Chin. Ann. Math.
31B(4), 2010, 497–506
DOI: 10.1007/s11401-010-0590-7

Chinese Annals of Mathematics, Series B

Finite p-Groups in Which the Number of Subgroups of Possible Order Is Less Than or Equal to p^3 ***

Haipeng QU* Ying SUN* Qinhai ZHANG**

Abstract In this paper, groups of order p^n in which the number of subgroups of possible order is less than or equal to p^3 are classified. It turns out that if $p > 2$, $n \geq 5$, then the classification of groups of order p^n in which the number of subgroups of possible order is less than or equal to p^3 and the classification of groups of order p^n with a cyclic subgroup of index p^2 are the same.

Keywords Inner abelian p-groups, Metacyclic p-groups, Groups of order p^n with a cyclic subgroup of index p^2, The number of subgroups
2000 MR Subject Classification 20D15

1 Introduction

The enumeration problem of p-groups is important in the study of finite p-groups, which includes two aspects: one is to study the number of subgroups, elements and subsets of finite p-groups, the other is to study the structure or properties of finite p-groups by means of the number of subgroups. For example, two well-known counting theorems are as follows.

Theorem 1.1 (see [1]) *Assume that G is a group of order p^n, $0 \leq k \leq n$. $s_k(G)$ denotes the number of subgroups of order p^k of G. Then $s_k(G) \equiv 1 \pmod{p}$.*

Theorem 1.2 (see [2]) *Assume that G is a non-cyclic group of order p^n, $p > 2$. If $1 \leq k \leq n-1$, then $s_k(G) \equiv 1 + p \pmod{p^2}$.*

For the possible cases of the number $s_k(G)$ of subgroups of a finite p-group G $\pmod{p^3}$, Hua and Tuan [3], and Berkovich [4] investigated this question and obtained some results. For example, we see the following theorems.

Theorem 1.3 (see [3]) *Assume that G is a group of order p^n, $p \geq 3$, $\exp(G) = p^{n-\alpha}$ and $n \geq 2\alpha + 1$. If $2\alpha + 1 \leq k \leq n$, then*

$$s_k(G) \equiv 1,\ 1+p,\ 1+p+p^2 \text{ or } 1+p+2p^2 \pmod{p^3}.$$

Theorem 1.4 (see [4]) *Assume that G is a group of order p^n, $p \geq 2$ and $\exp(G) = p$. Then for $1 < k < n-1$, $s_k(G) \equiv 1 + p + 2p^2 \pmod{p^3}$.*

Manuscript received September 7, 2009. Published online June 21, 2010.
*Department of Mathematics, Shanxi Normal University, Linfen 041004, Shanxi, China.
E-mail: quhaipeng@yahoo.cn orcawhale@163.com
**Corresponding author. Department of Mathematics, Shanxi Normal University, Linfen 041004, Shanxi, China. E-mail: zhangqh@dns.sxnu.edu.cn
***Project supported by the National Natural Science Foundation of China (No. 10671114), the Shanxi Provincial Natural Science Foundation of China (No. 2008012001) and the Returned Abroad-Student Fund of Shanxi Province (No. [2007]13–56).

How many possible cases does the number of subgroups of a finite p-group G (mod p^3) have? Up to now, the problem has no complete answer. Hua and Tuan had ever guessed: for an arbitrary finite p-group G, if $p > 2$, then $s_k(G) \equiv 1,\ 1+p,\ 1+p+p^2$ or $1+p+2p^2$ (mod p^3) (see [5, Problem 1]). For brief, in the following the conjecture is called Hua-Tuan's conjecture.

By Hua-Tuan's conjecture, for an arbitrary finite p-group G, if $p > 2$, then the least number of subgroups of possible order is one of $1,\ 1+p,\ 1+p+p^2$ or $1+p+2p^2$. Obviously, to study the structure of finite p-groups which have such number of subgroups is an interesting question. In fact, by Hall's enumeration principle, groups of order p^n in which the number of subgroups of possible order is less than or equal to $1+p$ are classified in [6]. In this paper, we classified groups of order p^n in which the number of subgroups of possible order is less than or equal to $1+p+2p^2$. We find that classifying groups of order p^n in which the number of subgroups of possible order is less than or equal to $1+p+2p^2$ is equivalent to classifying groups of order p^n in which the number of subgroups of possible order is less than or equal to p^3. It follows that classifying groups of order p^n in which the number of subgroups of possible order is less than or equal to $1+p+2p^2$ is equivalent to classifying groups of order p^n in which the number of subgroups of possible order is less than or equal to $1+p+tp^2$ $(2 < t < p)$. In particular, if $p > 2$, $n \geq 5$, then the classification of groups of order p^n in which the number of subgroups of possible order is less than or equal to p^3 and the classification of groups of order p^n with a cyclic subgroup of index p^2 are the same. This implies that Hua-Tuan's conjecture is true for finite p-groups with a cyclic subgroup of index p^2. However, Hua-Tuan's conjecture is not true for general cases (see [7]).

For $p = 2$, we also classified groups of order 2^n in which the number of subgroups of possible order is less than or equal to 2^3 by means of the method of central extension. Thus finite p-groups in which the number of subgroups of possible order is less than or equal to p^3 are completely classified.

For convenience, we use $s_k(G)$ and $c_k(G)$ to denote the number of subgroups of order p^k of a finite p-group G and the number of cyclic subgroups of order p^k of a finite p-group G, respectively; C_n and C_n^m to denote the cyclic group of order n and the direct product of m cyclic groups of order n, respectively; G_n to denote the nth term of lower central series of a p-group G; $H * K$ to denote a central product of H and K; and $c(G)$ and $d(G)$ to denote the nilpotency class and minimal number of generators, respectively.

Let G be a finite p-group. For an integer i, we define $\Lambda_i(G) = \{a \in G \mid a^{p^i} = 1\}$, $V_i(G) = \{a^{p^i} \mid a \in G\}$, $\Omega_i(G) = \langle \Lambda_i(G) \rangle = \langle a \in G \mid a^{p^i} = 1 \rangle$, and $\mho_i(G) = \langle V_i(G) \rangle = \langle a^{p^i} \mid a \in G \rangle$; G is called p^i-abelian if $(ab)^{p^i} = a^{p^i} b^{p^i}$ for all $a, b \in G$; G is called inner abelian if G is non-abelian, but every proper subgroup of G is abelian; G is called meta-abelian if $G'' = 1$.

The concepts and symbols in this paper are referred to [8].

