_1^{a_2^{p^{m_2+1}}} = a_1$, we have $k+1 \leq m_2+1$. Hence $k \leq m_2$.

Case 1: $k = m_2$.

In this case, $m_1 > m_2$ and $[a_1, a_2^{p^{m_2}}] \neq 1$. It follows that $c(\langle a_1,a_3\rangle) > 2$, Corollary 2.9 gives that $p > 2$ and $\langle a_1,a_3\rangle \in \mathcal{A}_2$. If $m_3 > 1$, then $\langle a_1, a_2^{p^{m_2}}a_3^p\rangle$ is neither abelian nor normal in G, a contradiction. Hence we have $m_3 = 1$. If $A \neq 1$, then, letting $1 \neq e \in A$, $\langle a_1, a_2^{p^{m_2}}e\rangle$ is neither abelian nor normal in G, a contradiction. Hence we have $A = 1$. Assume that $a_3^p = a_1^{vp^{m_1+1}}$. Replacing a_3 with $a_3a_1^{-vp^{m_1}}$, we have $a_3^p = 1$.

Assume that $[a_1,a_3] = a_2^{p^{m_2}}a_1^{wp^{m_1+1}}$. Then $a_2^{p^{m_2+1}}a_1^{wp^{m_1+2}} = 1$. Since

$$(a_2a_1^{wp^{m_1-m_2+1}})^{p^{m_2+1}} = 1,$$

we may assume that

$$(a_2a_1^{wp^{m_1-m_2+1}})^{p^{m_2}} = a_2^{p^{m_2}}a_1^{wp^{m_1+1}}a_1^{xp^{m_1+m_2}}.$$

Replacing a_2 with $a_2a_1^{wp^{m_1-m_2+1}}a_1^{-xp^{m_1}}$, we have $a_2^{p^{m_2+1}}=1$ and $[a_1,a_3]=a_2^{p^{m_2}}$. Hence G is a group of Type (G1) in Theorem 4.1.

Case 2: $k<m_2$.

In this case $[a_1,a_2^{p^{m_2}}]=1$. Since $[a_1,a_3,a_1]=1$, $[a_1^p,a_3]=[a_1,a_3]^p=1$. Since $G'\not\leq\langle a_2,a_3a_1^{p^{m_1-m_3+1}}\rangle$, $[a_2,a_3a_1^{p^{m_1-m_3+1}}]=1$. It follows that

$$1=[a_1^{p^{m_1-m_3+1}},a_2]=a_1^{p^{2m_1-m_3+1}}.$$

Hence $2m_1-m_3+1\geq m_1+1+k$. That is, $m_1-m_3\geq k$. Since $G'\not\leq\langle a_1,a_2^{p^{m_2-m_3+2}}a_3^p\rangle$, $[a_1,a_2^{p^{m_2-m_3+2}}a_3^p]=1$. It follows that

$$a_1^{a_2^{p^{m_2-m_3+2}}}=a_1^{(1+p^{m_1})^{p^{m_2-m_3+2}}}=a_1.$$

By Lemma 4.3 and Lemma 4.4, in the multiplicative group consisting of all invertible elements of $\mathbb{Z}/p^{m_1+1+k}\mathbb{Z}$, the order of $1+p^{m_1}$ is p^{k+1}. Hence we have $m_2-m_3+2\geq k+1$. That is, $k\leq m_2-m_3+1$.

Let $b\in A$ and the order of b be p^e. Since $G'\not\leq\langle a_1,a_2^{p^{m_2-e+1}}b\rangle$, $[a_1,a_2^{p^{m_2-e+1}}b]=1$. It follows that $a_1^{a_2^{p^{m_2-e+1}}}=a_1^{(1+p^{m_1})^{p^{m_2-e+1}}}=a_1$. By Lemma 4.3 and Lemma 4.4, in the multiplicative group consisting of all invertible elements of $\mathbb{Z}/p^{m_1+1+k}\mathbb{Z}$, the order of $1+p^{m_1}$ is p^{k+1}. Hence we have $m_2-e+1\geq k+1$. That is, $e\leq m_2-k$. By the arbitrariness of b, $\exp(A)\leq p^{m_2-k}$.

Assume that $a_3^p=a_1^{vp^{m_1+1}}$. Replacing a_3 with $a_3a_1^{-vp^{m_1}}$, we have $a_3^p=1$.

Assume that $[a_1,a_3]=a_2^{p^{m_2}}a_1^{wp^{m_1+1}}$. Then $a_2^{p^{m_2+1}}a_1^{wp^{m_1+2}}=1$. Replacing a_2 with $a_2a_1^{wp^{m_1-m_2+1}}$, we have $a_2^{p^{m_2+1}}=1$ and $[a_1,a_3]=a_2^{p^{m_2}}$. Hence G is a group of Type (G2) in Theorem 4.1. □

Summarizing, we have the following

Main Theorem. Suppose that G is a finite metahamiltonian p-group. If $\exp(G')=p$, then G is one of the groups listed in Theorem 3.1. If $\exp(G')>p$, then G is one of the groups listed in Theorem 4.1.

