

On Groups with the Same Set of Conjugacy Class Sizes as Nilpotent Groups

Zhou Wei

Sobolev Institute of Mathematics, Novosibirsk 630090, Russia

Email: zhouwyx@outlook.com

Abstract. We construct examples of groups which have the same set of conjugacy class sizes as nilpotent groups, while their center is trivial. This answers a question posed by A. R. Camina in 2006.

2020 Mathematics Subject Classification: 20D15, 20D60.

Keywords: finite group, nilpotent group, conjugacy class.

1 Introduction

Let G be a finite group. In [1], Baer defined the index of x in G , denoted by $\text{Ind}_G(x)$, as $|G : C_G(x)|$, which represents the size of the conjugacy class of G containing x . In [11], Itô defined the conjugate type vector of G as (n_1, n_2, \dots, n_r) , where $n_1 > n_2 > \dots > n_r = 1$ are the indices of all elements in G . Since we are not interested in the ordering of these indices, we will denote the set of indices (sizes of conjugacy classes) by $N(G)$, i.e., $N(G) = \{n_1, n_2, \dots, n_r\}$.

Many authors have studied the relationship between the structure of finite groups and the sizes of their conjugacy classes. Itô proved that if $N(G) = \{1, n\}$, then G must be the direct product of a p -group and an abelian p' -group [11]. Ishikawa proved that the nilpotent class of such groups is at most 3 [10]. More results can be found in [4].

It is easy to see that if G is nilpotent, then $N(G) = N(P_1) \times N(P_2) \times \dots \times N(P_k)$, where P_1, P_2, \dots, P_k are the Sylow subgroups of G . A natural question is whether the converse holds:

Question 1 ([3, Question 1]). *Let G and H be finite groups with H nilpotent. Suppose G and H have the same sets of conjugacy class sizes, is G nilpotent?*

In [6], Cossey proved that every finite set of p -powers containing 1 can be the set of conjugacy class sizes of some p -group. Therefore, the above question can be restated as follows: If $N(G) = \Omega_1 \times \Omega_2 \times \dots \times \Omega_r$, where Ω_i is a finite set of p_i -powers containing 1 and p_1, p_2, \dots, p_r are distinct primes, is G nilpotent? The answer is positive in some special cases. For example, if $N(G) = \{1, p_1^{m_1}\} \times \{1, p_2^{m_2}\} \times \dots \times \{1, p_k^{m_k}\}$, where $p_1^{m_1}, p_2^{m_2}, \dots, p_k^{m_k}$ are powers of distinct primes, then G is nilpotent [5]. More generally, if $N(G) = \{1, n_1\} \times \{1, n_2\} \times \dots \times \{1, n_r\}$, where n_1, n_2, \dots, n_r are pairwise coprime integers, then G is nilpotent [9].

A more general question is as follows:

Question 2 ([8, Question 0.1]). *Let G be a group such that $N(G) = \Omega \times \Delta$. Which Δ and Ω guarantee that $G \cong A \times B$, where A and B are subgroups such that $N(A) = \Omega$ and $N(B) = \Delta$?*

However, the answer to Question 1 is not always true, as some counterexamples are provided in [3]. In that paper, A. R. Camina posed a number of questions about the structure of groups with the same set of conjugacy class sizes as nilpotent groups. One of them is as follows:

Question 3 ([3, Question 4]). *Let G and H be finite groups with H nilpotent. Suppose $N(G) = N(H)$, but G is not nilpotent. Does G have a nontrivial centre?*

Using GAP[7], we find that Question 3 does not have a positive answer in general. The smallest counterexamples are two groups of order $486 = 3^5 \times 2$, with the set of conjugacy class sizes $\{1, 3, 27\} \times \{1, 2\}$. One of them is `SmallGroup(486, 36)`, and the other is `SmallGroup(486, 38)`. Moreover, we constructed the following series of counterexamples.