2 The Classification of Finite p-Groups with $s_k(G) \leq p^3$

2.1 Preliminaries

Lemma 2.1 (see [9] or [8, p. 339]) *Finite 2-groups are maximal class if and only if* $|G : G'| = 4$.

Lemma 2.2 (see [10]) *Assume that G is an inner abelian p-group. Then G is one of the following:*

(1) Q_8;

(2) $M(n,m) = \langle a, b \mid a^{p^n} = b^{p^m} = 1,\ a^b = a^{1+p^{n-1}} \rangle,\ n \geq 2$ (*metacyclic*);

(3) $M(n,m,1)=\langle a,b,c \mid a^{p^n}=b^{p^m}=c^p=1,\ [a,b]=c,\ [c,a]=[c,b]=1\rangle,\ n\geq m$. *If* $p=2$, $m+n\geq 3$ *(non-metacyclic).*

Theorem 2.1 (see [11]) *Assume that G is a group of order p^n, $p>2$, $n\geq 5$. Then G has a cyclic subgroup of index p^2 if and only if G is isomorphic to one of the following:*

(I) *Abelian groups*

(1) C_{p^n}; (2) $C_{p^{n-1}}\times C_p$; (3) $C_{p^{n-2}}\times C_{p^2}$; (4) $C_{p^{n-2}}\times C_p\times C_p$;

(II) $d(G)=2$ *and* $|G'|=p$

(5) $M(n-1,1)$; (6) $M(n-2,2)$; (7) $M(2,n-2)$; (8) $M(n-2,1,1)$;

(III) $d(G)=2$ *and* $|G'|=p^2$

(9) $\langle a,b \mid a^{p^{n-2}}=b^p=c^p=1,\ [a,b]=c,\ [a,c]=1,\ [b,c]=a^{\nu p^{n-3}}\rangle$, *$\nu$ is 1 or a fixed quadratic non-residue* (mod p)*;*

(10) $\langle a,b \mid a^{p^{n-2}}=b^p=c^p=1,\ [a,b]=c,\ [a,c]=a^{p^{n-3}},\ [b,c]=1\rangle$;

(11) $\langle a,b \mid a^{p^{n-2}}=b^{p^2}=1,\ [a,b]=a^{p^{n-4}}\rangle$;

(12) $\langle a,b \mid a^{p^{n-2}}=b^{p^2}=1,\ [a,b]=a^{p^{n-4}}b^p\rangle$;

(IV) $d(G)=3$ *and* $|G'|=p$

(13) $M(n-2,1)\times C_p$; (14) $M(1,1,1)*C_{p^{n-2}}$.

Here we give a new and short proof to the following theorem due to [6].

Theorem 2.2 (see [6]) *Assume that G is a group of order p^n. Then for $1\leq k\leq n-1$, $s_k(G)=1+p$ holds if and only if G is one of the following non-isomorphic groups:*

(1) $C_{p^{n-1}}\times C_p$;

(2) $M(n-1,1)$ *except for* D_8.

Proof First we assert that G has a cyclic maximal subgroup. If not, we take two distinct maximal subgroups M_i $(i=1,2)$, then, by hypothesis, $s_{n-2}(M_i)\geq 1+p$. Thus $s_{n-2}(G)\geq s_{n-2}(M_1)+s_{n-2}(M_2)-1\geq 1+2p$, which is a contradiction. By hypothesis and [12], or [1, Theorem 1.2] (i.e., the classification of finite p-groups with a cyclic maximal subgroup), $G\cong C_{p^{n-1}}\times C_p$ or $G\cong M(n-1,1)$ except for D_8. Conversely, if G is the group listed in Theorem 2.2, then for arbitrary integer k $(1\leq k\leq n-1)$, $|\Omega_k(G)|=p^{k+1}$. Thus $c_k(G)=\frac{|\Omega_k(G)|-|\Omega_{k-1}(G)|}{p^k-p^{k-1}}=p$. It follows that $s_k(G)=1+c_k(G)=1+p$.

2.2 The classification of finite p-groups with $s_k(G)\leq p^3$ for $p\neq 2$

First, we give some lemmas, which are necessary for the classification.

Lemma 2.3 *Assume that G is a group of order p^n. If $s_{n-1}(G)\leq p^3$, then $d(G)\leq 3$.*

Proof $s_{n-1}(G)=1+p+p^2+\cdots+p^{d(G)-1}$. It follows by hypothesis that $d(G)-1\leq 2$. That is, $d(G)\leq 3$.

Lemma 2.4 *Assume that G is a finite p-group, $N\trianglelefteq G$. If for arbitrary integer k satisfying $s_k(G)\leq t$, where t is an integer, then $s_k(G/N)\leq t$.*

Proof Assume that $|N|=p^i$, H/N is a subgroup of order p^k of G/N. Then H is a subgroup of order p^{k+i} of G containing N. Thus $s_k(G/N)\leq s_{k+i}(G)\leq t$.

Lemma 2.5 *Assume that G is a group of order p^n,* $\exp(G)=p^e$, *s is a positive integer. If for $1\leq k\leq n$, $c_k(G)\leq p^s$, then $e\geq n-s+1$.*

Proof We assert that for an arbitrary positive integer k, $|\Lambda_k(G)| < p^{k+s}$. In fact, since $c_1(G) = \frac{|\Lambda_1(G)|-1}{\varphi(p)} = \frac{|\Lambda_1(G)|-1}{p-1} \le p^s$, $|\Lambda_1(G)| \le p^{s+1} - p^s + 1 < p^{s+1}$. Assume that the assert is true for $k < m$. When $k = m$, since $c_m(G) = \frac{|\Lambda_m(G)|-|\Lambda_{m-1}(G)|}{\varphi(p^m)} = \frac{|\Lambda_m(G)|-|\Lambda_{m-1}(G)|}{p^{m-1}(p-1)} \le p^s$, $|\Lambda_m(G)| \le p^{s+m} - p^{s+m-1} + |\Lambda_{m-1}(G)| < p^{s+m}$. It follows that the assert is true. In particular, $p^n = |G| = |\Lambda_e(G)| < p^{e+s}$. The conclusion is followed.

Remark 2.1 In particular, when $s = 2$, Lemma 2.5 give another proof for Theorem 2.2.

Lemma 2.6 *Assume that G is a group of order p^n, $p > 2$, $n \ge 5$, $\exp(G) = p^e$. If $e \ge n-2$, then for $1 \le k \le n$, $s_k(G) \le 1 + p + 2p^2$.*

Proof We discuss by the value of e.

