Quasigroups and Related Systems **26** (2018), 247 − 250

Maximal non-commuting set in finite odd order metacyclic p-group

Pradeep Kumar

Abstract. Let G be a finite group and W be a subset of G. If $ab \neq ba$ for any two distinct elements a and b in W, then W is said to be a non-commuting set. Further, if $|W| \geqslant |X|$ for any other non-commuting set X in G, then W is said to be a maximal non-commuting set. Fouladi and Orfi determined in [3] the size of maximal non-commuting sets in finite non-abelian metacyclic p-groups. Below we give an elementary proof of this result.

1. Introduction

Let G be a finite group and W be a subset of G. If for any two distinct elements $a, b \in W$, $[a,b] = a^{-1}b^{-1}ab \neq 1$, then W is said to be a *non-commuting set*. The size of a maximal non-commuting set is denoted by $w(G)$. Also $w(G)$ is known as the clique number of the non-commuting graph of a finite group G. The non-commuting graph of a finite group G with the center $Z(G)$ is a graph with vertex set $G \backslash Z(G)$ and two vertices are joined if and only if they do not commute. Moreover, $w(G)$ is related to the index of $Z(G)$. Namely, as proved Pyber [7], there is a constant c such that $|G : Z(G)| \leqslant c^{w(G)}$. By a famous result of Neumann [6], answering Erdős's question, the finiteness of $w(G)$ is equivalent to the finiteness of the factor group $G/Z(G)$. More interesting results on $w(G)$ one can find in [1, 3, 4].

In this paper, we give an elementary proof of the theorem of Fouladi and Orfi for finite non-abelian metacyclic p-groups, i.e., finite non-abelian p-groups G with a cyclic normal subgroup H such that the factor group G/H is also cyclic.

2. Preliminaries

We will start with the basic facts that will be needed later.

Lemma 1. (cf. [4]) *Let G be a group and W be a non-commuting set in G such that $G = \bigcup_{a \in W} C_G(a)$ and $C_G(a)$ is abelian for each $a \in W$. Then W is a maximal non-commuting set in G, and $w(G) = |W|$.*

2010 Mathematics Subject Classification: 20D15
Keywords: Metacyclic p-group, non-commuting set, centralizer.

Proposition 1. (cf. [2, Proposition 1]) *Let n be a natural number and p be a prime number. Let $V_p(n)$ denote the exact power of p dividing n. If $k \equiv 1 (\mathrm{mod}\, p)$ and $p > 2$, then $V_p(n) = V_p(1 + k + k^2 + \cdots + k^{n-1})$.*

Lemma 2. *Let $k \equiv 1\, (\mathrm{mod}\, p)$, $1 \leqslant t \leqslant p^l$ and p be an odd prime number. Then $1 + k + k^2 + k^3 + \cdots + k^{t-1} \equiv 0\, (\mathrm{mod}\, p^l)$ if and only if $t = p^l$. Moreover, if $gcd(t, p) = 1$, then $gcd(1 + k + \cdots + k^{t-1}, p) = 1$.*

Proof. This follows from Proposition 1. □

Let G be a finite odd order non-ablelian metacyclic p-group and $\langle a\rangle$ be a cyclic subgroup generated by element $a \in G$. Further, suppose a is such that $\langle a\rangle \trianglelefteq G$ and $G/\langle a\rangle$ is cyclic. Then there exists an element $b \in G$ and a number $k \geqslant 1$ such that $G = \langle b, a\rangle$ and $b^{-1}ab = a^k$. Every element of G can be written in the form $b^j a^i$ for $i, j \geqslant 0$. For more details see [8]. Let $\gamma_2(G)$ denote the commutator subgroup of the group G. With above notation, we have the following two lemmas:

Lemma 3. (cf. [3, Lemma 2.1])
1. $k \equiv 1(\mathrm{mod}\, p)$.
2. *Any two arbitrary elements $g_1 = b^j a^i$ and $g_2 = b^s a^r$ in G commute if and only if $(1 + k + k^2 + \cdots + k^{s-1})i \equiv (1 + k + k^2 + \cdots + k^{j-1})r(\mathrm{mod}\, |\gamma_2(G)|)$, where $i, j, r, s \geqslant 0$ and take $1 + k + \cdots + k^{n-1} = 0$ for $n = 0$.*
3. $(ba^i)^r = b^r a^{i(1+k+\cdots+k^{r-1})}$ *for $i, r \geqslant 1$.*

Lemma 4. (cf. [5]) *If $|\gamma_2(G)| = p^l$, then $Z(G) = \langle b^{p^l}, a^{p^l}\rangle$.*

3. Construction of a maximal non-commuting set

We will construct a maximal non-commuting set by a method used in [4].