Main Theorem. *Let p and q be primes such that $p = 2q + 1$. Let $G = H \rtimes (A \rtimes B)$, where H , A and B are defined as follows:*

1) $H = K/N$, where $K = \langle k_1 \rangle \times \langle k_2 \rangle \times \dots \times \langle k_p \rangle$ is the direct product of p cyclic groups of order p , and $N = \langle k_1 k_2 \dots k_p \rangle$;

2) $A \rtimes B$ is a subgroup of the symmetric group Sym_p : $A = \langle \alpha \rangle$ and $B = \langle \beta \rangle$, where $\alpha = (12 \dots p)$ and $\beta = (m_1 \dots m_q)(n_1 \dots n_q)$, with $\{m_1, \dots, m_q, n_1, \dots, n_q\} = \{2, 3, \dots, p\}$. Additionally, $\alpha^\beta = \alpha^r$ where $1 < r < q$ and $r^q \equiv 1 \pmod{p}$. For any $\gamma \in A \rtimes B$ and $k_1^{x_1} k_2^{x_2} \dots k_p^{x_p} N \in H$, $(k_1^{x_1} k_2^{x_2} \dots k_p^{x_p} N)^\gamma = k_1^{x_1} k_2^{x_2} \dots k_p^{x_p} N$.

Then $N(G) = \{1, p, p^{p-2}\} \times \{1, q\}$, and $Z(G) = 1$.

From this theorem, the following corollary can be derived.

Corollary. *Let p and q be primes such that $p = 2q + 1$. Let G , H and A be as defined above. Let $L = P \times Q$, where $P = H \rtimes A$ and $Q = C_{q^2} \rtimes C_q$. Then, we have $N(G) = N(L)$.*

A prime number q such that $2q + 1$ is also a prime is called a Sophie Germain prime. The largest known proven Sophie Germain prime is $2618163402417 \times 2^{1290000} - 1$ [2]. It is conjectured that there are infinitely many Sophie Germain primes, but this has not been proven. So we cannot conclude that there are infinitely many counterexamples to Question 3.

2 Preliminaries

Lemma 1. *Let G be a finite group, $H \leq G$ and $x \in G$. If n is an integer and $(n, |x|) = 1$, then $C_H(x) = C_H(x^n)$.*

Proof. It is clear that $C_H(x) \leq C_H(x^n)$. By Euler's theorem, we have $n^t \equiv 1 \pmod{|x|}$, where $t = \varphi(|x|)$. Hence $x = (x^n)^{n^{t-1}}$ and so $C_H(x^n) \leq C_H(x)$. Therefore $C_H(x) = C_H(x^n)$. \square

Lemma 2. *Let $G = H \rtimes \langle a \rangle$, where H is an abelian group and $(|H|, |a|) = 1$. Then for any element h of H , $\text{Ind}_G(ha) = \text{Ind}_G(a) = |H : C_H(a)|$.*

Proof. Let $|a| = n$. It is easy to verify that $C_G(a) = C_H(a)\langle a \rangle$ and $\text{Ind}_G(a) = |H : C_H(a)|$. Since $(ha)^n = hh^{a^{-1}} \dots h^{a^{1-n}} a^n = hh^{a^{-1}} \dots h^{a^{1-n}} \in H$, n is a divisor of $|ha|$. Let $t = |ha|/n$. We have $(ha)^t$ is an element of order n and $\langle (ha)^t \rangle$ is a complement to H in G . Hence $G = H \rtimes \langle (ha)^t \rangle$ and so $C_G((ha)^t) = C_H((ha)^t)\langle (ha)^t \rangle$. Since $(|H|, n) = 1$, we have $(t, n) = 1$. By Lemma 1, $C_H((ha)^t) = C_H(a^t) = C_H(a)$. Since $C_H(a)\langle (ha)^t \rangle \leq C_G(ha) \leq C_G((ha)^t)$, we have $C_G(ha) = C_H(a)\langle (ha)^t \rangle$. Therefore $\text{Ind}_G(ha) = \text{Ind}_G(a) = |H : C_H(a)|$. \square