If $e = n$, then G is cyclic, the conclusion is followed. If $e = n-1$, then G has at least a cyclic maximal subgroup. Since $p > 2$, by [1, Theorem 1.2], $G \cong C_{p^{n-1}} \times C_p$ or $M(n-1, 1)$. By Theorem 2.2, for $1 \le k < n$, $s_k(G) = 1 + p$ holds. The conclusion is followed.

If $e = n-2$, then, by Theorem 2.1, $|G'| \le p^2$, $d(G) \le 3$ and G is p^2 abelian. It follows that $\Omega_i(G) = \Lambda_i(G)$ and $d(\Omega_i(G)) \le 3$ $(2 \le i \le e)$. Since $e = n-2$ and $p^n = |G| = |\Omega_2(G)| \prod\limits_{s=3}^{e} \big|\Omega_s(G)/\Omega_{s-1}(G)\big|$, $|\Omega_2(G)| \le p^4$ and $\Omega_2(G) < G$. If $d(G) = 3$, then $|G'| \le p$ by Theorem 2.1. If $d(G) = 2$, then $|G'| \le p^2$ by Theorem 2.1 again. Taking a normal subgroup N of order p of G contained in G'. It is easy to prove that G/N is abelian or inner abelian. It follows that the derived subgroups of all proper subgroups of G are contained in N. Thus we get $|\Omega_2(G)'| \le p$. So $\Omega_2(G)$ is p-abelian. It means that $\Lambda_1(G) = \Lambda_1(\Omega_2(G)) = \Omega_1(\Omega_2(G))$ is a group. It follows that $\Lambda_1(G) = \Omega_1(G)$.

Since $e = n-2$ and $p^n = |G| = |\Omega_1(G)| \prod\limits_{s=2}^{e} \big|\Omega_s(G)/\Omega_{s-1}(G)\big|$, $|\Omega_1(G)| \le p^3$. Since G is not cyclic, $|\Omega_1(G)| \ne p$. We discuss in two cases according to $|\Omega_1(G)| = p^2$ and $|\Omega_1(G)| = p^3$.

Case 1 Assume $|\Omega_1(G)| = p^2$. Then $s_1(G) = \frac{|\Omega_1(G)|-1}{\varphi(p)} = 1 + p$. Since $e = n-2$ and $p^n = |G| = |\Omega_1(G)| \prod\limits_{s=2}^{e} \big|\Omega_s(G)/\Omega_{s-1}(G)\big|$, there exists an integer t such that $\big|\Omega_t(G)/\Omega_{t-1}(G)\big| = p^2$. Moreover, if $2 \le i \le e$ and $i \ne t$, then $\big|\Omega_i(G)/\Omega_{i-1}(G)\big| = p$. Therefore, if $s \le t-1$, then $|\Omega_s(G)| = p^{s+1}$; if $e \ge s \ge t$, then $|\Omega_s(G)| = p^{s+2}$. We calculate the number of subgroups of order p^j $(2 \le j \le n-1)$ of G as follows.

If $2 \le j \le t-1$, then, by $\Omega_i(G) = \Lambda_i(G)$ $(2 \le i \le e)$, $c_j(G) = \frac{|\Omega_j(G)|-|\Omega_{j-1}(G)|}{\varphi(p^j)} = \frac{p^j(p-1)}{p^{j-1}(p-1)} = p$. Since $|\Omega_{j-1}(G)| = p^j$, $s_j(\Omega_{j-1}(G)) = 1$. So $s_j(G) = c_j(G) + s_j(\Omega_{j-1}(G)) = 1 + p$.

If $j = t$, then $c_t(G) = \frac{|\Omega_t(G)|-|\Omega_{t-1}(G)|}{\varphi(p^t)} = \frac{p^t(p^2-1)}{p^{t-1}(p-1)} = p + p^2$. Since $|\Omega_{t-1}(G)| = p^t$, $s_t(\Omega_{t-1}(G)) = 1$. So $s_t(G) = c_t(G) + s_t(\Omega_{t-1}(G)) = 1 + p + p^2$.

If $e \ge j > t$, then $c_j(G) = \frac{|\Omega_j(G)|-|\Omega_{j-1}(G)|}{\varphi(p^j)} = \frac{p^{j+1}(p-1)}{p^{j-1}(p-1)} = p^2$. Since $|\Omega_{j-1}(G)| = p^{j+1}$ and $d(\Omega_{j-1}(G)) \le 3$, $s_j(\Omega_{j-1}(G)) \le 1 + p + p^2$. So $s_j(G) = c_j(G) + s_j(\Omega_{j-1}(G)) = 1 + p + 2p^2$.

If $j = e + 1 = n - 1$, then, by $d(G) \le 3$, we have $s_j(G) \le 1 + p + p^2$.

In this case, $s_k(G) \le 1 + p + 2p^2$ for $1 \le k \le n$.

Case 2 Assume $|\Omega_1(G)| = p^3$. Then $s_1(G) = \frac{|\Omega_1(G)|-1}{\varphi(p)} = 1 + p + p^2$. Since $e = n-2$ and $p^n = |G| = |\Omega_1(G)| \prod\limits_{s=2}^{e} \big|\Omega_s(G)/\Omega_{s-1}(G)\big|$, $\big|\Omega_i(G)/\Omega_{i-1}(G)\big| = p$ for $2 \le i \le e$. Thus $|\Omega_i(G)| = p^{i+2}$ and $c_i(G) = \frac{|\Omega_i(G)|-|\Omega_{i-1}(G)|}{\varphi(p^i)} = \frac{p^{i+1}(p-1)}{p^{i-1}(p-1)} = p^2$. Since $d(\Omega_{i-1}(G)) \le 3$ and $|\Omega_{i-1}(G)| = p^{i+1}$, we have $s_i(\Omega_{i-1}(G)) \le 1 + p + p^2$. So we get $s_i(G) = c_i(G) + s_i(\Omega_{i-1}(G)) \le 1 + p + 2p^2$. Since $d(G) \le 3$, we have $s_{n-1}(G) \le 1 + p + p^2$.

In this case, we also have $s_k(G) \le 1+p+2p^2$ for $1 \le k \le n$.

To sum up, the conclusion is followed.

Remark 2.2 Lemma 2.6 is not true for $p=2$ or $n=4$. For example, D_{2^n} $(n \ge 4)$ and $\langle a,b \mid a^{3^2}=b^3=c^3=1,\ [a,b]=c,\ [c,a]=1,\ [c,b]=a^6\rangle$ are counterexamples.

By Lemmas 2.5 and 2.6, we have the following theorem.