Let $G = \langle b, a\rangle$, where $b^{-1}ab = a^k$, be a non-abelian metacylic p-group of a finite odd order and $|\gamma_2(G)| = p^l$.

We will construct a non-commuting set X in G. It is clear that the elements of X are contained in distinct non-trivial cosets of $Z(G)$ in G. By Lemma 4, we have

$$G = Z(G) \cup A_1 \cup A_2 \cup \Big(\bigcup_{s=1}^{p^l-1} A_{3,s}\Big),$$

where $A_1 = \bigcup_{i=1}^{p^l-1} b^i Z(G)$, $A_2 = \bigcup_{i=1}^{p^l-1} a^i Z(G)$ and $A_{3,s} = \bigcup_{i=1}^{p^l-1} b^s a^i Z(G)$ for $1 \leqslant s \leqslant p^l - 1$.

It is evident that any two elements of A_m, $m = 1, 2$, commute with each other, so X can contain at most one element from each A_m, $m = 1, 2$. We have that $ba \neq ab$. So, take $b \in A_1$ and $a \in A_2$ in the set X. Now, we determine the possible choices of elements from $A_{3,s}$ that can be included in the set X.

Suppose, $s = 1$. Then $[ba^i, a] = 1$ if and only if $1 \equiv 0(\mathrm{mod}\, p^l)$ (Lemma 3), that is not possible. Again, ba^i commutes with b if and only if $i \equiv 0(\mathrm{mod}\, p^l)$ (Lemma

3). Thus, for $i \in \{1, 2, \ldots, p^l - 1\}$, ba^i does not commute with a, b. Further, if $[ba^i, ba^r] = 1$, then $i \equiv r(\bmod p^l)$ (Lemma 3). Thus, X can contain at most $p^l - 1$ elements from $A_{3,1}$. Now take subset $\{ba^i \mid 1 \leqslant i \leqslant p^l - 1\}$ from $A_{3,1}$ in the set X. Thus $S_1 = \{b, a, ba^i \mid 1 \leqslant i \leqslant p^l - 1\} \subseteq X$.

Now, suppose $\gcd(s, p^l) = 1$ and $s \neq 1$. By Lemma 3, $[b^s a^i, ba^r] = 1$ if and only if $i \equiv r(1 + k + k^2 + \cdots + k^{s-1})(\bmod p^l)$. Since, by Lemma 2, $gcd(1 + k + \cdots + k^{s-1}, p^l) = 1$, so the last congruence has a solution $r \in \{1, 2, \ldots, p^l - 1\}$. Thus for each $b^s a^i \in A_{3,s}$ there exists $r \in \{1, 2, \ldots, p^l - 1\}$ such that $[b^s a^i, ba^r] = 1$. So, X does not contain any element from $A_{3,s}$ in this case.