References

[1] An L J, Hu R F, Zhang Q H. Finite p-groups with a minimal non-abelian subgroup of index p (IV), J Algebra Appl, 2015, 14(2): 1550020, 54pp

[2] An L J, Li L L, Qu H P et al. Finite p-groups with a minimal non-abelian subgroup of index p (II), Sci China Math, 2014, 57: 737-753

[3] An L J, Peng J. Finite p-groups in which any two noncommutative elements generate an inner abelian group of order p^4. Algebra Colloq, 2013, 20:215–226

[4] An L J, Zhang Q H. Finite metahamilton p-groups, J Algebra, 2015, 442:23–35

[5] Berkovich Y. Finite p-groups with few minimal nonabelian subgroups, J Algebra, 2006, 297: 62–100

[6] Berkovich Y, Janko Z. Structure of finite p-groups with given subgroups, Contemp Math 402, Amer Math Soc, Providence, RI, 2006: 13–93

[7] Berkovich Y, Janko Z. Groups of Prime Power Order, Vol.2. Berlin: Walter de Gruyter, 2008

[8] Blackburn N. On prime power groups with two generators, Proc Cambrige Phil Soc, 1957, 54: 327–337

[9] Dedekind R. Über Gruppen, deren samtliche Teiler Normalteiler sind. Math Ann, 1897, 48: 548–561

[10] Draganyuk S V. On the structure of finite primary groups all 2-maximal subgroups of which are abelian (Russian), in Complex analysis, Algebra and topology, Akad Nauk Ukrain SSR, Inst Mat, Kiev, 1990: 42–51

[11] Kazarin L S. On certain classes of finite groups. Dokl Akad Nauk SSSR (Russian), 1971, 197: 773–776

[12] King B W. Presentations of metacyclic groups. Bull Austral Math Soc, 1973, 8: 103-131

[13] Nagrebeckii V T. Finite non-nilpotent groups, any non-abelian subgroup of which is normal. Ural Gos Univ Mat Zap, 1967, 6: 80–88

[14] Newman M F, Xu M Y. Metacyclic groups of prime-power order (Research announcement). Adv in Math (Beijing), 1988, 17: 106-107

[15] Passman D S. Nonnormal subgroups of p-groups. J Algebra, 1970, 15: 352–370

[16] Qu H P, Yang S S, Xu M Y et al. Finite p-groups with a minimal non-abelian subgroup of index p (I), J Algebra, 2012, 358: 178–188.

[17] Qu H P, Xu M Y, An L J. Finite p-groups with a minimal non-abelian subgroup of index p (III), Sci China Math, 2015, 58: 763-780

[18] Qu H P, Zhao L P, Gao J et al. Finite p-groups with a minimal non-abelian subgroup of index p (V), J Algebra Appl, 2014, 13(7): 1450032(35 pages)

[19] Rédei L. Das "schiefe Produkt" in der Gruppentheorie mit Anwendung auf die endlichen nichtkommutativen Gruppen mit lauter kommutativen echten Untergruppen und die Ordnungszahlen, zu denen nur kommutative Gruppen gehören(German). Comm Math Helvet, 1947, 20: 225-264

[20] Sheriev V A. A description of the class of finite p-groups whose 2-maximal subgroups are all abelian II, in Primary groups. Proc Sem Algebraic Systems, 1970, 2: 54–76

[21] Xu M Y, An L J, Zhang Q H. Finite p-groups all of whose non-abelian proper subgroups are generated by two elements, J Algebra, 2008, 319: 3603–3620

[22] Xu M Y, Zhang Q H. A classification of metacyclic 2-groups, Algebra Colloq, 2006, 13: 25–34

[23] Zhang Q H, Guo X Q, Qu H P et al. Finite groups which have many normal subgroups, J Korean Math Soc, 2009, 46: 1165-1178

[24] Zhang Q H, Li X X, Su M J. Finite p-groups whose nonnormal subgroups have orders at most p^3, Front Math China, 2014, 9(5): 1169-1194

[25] Zhang Q H, Su M J. Finite 2-groups whose nonnormal subgroups have orders at most 2^3, Front Math China, 2012, 7(5): 971-1003

[26] Zhang Q H, Sun X J, An L J, et al. Finite p-groups all of whose subgroups of index p^2 are abelian, Algebra Colloq, 2008, 15: 167-180

[27] Zhang Q H, Zhao L B, Li M M et al. Finite p-groups all of whose subgroups of index p^3 are abelian, Commun Math Stat, 2015, 3(1): 69-162