Theorem 2.3 *Assume that G is a group of order p^n, $p>2$, $n \ge 5$, $\exp(G)=p^e$. Then the following conditions are equivalence:*

(1) $e \ge n-2$;

(2) *for* $1 \le k \le n$, $s_k(G) \le 1+p+2p^2$;

(3) *for* $1 \le k \le n$, $s_k(G) \le 1+p+tp^2$, *where* $2<t<p$;

(4) *for* $1 \le k \le n$, $s_k(G) \le p^3$;

(5) *for* $1 \le k \le n$, $c_k(G) \le p^3$.

Theorem 2.3 implies that if $p>2$ and $n \ge 5$, then finite p-groups in which the number of subgroups of possible order is less than or equal to p^3 are exactly those groups listed in Theorem 2.1. It is easy to verify that for p-groups G with $|G| \le p^3$, the number of subgroups of possible order of G is less than or equal to p^3. Therefore, in the case of $p>2$, by Theorem 2.3, we know that in order to classify finite p-groups in which the number of subgroups of possible order is less than or equal to p^3, we only need to consider those groups of order p^4.

Theorem 2.4 *Assume that G is a group of order p^4, where $p>2$. Then for arbitrary integer k, $s_k(G) \le p^3$ holds if and only if G is isomorphic to one of the following:*

(1) C_{p^4}; (2) $C_{p^3} \times C_p$; (3) $C_{p^2} \times C_{p^2}$; (4) $C_{p^2} \times C_p \times C_p$;

(5) $M(3,1)$; (6) $M(2,2)$; (7) $M(2,1,1)$; (8) $M(2,1) * C_{p^2}$;

(9) $\langle a,b \mid a^{p^2}=b^p=c^p=1,\ [a,b]=c,\ [c,a]=1,\ [c,b]=a^{ip}\rangle$, *where $i=1$ or a fixed quadratic non-residue* $(\bmod\ p)$. *If $p=3$, then $i \ne 2$;*

(10) $\langle a,b \mid a^{p^2}=b^p=c^p=1,\ [a,b]=c,\ [c,a]=a^p,\ [c,b]=1\rangle$;

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

Proof By checking the list of groups of order p^4, the conclusion is followed. Conversely, those groups listed in Theorem 2.4 satisfy the hypothesis.

Remark 2.3 By checking the group lists in Theorem 2.4, we know that the restriction for $n \ge 5$ in Theorem 2.3 can be removed.

By Theorems 2.1, 2.3, 2.4, a direct consequence is as follows.

Theorem 2.5 *Assume that G is a finite p-group, $p>2$. Then for arbitrary integer k, $s_k(G) \le p^3$ holds if and only if G is isomorphic to one of the following:*

(I) *Abelian groups*

(1) C_{p^n}; (2) $C_{p^n} \times C_p$; (3) $C_{p^n} \times C_{p^2}$ $(n \ge 2)$; (4) $C_{p^n} \times C_p \times C_p$;

(II) $d(G)=2$ *and* $|G'|=p$

(5) $M(n,1)$ $(n \ge 2)$; (6) $M(n,2)$ $(n \ge 2)$; (7) $M(2,n)$ $(n \ge 3)$; (8) $M(n,1,1)$ $(n \ge 2)$;

(III) $d(G)=2$ *and* $|G'|=p^2$

(9) $\langle a,b \mid a^{p^{n+1}}=b^p=c^p=1,\ [a,b]=c,\ [a,c]=1,\ [b,c]=a^{vp^n}\rangle$, *where $v=1$ or a fixed quadratic non-residue* (mod p). *If $p=3$ and $n=1$, then $v \ne 2$;*

(10) $\langle a,b \mid a^{p^{n+1}}=b^p=c^p=1,\ [a,b]=c,\ [a,c]=a^{p^n},\ [b,c]=1\rangle$;

(11) $\langle a,b \mid a^{p^{n+1}} = b^{p^2} = 1,\ [a,b] = a^{p^{n-1}}\rangle$ $(n \geq 2)$;
(12) $\langle a,b \mid a^{p^{n+1}} = b^{p^2} = 1,\ [a,b] = a^{p^{n-1}}b^p\rangle$ $(n \geq 2)$;
(13) $\langle a,b \mid a^9 = c^3 = 1,\ b^3 = a^3,\ [a,b] = c,\ [c,a] = 1,\ [c,b] = a^{-3}\rangle$;

(IV) *$d(G) = 3$ and $|G'| = p$*

(14) $M(n,1) \times C_p$ $(n \geq 2)$; (15) $M(1,1,1) * C_{p^n}$ $(n \geq 2)$.

Corollary 2.1 *Assume that G is a finite p-group, $p > 2$. Then for arbitrary integer k, $s_k(G) \leq 1 + p + p^2$ holds if and only if G is isomorphic to one of the following:*

(I) *Abelian groups*

(1) C_{p^n}; (2) $C_{p^n} \times C_p$; (3) $C_{p^n} \times C_{p^2}$ $(n \geq 2)$; (4) $C_p \times C_p \times C_p$;

(II) $|G'| = p$

(5) $M(n,1)$ $(n \geq 2)$; (6) $M(n,2)$ $(n \geq 2)$; (7) $M(2,n)$ $(n \geq 3)$; (8) $M(1,1,1)$; (9) $M(1,1,1)* C_{p^2}$;

(III) $|G'| = p^2$

(10) $\langle a,b \mid a^{p^{n+1}} = b^{p^2} = 1,\ [a,b] = a^{p^{n-1}}\rangle$ $(n \geq 2)$;
(11) $\langle a,b \mid a^{p^{n+1}} = b^{p^2} = 1,\ [a,b] = a^{p^{n-1}}b^p\rangle$ $(n \geq 2)$;
(12) $\langle a,b \mid a^{p^2} = b^p = c^p = 1,\ [a,b] = c,\ [a,c] = 1,\ [b,c] = a^{vp}\rangle$, *where $v = 1$ or a fixed quadratic non-residue* (mod p). *If $p = 3$, then $v \neq 2$;*
(13) $\langle a,b \mid a^9 = c^3 = 1,\ a^3 = b^3,\ [a,b] = c,\ [c,b] = 1,\ [c,a] = a^3\rangle$.

Corollary 2.2 *Assume that G is a group of order p^n. Then for $1 \leq k \leq n-1$, $s_k(G) = 1 + p + p^2$ holds if and only if G is isomorphic to one of the following:*

(1) $C_p \times C_p \times C_p$;

(2) $\langle a,b,c \mid a^{p^2} = b^p = c^p = 1,\ [b,c] = a^p,\ [a,b] = [a,c] = 1\rangle \cong M(1,1,1) * C_{p^2} \cong M(2,1) * C_{p^2}$.