Again, take $s = p^\alpha$, $1 \leqslant \alpha \leqslant l - 1$. We have $[b^{p^\alpha} a^i, b^{p^\alpha} a^j] = 1$ if and only if $i(1 + k + \cdots + k^{p^\alpha - 1}) \equiv j(1 + k + \cdots + k^{p^\alpha - 1})(\bmod p^l)$ (Lemma 3). By Lemma 2, there exists a positive integer k_1 such that $1 + k + \cdots + k^{p^\alpha - 1} = p^\alpha k_1$, with $\gcd(k_1, p) = 1$. Thus $b^{p^\alpha} a^i$ commutes with $b^{p^\alpha} a^j$ if and only if $i \equiv j(\bmod p^{l-\alpha})$. Again $[b^{p^\alpha} a^i, b^{p^\beta} a^j] = 1$ for $0 \leqslant \beta \leqslant \alpha - 1$ if and only if $i(1 + k + \cdots + k^{p^\beta - 1}) \equiv j(1 + k + \cdots + k^{p^\alpha - 1})(\bmod p^l)$ (Lemma 3). By Lemma 2, there exist positive integers k_1 and k_2 such that $1 + k + \cdots + k^{p^\alpha - 1} = p^\alpha k_1$, with $\gcd(k_1, p) = 1$ and $1 + k + \cdots + k^{p^\beta - 1} = p^\beta k_2$, with $\gcd(k_2, p) = 1$. Thus $b^{p^\alpha} a^i$ commutes with $b^{p^\beta} a^j$ if and only if $ik_2 p^\beta \equiv jk_1 p^\alpha(\bmod p^l)$. The last congruence is equivalent to $ik_2 \equiv jk_1 p^{\alpha-\beta}(\bmod p^{l-\beta})$. Thus if $[b^{p^\alpha} a^i, b^{p^\beta} a^j] = 1$, then $p^{\alpha-\beta} | i$. Further, for given α, β and i such that $p^{\alpha-\beta} | i$, the equation $ik_2 p^\beta \equiv jk_1 p^\alpha(\bmod p^l)$ has a solution j, that is given α, β, i we can find some j such that $[b^{p^\alpha} a^i, b^{p^\beta} a^j] = 1$. Thus, if we choose $b^{p^\alpha} a^i \in A_{3,p^\alpha}$ such that $p | i$, then there exists j such that $b^{p^{\alpha-1}} a^j$ commutes with $b^{p^\alpha} a^i$. Clearly, in $\bigcup_{\alpha=1}^{l-1} A_{3,p^\alpha}$, the set $S_2 = \{b^{p^\alpha} a^i \mid p \nmid i, 1 \leqslant i \leqslant p^{l-\alpha}, 1 \leqslant \alpha \leqslant l - 1\}$ is non-commuting and its elements do not commute with any element of S_1. Thus, $S_1 \cup S_2 \subseteq X$.

Further, take $s = mp^\alpha$ for fixed α with $\gcd(m, p) = 1$ and $m \neq 1$. Take an arbitrary element $b^{mp^\alpha} a^i \in A_{3,mp^\alpha}$. Now for $p \nmid i$, $[b^{mp^\alpha} a^i, b^{p^\alpha} a^r] = 1$ if and only if $r(1 + k + \cdots + k^{mp^\alpha - 1}) \equiv i(1 + k + \cdots + k^{p^\alpha - 1})(\bmod p^l)$ (Lemma 3). By Lemma 2, there exist positive integers k_1 and k' such that $1 + k + \cdots + k^{p^\alpha - 1} = p^\alpha k_1$, with $\gcd(k_1, p) = 1$ and $1 + k + \cdots + k^{mp^\alpha - 1} = k' p^\alpha$, with $\gcd(k', p) = 1$. Thus the last congruence is equivalent to $rk' \equiv ik_1(\bmod p^{l-\alpha})$. Since, $\gcd(k', p^{l-\alpha}) = 1$, so for a given i, there exists $r \in \{1, 2, \ldots, p^{l-\alpha}\}$ such that $rk' \equiv ik_1(\bmod p^{l-\alpha})$. Also $p \nmid i$, so $p \nmid r$. Thus $b^{mp^\alpha} a^i$ commutes with $b^{p^\alpha} a^r \in X$. Now, assume $i = t' p^e$, $\gcd(t', p) = 1$ and $1 \leqslant e \leqslant \alpha$. By Lemma 3, $[b^{mp^\alpha} a^{t' p^e}, b^{p^{\alpha-e}} a^r] = 1$ if and only if $t' p^e(1 + k + k^2 + \cdots + k^{p^{\alpha-e} - 1}) \equiv r(1 + k + k^2 + \cdots + k^{mp^\alpha - 1})$. We have $1 + k + k^2 + \cdots + k^{p^{\alpha-e} - 1} = p^{\alpha-e} k_3$ and $1 + k + k^2 + \cdots + k^{mp^\alpha - 1} = p^\alpha k'$, where $p \nmid k_3$ and $p \nmid k'$. Thus $[b^{mp^\alpha} a^{t' p^e}, b^{p^{\alpha-e}} a^r] = 1$ if and only if $t' k_3 \equiv rk'(\bmod p^{l-\alpha})$. Since $\gcd(k', p^{l-\alpha}) = 1$, so the last congruence has the solution $r \in \{1, 2, \ldots, p^{l-\alpha}\}$. Since $p \nmid r$, so $b^{mp^\alpha} a^{t' p^e}$ commutes with $b^{p^{\alpha-e}} a^r \in X$. Again for $i = t' p^e$, $\alpha < e \leqslant l - 1$ and $\gcd(t', p) = 1$, $b^{mp^\alpha} a^i$ commutes with some $ba^r \in X$. Indeed, if $b^{mp^\alpha} a^{t' p^e}$ commutes with ba^r, then $r(1 + k + \cdots + k^{mp^\alpha - 1}) \equiv t' p^e(\bmod p^l)$, that is equivalent to $rk' \equiv t' p^{e-\alpha}(\bmod p^{l-\alpha})$. The last congruence has a solution

$r \in \{1, 2, \ldots, p^l - 1\}$. So, in this case X does not contain any element from $A_{3,s}$.