3 Proof the main theorem

Let G, A, B, H, N be as defined in the main theorem. For convenience, we use (x_1, x_2, \dots, x_p) to represent the element $k_1^{x_1} k_2^{x_2} \dots k_p^{x_p} N$ of H , $x_1, \dots, x_p \in \mathbb{N}$. Under this notation, we have $(x, x, \dots, x) = 1$, $\forall x \in \mathbb{N}$. We can always set $x_1 = 0$, in which case x_2, \dots, x_p are determined. Let $h = (0, x_2, \dots, x_p) \in H$, $a \in A$, $b \in B$ and $h, a, b \neq 1$. It is clear that $|G| = p^2 q$.

$$(1) |C_H(a)| = p \text{ and } \text{Ind}_G(a) = p^{p-2} q.$$

By Lemma 1, it suffices to consider the case $a = \alpha$, i.e., when $(0, x_2, \dots, x_{p-1}, x_p)^\alpha = (x_p, 0, x_1, \dots, x_{p-1})$. If $h \in C_H(a)$, we have $0 - x_p \equiv x_2 - 0 \equiv \dots \equiv x_p - x_{p-1} \pmod{p}$. If $x_p = 1$, then $h = (0, p-1, p-2, \dots, 1)$. In fact, $C_H(a) = \langle (0, p-1, p-2, \dots, 1) \rangle$. Therefore $|C_H(a)| = p$.

Let $h_1 a_1 b_1 \in C_G(a)$, where $h_1 \in H$, $a_1 \in A$ and $b_1 \in B$. We have $h_1 a_1 b_1 = (h_1 a_1 b_1)^\alpha = h_1^\alpha a_1 b_1^\alpha = h_1^\alpha (a_1 a^{-1} a^{b_1^{-1}}) b_1$. It follows that $h_1 \in C_H(a)$ and $b_1 = 1$. Hence $C_G(a) = C_H(a)A$. Thus, $|C_G(a)| = p^2$ and so $\text{Ind}_G(a) = p^{p-2} q$.

$$(2) |C_H(b)| = p^2 \text{ and } \text{Ind}_G(b) = p^{p-2}.$$

It is easy to verify that $C_G(b) = \langle k_{m_1} \dots k_{m_q} N, k_{n_1} \dots k_{n_q} N \rangle$. Therefore, $C_H(b) = p^2$. Moreover, $C_H(a) \cap C_H(b) = 1$.

If $h_1 a_1 b_1 \in C_G(b)$, then $h_1 a_1 b_1 = (h_1 a_1 b_1)^b = h_1^b a_1^b b_1$. It follows that $h_1 \in C_H(b)$ and $a_1 = 1$. Therefore $C_G(b) = C_H(b)B$. We have $|C_G(b)| = p^2 q$ and so $\text{Ind}_G(b) = p^{p-2}$.

$$(3) \text{Ind}_G(ab) = p^{p-2}.$$

By Sylow's theorems, AB has p Sylow q -subgroups. Since that $p(q-1) + p = pq = |AB|$, every element in $AB - A$ has order q . Hence ab must be contained in some conjugate of B . Thus, $\text{Ind}_G(ab) = \text{Ind}_G(b) = p^{p-2}$.

$$(4) \{ \text{Ind}_G(h) \mid h \in H \} = \{ p, q, pq \}.$$

It is clear that $H \leq C_G(h)$. If $h \in C_G(a)$, then $C_G(h) = HA$ and $\text{Ind}_G(h) = q$. If $h \in C_G(b)$ or $C_G(ab)$, $C_G(h) = HB$ or $H\langle ab \rangle$ and $\text{Ind}_G(h) = p$. The number of such h in all the cases above is at most $|C_H(a)| + p|C_H(b)| = p^3 + p$. Here p must be greater than or equal to 5, so $p^3 + p < p^{p-1} = |H|$. Hence there exists $h \in H$ such that $C_G(H) = H$. For such h , $\text{Ind}_G(h) = pq$.