2.3 The Classification of Finite 2-Groups with $s_k(G) \leq 2^3$

If G is a finite group of order 2^n with $s_k(G) \leq 2^3$ for $1 \leq k \leq n$, then by Lemma 2.3 we have $d(G) \leq 3$. In the following, we will prove that if $d(G) = 2$, then $|G'| \leq 4$; if $d(G) = 3$, then $|G'| \leq 2$. We discuss in two cases.

Lemma 2.7 *Assume that G is a finite 2-group and $d(G) \leq 2$. If $|G'| \leq 2$, then for arbitrary integer k, $s_k(G) \leq 8$ holds if and only if G is isomorphic to one of the following:*

(1) C_{2^n}; (2) $C_{2^n} \times C_2$; (3) $C_{2^n} \times C_4$ $(n \geq 2)$;

(4) $M(n,1)$; (5) $M(n,2)$; (6) $M(2,m)$ $(m \geq 3)$; (7) Q_8.

Proof Since $d(G) \leqslant 2$ and $|G'| \leqslant 2$, G is abelian or inner abelian.

If $d(G) = 1$, then $G \cong C_{2^n}$.

If $d(G) = 2$ and G is abelian, then it is easy to get $G \cong C_{2^n} \times C_2$ or $G \cong C_{2^n} \times C_{2^2}$.

If $d(G) = 2$ and G is inner abelian, it is easy to check that $s_k(G) \leq 8$ for $1 \leq k \leq 3$ for all groups of order 2^3. Assume $|G| > 2^3$. If $G \cong M(n,m,1)$, then for $i \leq m$, $s_i(G) = 1 + 2 + 2(2^2 + \cdots 2^i) + 2^{i+1}$. By hypothesis, we get $m = 1$, that is, $G \cong M(n,1,1)$. By checking we get $s_2(G) = 1 + 2 + 2^3 > 8$, which is a contradiction. Thus $G \cong M(n,m)$. By calculating, we get $s_i(G) = 1 + 2 + 2^2 + \cdots + 2^i$ for $i \leq \min(m,n)$. By hypothesis, we get $\min(m,n) \leq 2$. It follows that G is isomorphic to one of the following: $M(n,1)$, $M(n,2)$, $M(2,m)$ $(m \geq 3)$. Conversely, it is easy to check that these three groups satisfy the hypothesis. The conclusion holds.

Assume that G is a finite group of order 2^n, $d(G)=2$ and $|G'|=4$. Then there exists a normal subgroup N of order 2 of G contained in G'. If $s_k(G)\le 8$ holds for $1\le k\le n$, then, by Lemma 2.4, $s_k(G/N)\le 8$. Thus, by Lemma 2.7, $G/N\cong M(n,1)$, $M(n,2)$, $M(2,m)$ $(m\ge 3)$ or Q_8. On the other hand, there does not exist a G such that $|G'|=4$ and $G/N\cong Q_8$ by [13, Lemma 8]. Thus, in the following, according to the structure of G/N, we determine G by means of the method of central extension.

Theorem 2.6 *Assume that G is a finite 2-group, $d(G)=2$ and $|G'|=4$. If there exists an $N\le G'$ with $|N|=2$ such that $G/N\cong M(n,1)$, then for arbitrary integer k, $s_k(G)\le 8$ holds if and only if G is isomorphic to one of the following:*

(I) $\langle a,b \mid a^8=b^2=1,\ [a,b]=a^2\rangle\cong SD_{16}$;

(II) $\langle a,b \mid a^8=1,\ b^2=a^4,[a,b]=a^{-2}\rangle\cong Q_{16}$.

Proof Since $|G'|=4$, there exists a subgroup N of order 2 of G contained in G' such that $N\le Z(G)$. Since $G/N\cong M(n,1)$, by [13, Theorem 10], we know that G is isomorphic to one of the following:

(1) $\langle a,b \mid a^8=b^2=1,\ [a,b]=a^2\rangle\cong SD_{16}$;

(2) $\langle a,b \mid a^8=b^2=1,\ [a,b]=a^{-2}\rangle\cong D_{16}$;

(3) $\langle a,b \mid a^8=1,\ b^2=a^4,\ [a,b]=a^{-2}\rangle\cong Q_{16}$.

By calculation, we get that for D_{16}, $s_1(D_{16})=9$, which is contrary to our hypothesis. For SD_{16}, $s_1(SD_{16})=5$, $s_2(SD_{16})=5$, $s_3(SD_{16})=3$; for Q_{16}, $s_1(Q_{16})=1$, $s_2(Q_{16})=5$, $s_3(Q_{16})=3$. Conversely, it is easy to check that these groups listed in the theorem satisfy the hypothesis. The conclusion holds.

Theorem 2.7 *Assume that G is a finite 2-group, $d(G)=2$ and $|G'|=4$. If there exists an $N\le G'$ with $|N|=2$ such that $G/N\cong M(n,2)$, then for arbitrary integer k, $s_k(G)\le 8$ holds if and only if G is isomorphic to one of the following:*

(I) $\langle a,b \mid a^{2^{n+1}}=b^4=1,\ [a,b]=a^{2^{n-1}}\rangle$ $(n\ge 3)$;

(II) $\langle a,b \mid a^8=1,\ b^4=a^4,\ [a,b]=a^{-2}\rangle$.

Proof Since $|G'|=4$, there exists a subgroup N of order 2 of G contained in G' such that $N\le Z(G)$. Since $G/N\cong M(n,2)$, by [13, Theorem 10], we know that G is isomorphic to one of the following four groups:

$H_{(1)}=\langle a,b \mid a^{2^{n+1}}=b^4=1,\ [a,b]=a^{2^{n-1}}\rangle$ $(n\ge 3)$;

$H_{(2)}=\langle a,b \mid a^8=b^4=1,\ [a,b]=a^2\rangle$;

$H_{(3)}=\langle a,b \mid a^8=b^4=1,\ [a,b]=a^{-2}\rangle$;

$H_{(4)}=\langle a,b \mid a^8=1,\ b^4=a^4,\ [a,b]=a^{-2}\rangle$.