Thus,

$X = \{b, a\} \cup \{ba^i \mid 1 \leqslant i \leqslant p^l - 1\} \cup \{b^{p^\alpha} a^i \mid p \nmid i, 1 \leqslant i \leqslant p^{l-\alpha} \text{ and } 1 \leqslant \alpha \leqslant l-1\}$ is a non-commuting set in G.

Now, by Lemma 3, it is easy to deduce that $C_G(a) = \langle a, b^{p^l}\rangle$ and $C_G(b) = \langle a^{p^l}, b\rangle$. Thus, $C_G(a)$ and $C_G(b)$ are abelian. Consider $b^{p^\alpha} a^i$ with $p \nmid i$, $1 \leqslant i \leqslant p^{l-\alpha}$ and $1 \leqslant \alpha \leqslant l-1$. Since $p \nmid i$, $G = \langle b, b^{p^\alpha} a^i \rangle$. Thus, $C_G(b^{p^\alpha} a^i) = \langle b^{p^\alpha} a^i, b^{p^l}\rangle$ is abelian. Now for $i \in \{1, 2, \ldots, p^l - 1\}$, by Lemma 3, we have

$$\begin{aligned} C_G(ba^i) &= \{b^r a^s \in G \mid i(1 + k + \cdots + k^{r-1}) \equiv s (\operatorname{mod} p^l), 1 \leqslant r \leqslant o(b)\}, \\ &= \{b^r a^{i(1+k+\cdots+k^{r-1}) + p^l t} \mid 1 \leqslant r \leqslant o(b), t \in \mathbb{Z}\}, \\ &= \{(ba^i)^r a^{p^l t} \mid 1 \leqslant r \leqslant o(b)\} = \langle ba^i, Z(G)\rangle. \end{aligned}$$

Obviously, $C_G(ba^i)$ is abelian. Moreover, from the construction of X it follows that $G = \cup_{x \in X} C_G(x)$. Thus by Lemma 1, X is a maximal non-commuting set and the size of X is equal to

$$|X| = 1 + 1 + (p^l - 1) + \sum_{\alpha=1}^{l-1} \phi(p^{l-\alpha}) = p^l + p^{l-1},$$

where $\phi(n)$ is Euler's function. Hence, we can conclude the following theorem.

Theorem 1. (**Fouladi and Orfi**) *The size of a maximal non-commuting set in a finite non-abelian metacyclic p-group G, $p > 2$ is $p^l + p^{l-1}$, where $|\gamma_2(G)| = p^l$.*

References

[1] **A. Abdollahi, S. Akbari and H. R. Maimani**, *Non-commuting graph of a group*, J. Algebra **298** (2006), 468 – 492.

[2] **F.R. Beyl**, *Cyclic subgroups of the prime residue group*, Am. Math. Mon. **84** (1977), no. 1, 46 – 48.

[3] **S. Fouladi and R. Orfi**, *Maximum size of subsets of pairwise non-commuting elements in finite metacyclic p-groups*, Bull. Aust. Math. Soc. **87** (2013), 18 – 23.

[4] **P. Kumar and V.K. Jain**, *Maximal non-commuting set in 2-generated p-groups of class two*, J. Algebra Appl. **17** (2018), no. 9, 1850164.

[5] **X. Li and J. Zhang**, *Finite p-groups and centralizers of noncentral elements*, Commun. Algebra **41** (2013), 3267 – 3276.

[6] **B. H. Neumann**, *A problem of Paul Erdős on groups*, J. Aust. Math. Soc. Ser. A **21** (1976), 467 – 472.

[7] **L. Pyber**, *The number of pairwise non-commuting elements and the index of the center in a finite group*, J. Lond. Math. Soc. **35** (1987), 287 – 295.

[8] **M. Xu**, *A complete classification of metacyclic p-groups of odd order*, Adv. Math. (Beijing) **12** (1983), 72 – 73.

Received July 3, 2018

Department of Mathematics, Central University of South Bihar, Gaya - 824236, Bihar, India
E-mail: 14p.shaoran@gmail.com