For $H_{(1)}$, we have $|H_{(1)}|=2^{n+3}$. Since $[a^4,b]=[a,b]^4=a^{2^{n+1}}=1$, we have $a^4\in Z(H_{(1)})$. By calculation, we get $\Omega_1(H_{(1)})=\Lambda_1(H_{(1)})=\langle a^{2^n},b^2\rangle\cong C_2\times C_2$, $\Omega_i(H_{(1)})=\Lambda_i(H_{(1)})=\langle a^{2^{n+1-i}},b\rangle\cong C_{2^i}\times C_4$ $(2\le i\le n-1)$, $\Omega_n(H_{(1)})=\Lambda_n(H_{(1)})=\langle a^2,b\rangle\cong M(n,2)$, $\Omega_{n+1}(H_{(1)})=\Lambda_{n+1}(H_{(1)})=H_{(1)}$. It follows that $s_1(H_{(1)})=3$, $s_i(H_{(1)})=c_i(H_{(1)})+s_i(\Omega_{i-1}(H_{(1)}))=7$ $(2\le i\le n+1)$, $s_{n+2}(H_{(1)})=3$. So $H_{(1)}$ is the required group.

For $H_{(2)}$ and $H_{(3)}$, we have $s_2(H_{(2)})=s_2(H_{(3)})=11$, so $H_{(2)}$ and $H_{(3)}$ are not the required groups.

For $H_{(4)}$, we have $s_1(H_{(4)})=3$, $s_2(H_{(4)})=3$, $s_3(H_{(4)})=7$, so $H_{(4)}$ is the required groups.

Conversely, it is easy to check that $H_{(1)}$ and $H_{(4)}$ satisfy the hypothesis, respectively. The conclusion holds.

Theorem 2.8 *Assume that G is a finite 2-group, $d(G)=2$ and $|G'|=4$. If there exists an $N\le G'$ with $|N|=2$ such that $G/N\cong M(2,m)$ $(m\ge 3)$, then for arbitrary integer k, $s_k(G)\le 8$ holds if and only if $G\cong\langle a,b\mid a^8=1,\ b^{2^m}=a^4,\ [a,b]=a^{-2}\rangle$ $(m\ge 3)$.*

Proof Since $|G'|=4$, there exists a subgroup N of order 2 of G contained in G' such that $N\le Z(G)$. Since $G/N\cong M(2,m)$ $(m\ge 3)$, by [13, Theorem 10], we know that G is isomorphic to one of the following:

$H_{(1)}=\langle a,b\mid a^8=b^{2^m}=1,\ [a,b]=a^2\rangle$ $(m\ge 3)$;
$H_{(2)}=\langle a,b\mid a^8=b^{2^m}=1,\ [a,b]=a^{-2}\rangle$ $(m\ge 3)$;
$H_{(3)}=\langle a,b\mid a^8=1,\ b^{2^m}=a^4,\ [a,b]=a^{-2}\rangle$ $(m\ge 3)$.

For $H_{(i)}$ $(i=1,2)$, we have $a^4,b^2\in Z(H_{(i)})$. By calculation, we get $\Omega_1(H_{(i)})=\Lambda_1(H_{(i)})=\langle a^4,b^{2^{m-1}}\rangle\cong C_2\times C_2$, $\Omega_2(H_{(i)})=\Lambda_2(H_{(i)})=\langle a^2,b^{2^{m-2}}\rangle\cong C_4\times C_4$, $\Omega_3(H_{(i)})=\Lambda_3(H_{(i)})=\langle a,b^{2^{m-3}}\rangle$, $|\Omega_3(H_{(i)})|=2^6$. It follows that $s_3(H_{(i)})=c_3(H_{(i)})+s_3(\Omega_2(H_{(i)}))=15$. So $H_{(i)}$ $(i=1,2)$ are not the required groups.

For $H_{(3)}$, we have $a^4,b^2\in Z(H_{(3)})$. By calculation, we get $\Omega_1(H_{(3)})=\Lambda_1(H_{(3)})=\langle a^4,a^2b^{2^{m-1}}\rangle\cong C_2\times C_2$; $\Omega_2(H_{(3)})=\Lambda_2(H_{(3)})=\langle a^2,b^{2^{m-1}},ab^{2^{m-2}}\rangle=\langle a^2,ab^{2^{m-2}}\rangle$, $|\Omega_2(H_{(3)})|=2^4$, $\Omega_i(H_{(3)})=\langle a,b^{2^{m-i+1}}\rangle$, $|\Omega_i(H_{(3)})|=2^{i+1}$ $(3\le i\le m+1)$, $\Omega_{m+1}(H_{(3)})=\Lambda_{m+1}(H_{(3)})=H_{(3)}$. It follows that $s_1(H_{(3)})=s_{m+2}(H_{(3)})=3$, $s_i(H_{(3)})=7$ $(2\le i\le m+1)$. So $H_{(3)}$ is the required group. Conversely, it is easy to check that $H_{(3)}$ satisfies the hypothesis.

By Theorems 2.6–2.8 we have the following theorem.

Theorem 2.9 *Assume that G is a finite 2-group, $d(G)=2$ and $|G'|=4$. Then for arbitrary integer k, $s_k(G)\le 8$ holds if and only if G is isomorphic to one of the following:*

(1) $\langle a,b\mid a^8=b^2=1,\ [a,b]=a^2\rangle\cong SD_{16}$;
(2) $\langle a,b\mid a^8=1,\ b^2=a^4,\ [a,b]=a^{-2}\rangle\cong Q_{16}$;
(3) $\langle a,b\mid a^{2^{n+1}}=b^4=1,\ [a,b]=a^{2^{n-1}}\rangle$ $(n\ge 3)$;
(4) $\langle a,b\mid a^8=1,\ b^{2^m}=a^4,\ [a,b]=a^{-2}\rangle$ $(m\ge 2)$.

Theorem 2.10 *Assume that G is a finite 2-group, $d(G)=2$. If for arbitrary integer k, $s_k(G)\le 8$ holds, then $|G'|\le 4$.*

Proof Assume that G is a counterexample of the smallest order. Then $|G'|=2^i$, where $i\ge 3$. Let M be a normal subgroup of order 2^{i-3} of G contained in G'. Then $d(G/M)=2$ and $s_k(G/M)\le 2^3$. Since $|(G/M)'|=2^3$, G/M is also a counterexample. Since G is a counterexample of the smallest order, we have $M=1$. That is, $|G'|=2^3$.

Taking a minimal subgroup N satisfying $N\le Z(G)$. Then $d(G/N)=2$, $s_k(G/N)\le 2^3$ and $|(G/N)'|=2^2$. By Theorem 2.9, G/N is isomorphic to one of the following:

(1) $\langle a,b\mid a^8=b^2=1,\ [a,b]=a^2\rangle\cong SD_{16}$;
(2) $\langle a,b\mid a^8=1,\ b^2=a^4,[a,b]=a^{-2}\rangle\cong Q_{16}$;
(3) $\langle a,b\mid a^{2^{n+1}}=b^4=1,\ [a,b]=a^{2^{n-1}}\rangle$ $(n\ge 3)$;
(4) $\langle a,b\mid a^8=1,\ b^{2^m}=a^4,\ [a,b]=a^{-2}\rangle$ $(m\ge 2)$.

Thus, G can be determined by central extension.

If G is the group which is determined by (1) or (2) by central extension, then, by $|G/G'|=4$ and Lemma 2.1, G is a 2-group of maximal class of order 2^5. But the quotient group of order 2^4 of a 2-group of maximal class of order 2^5 is exactly a dihedral group, which is a contradiction.

If G is the group which is determined by (3) by central extension, letting $G/N=\langle\overline{a},\overline{b}\mid\overline{a}^{2^{n+1}}=\overline{b}^4=1,[\overline{a},\overline{b}]=\overline{a}^{2^{n-1}}\rangle$, we have $G=\langle a,b\rangle$. If $N=\langle x\rangle$, $[a,b]=a^{2^{n-1}}x^i$ $(i=0$ or $1)$, then $[a,b,a]=1$, $[a,b,b]=a^{2^{2n-2}}$. It follows that $G'=\langle a^{2^{n-1}}x^i,a^{2^{2n-2}}\rangle=\langle a^{2^{n-1}}x^i\rangle$. Since $|G'|=8$, we have $o(a) = 2^{n+2}$. Hence $N = \langle a^{2^{n+1}} \rangle$. Assume $[a,b] = a^{2^{n-1}} a^{k2^{n+1}} = a^{2^{n-1}(1+4k)}$ ($k = 0$ or 1). Let $l = 1 + 4k$. Then $a^b = a^{2^{n-1}l+1}$, $(l, 2) = 1$. Since $b^4 \in N \leq Z(G)$, we have $a = a^{b^4} = a^{(1+l2^{n-1})^4} = a^{1+l2^{n+1}} \neq a$, which is a contradiction.

If G is the group which is determined by (4) by central extension, letting $G/N = \langle \overline{a}, \overline{b} \mid \overline{a}^8 = 1,\ \overline{b}^{2^m} = \overline{a}^4,\ [\overline{a}, \overline{b}] = \overline{a}^{(-2)} \rangle$ ($m \geq 2$), $N = \langle x \rangle$ and $[a,b] = a^6 x^i$ ($0 \leq i < 2$), we get $[a,b,a] = 1$, $[a,b,b] = a^{36}$. It follows that $G' = \langle a^6 x^i, a^{36} \rangle = \langle a^6 x^i \rangle$. Since $|G'| = 8$, we have $o(a) = 2^4$. Thus, $1 = [b^{2^m}, b] = [a^4, b] = [a,b]^4 = a^8 \neq 1$, which is a contradiction.

Theorem 2.11 *Assume that G is a finite 2-group, $d(G) = 3$ and $|G'| \leq 2$. Then for arbitrary integer k, $s_k(G) \leq 8$ holds if and only if G is isomorphic to one of the following:*

(I) $C_2 \times C_2 \times C_2$;

(II) $\langle a,b,c \mid a^4 = 1,\ a^2 = b^2,\ c^2 = 1,\ [a,b] = a^2,\ [c,a] = [c,b] = 1 \rangle \cong Q_8 \times C_2$;

(III) $\langle a,b,c \mid a^4 = b^2 = c^2 = 1,\ [b,c] = a^2,\ [a,b] = [a,c] = 1 \rangle \cong D_8 * C_4 \cong Q_8 * C_4$.

Proof If $|G'| = 1$, it follows by $d(G) = 3$ that $G \cong C_2 \times C_2 \times C_2$.

If $|G'| = 2$, then, by Lemma 2.3, $s_k(G/G') \leq 8$ holds for arbitrary integer k. Since $d(G/G') = 3$ and G/G' is abelian, $G/G' \cong C_2 \times C_2 \times C_2$. It follows that G is a group of order 2^4. Since $d(G) = 3$ and $|G'| \leq 2$, by the classification of group of order 2^4, G is isomorphic to one of the following:

$H_{(1)} = \langle a,b,c \mid a^4 = 1,\ b^2 = 1,\ c^2 = 1,\ [a,b] = a^2,\ [c,a] = [c,b] = 1 \rangle \cong D_8 \times C_2$;

$H_{(2)} = \langle a,b,c \mid a^4 = 1,\ b^2 = a^2,\ c^2 = 1,\ [a,b] = a^2,\ [c,a] = [c,b] = 1 \rangle \cong Q_8 \times C_2$;

$H_{(3)} = \langle a,b,c \mid a^4 = b^2 = c^2 = 1,\ [b,c] = a^2,\ [a,b] = [a,c] = 1 \rangle \cong D_8 * C_4 \cong Q_8 * C_4$.

For $H_{(1)}$, we have $s_1(H_{(1)}) = 11$. So $H_{(1)}$ is not the required group. For $H_{(2)}$, we have $s_1(H_{(2)}) = 3$, $s_2(H_{(2)}) = s_3(H_{(2)}) = 7$. For $H_{(3)}$, we have $s_1(H_{(3)}) = s_2(H_{(3)}) = s_3(H_{(3)}) = 7$. So $H_{(2)}$ and $H_{(3)}$ are the required groups. Conversely, it is easy to check that $H_{(2)}$ and $H_{(3)}$ satisfy the hypothesis, respectively.

Theorem 2.12 *Assume that G is a finite 2-group, $d(G) = 3$. If for arbitrary integer k, $s_k(G) \leq 8$ holds, then $|G'| \leq 2$.*

Proof Assume that G is a counterexample of the smallest order. Then $|G'| = 2^i$, where $i \geq 2$. Let M be a normal subgroup of order 2^{i-2} of G contained in G'. Then $d(G/M) = 3$, $s_k(G/M) \leq 2^3$. Since $|(G/M)'| = 2^2$, G/M is also a counterexample. But G is a counterexample of the smallest order, so $M = 1$. That is, $|G'| = 2^2$.

Taking a normal subgroup N of order 2 of G contained in G', we have $d(G/N) = 3$, $s_k(G/N) \leq 2^3$, $|(G/N)'| = 2$. By Lemma 2.11, G/N is isomorphic to one of the following:

(1) $\langle \overline{a}, \overline{b}, \overline{c} \mid \overline{a}^4 = 1,\ \overline{a}^2 = \overline{b}^2, \overline{c}^2 = 1,\ [\overline{a}, \overline{b}] = \overline{a}^2,\ [\overline{c}, \overline{a}] = [\overline{c}, \overline{b}] = 1 \rangle \cong Q_8 \times C_2$;

(2) $\langle \overline{a}, \overline{b}, \overline{c} \mid \overline{a}^4 = \overline{b}^2 = \overline{c}^2 = 1,\ [\overline{b}, \overline{c}] = \overline{a}^2,\ [\overline{a}, \overline{b}] = [\overline{a}, \overline{c}] = 1 \rangle \cong D_8 * C_4 \cong Q_8 * C_4$.

Thus, G can be determined by central extension.

Note $G' = \langle a^2 \rangle N$. It is easy to see that $[a^2, b] = [a^2, c] = 1$. It follows that $G' \leq Z(G)$, $c(G) = 2$. If G is the group which is determined by (1) by central extension, then $1 = [a^2, b] = [a,b]^2 = a^4$. If G is the group which is determined by (2) by central extension, then, by $c^2 \in N$, $1 = [b, c^2] = [b,c]^2 = a^4$. That is, $o(a) = 4$. So $\exp(G) = \exp(G/N)$. It follows that $|\Lambda_2(G)| = |G| = 2^5$. But by the argument of Lemma 2.5, we get $|\Lambda_2(G)| < 2^5$. This is a contradiction.

Theorem 2.13 *Assume that G is a finite 2-group. Then for arbitrary integer k, $s_k(G) \leq 8$ holds if and only if G is isomorphic to one of the following:*

(I) *Abelian groups*

(1) C_{2^n}; (2) $C_{2^n} \times C_2$; (3) $C_{2^n} \times C_4$ $(n \geq 2)$; (4) $C_2 \times C_2 \times C_2$;

(II) $d(G) = 2$ *and* $|G'| = 2$

(5) $M(n, 1)$; (6) $M(n, 2)$ $(n \geq 2)$; (7) $M(2, m)$ $(m \geq 3)$; (8) Q_8;

(III) $d(G) = 2$ *and* $|G'| = 4$

(9) $\langle a, b \mid a^8 = b^2 = 1,\ [a, b] = a^2 \rangle \cong SD_{16}$;

(10) $\langle a, b \mid a^8 = 1,\ b^2 = a^4,\ [a, b] = a^{-2} \rangle \cong Q_{16}$;

(11) $\langle a, b \mid a^{2^{n+1}} = b^4 = 1,\ [a, b] = a^{2^{n-1}} \rangle$ $(n \geq 3)$;

(12) $\langle a, b \mid a^8 = 1,\ b^{2^m} = a^4,\ [a, b] = a^{-2} \rangle$ $(m \geq 2)$;

(IV) $d(G) = 3$

(13) $\langle a, b, c \mid a^4 = 1,\ a^2 = b^2,\ c^2 = 1,\ [a, b] = a^2,\ [c, a] = [c, b] = 1 \rangle \cong Q_8 \times C_2$;

(14) $\langle a, b, c \mid a^4 = b^2 = c^2 = 1,\ [b, c] = a^2,\ [a, b] = [a, c] = 1 \rangle \cong D_8 * C_4 \cong Q_8 * C_4$.

Proof By Lemma 2.3, we get $d(G) \leq 3$. By Theorems 2.12 and 2.10, we have $|G'| \leq 4$. Thus the conclusion is followed by Theorems 2.7, 2.9 and 2.11.

Corollary 2.3 *Assume that G is a group of order 2^n. Then for $1 \leq k < n$, $s_k(G) = 7$ holds if and only if G is isomorphic to one of the following:*

(1) $C_2 \times C_2 \times C_2$;

(2) $\langle a, b, c \mid a^4 = b^2 = c^2 = 1,\ [b, c] = a^2,\ [a, b] = [a, c] = 1 \rangle \cong D_8 * C_4 \cong Q_8 * C_4$.

Corollary 2.4 *Assume that G is a finite 2-group. Then for arbitrary integer k, $s_k(G) \leq 5$ holds if and only if G is isomorphic to one of the following:*

(1) C_{2^n}; (2) $C_{2^n} \times C_2$; (3) $M(n, 1)$;

(4) $\langle a, b \mid a^8 = b^2 = 1,\ [a, b] = a^2 \rangle \cong SD_{16}$;

(5) $\langle a, b \mid a^8 = 1,\ b^2 = a^4,\ [a, b] = a^{-2} \rangle \cong Q_{16}$.

References

[1] Berkovich, Y., Groups of Prime Power Order I, Walter de Gruyter, Berlin, 2008.

[2] Kulakoff, A., Über die Anzahl der eigentlichen Untergruppen und der Elemente von gegebener Ordnung in p-Gruppen, *Math. Ann.*, **104**, 1931, 778–793.

[3] Tuan, H. F., An "Anzahl" theorem of Kulakoff's type for p-groups, *Sci. Rep. Nat. Tsing-Hua Univ. Ser. A.*, **5**, 1948, 182–189.

[4] Berkovich, Y., On the number of subgroups of given order in a finite p-group of exponent p, *Proc. Amer. Math. Soc.*, **109**, 1990, 875–879.

[5] Xu, M. Y., Some Problems on Finite p-Groups (in Chinese), *Adv. Math.*, **14**(3), 1985, 205–226.

[6] Chen, Y. H. and Cao, H. P., The complete classification of p-group with $p+1$ nontrivial subgroups of each order (in Chinese), *J. Southwest Univ.*, **29**(2), 2007, 11–14.

[7] Zhang, Q. H. and Qu, H. P., On Hua-Tuan's conjecture, *Sci. in China Ser. A, Math.*, **52**(2), 2009, 389–393.

[8] Huppert, B., Endliche Gruppen I, Springer-Verlag, Berlin, 1967.

[9] Taussky, O., Remark on the class field tower, *J. London Math. Soc.*, **12**, 1937, 82–85.

[10] Rédei, L., Das schiefe product in der Gruppentheorie, *Comm. Math. Helvet*, **20**, 1947, 225–267.

[11] Hua, L. K. and Tuan, H. F., Determination of the groups of odd-prime-power order p^n which contain a cyclic subgroup of index p^2, *Sci. Rep. Nat. Tsing Hua Univ. Ser. A.*, **4**, 1940, 145–151.

[12] Burnside, W., Theory of Groups of Finite Order, Cambridge University Press, London, 1897.

[13] Li, L. L., Qu, H. P. and Chen, G. Y., Central extension of inner abelian p-groups I (in Chinese), *Acta Math. Sinica*, **53**(4), 2010, to appear.