$$(5) \text{Ind}_G(ha) = p^{p-2} q.$$

Let $h_1 a_1 b_1 \in C_G(ha)$, where $h_1 \in H$, $a_1 \in A$ and $b_1 \in B$. We have $ha = (ha)^{h_1 a_1 b_1} = (hh_1^{-1} h_1^{a_1^{-1}})^{a_1 b_1} a^{b_1}$. Hence $b_1 = 1$ and so $C_G(ha) = C_{HA}(ha)$. We have $(ha)^p = (hh^{a^{-1}} h^{a^{-2}} \dots h^{a^{1-p}}) a^p = hh^{a^{-1}} h^{a^{-2}} \dots h^{a^{1-p}}$. If $h = (x_1, x_2, \dots, x_p)$, then $hh^{a^{-1}} h^{a^{-2}} \dots h^{a^{1-p}} = (x_1 + \dots + x_p, \dots, x_1 + \dots + x_p) = 1$. Hence ha is an element

of order p . Since $\langle ha \rangle \cap H = 1$, We have $HA = H \rtimes \langle ha \rangle$. Therefore $C_G(ha) = C_H(ha)\langle ha \rangle = C_H(a)\langle ha \rangle$. Thus $|C_G(ha)| = p^2$ and so $\text{Ind}_G(ha) = p^{p-2}q$.

$$(6) \text{Ind}_G(hab) = \text{Ind}_G(hb) = p^{p-2}.$$

By (3), ab and b are conjugate, so hab must be conjugate to $h'b$ where h' is some element in H . Thus, we only need to consider $\text{Ind}_G(hb)$. Let $h_1a_1b_1 \in C_G(hb)$ where $h_1 \in H, a_1 \in A, b_1 \in B$. We have $hb = (hb)^{h_1a_1b_1} = (hh_1^{-1}h_1^{b_1^{-1}}b)^{a_1b_1} = (hh_1^{-1}h_1^{b_1^{-1}})^{a_1b_1}(a_1^{-1}a_1^{b_1^{-1}})^{b_1}b$. Hence $a_1 = 1$ and $C_G(hb) = C_{HB}(hb)$. It follows that $\text{Ind}_G(hb) = \text{Ind}_{HB}(hb) \times p$. By Lemma 2, $\text{Ind}_{HB}(hb) = |H : C_H(b)| = p^{p-3}$. Therefore, $\text{Ind}_G(hb) = p^{p-2}$.

From (1)–(6), all nontrivial elements of G have been considered, so $N(G) = \{1, p, p^{p-2}\} \times \{1, q\}$ and $Z(G) = 1$. The theorem is proved.

References

- [1] R. Baer, Group elements of prime power index, *Transactions of the American Mathematical Society*, **75**(1) (1953), 20–47.
- [2] R. Bastan, C. Akin, Notes on Sophie Germain Primes, *Proceedings of International Conference on Mathematics*, **10** (2018), 18–21.
- [3] A. R. Camina, R. D. Camina, Recognising nilpotent groups, *Journal of Algebra*, **300**(1) (2006), 16–24.
- [4] A. R. Camina, R. D. Camina, The influence of conjugacy class sizes on the structure of finite groups: a survey, *Asian-European Journal of Mathematics*, **4**(4) (2011), 559–588.
- [5] C. Casolo, E. M. Tombari, Conjugacy class sizes of certain direct products, *Bulletin of the Australian Mathematical Society*, **85**(2) (2012), 217–231.
- [6] J. Cossey, T. Hawkes, Sets of p -powers as conjugacy class sizes, *Proceedings of the American Mathematical Society*, **128**(1) (2000), 49–51.
- [7] The GAP Group, *GAP – Groups, Algorithms, and Programming*, Version 4.14.0 (2024). (<https://www.gap-system.org>)
- [8] I. B. Gorshkov, Structure of finite groups with restrictions on the set of conjugacy classes sizes, *Communications in Mathematics*, **32**(1) (2023), 63–71.
- [9] I. B. Gorshkov, C. Shao, T. M. Mudziiri Shumba, Description of direct products by sizes of conjugacy classes, *Communications in Algebra*, **Online First** (2024), 1–7.
- [10] K. Ishikawa, On finite p -groups which have only two conjugacy lengths, *Israel Journal of Mathematics*, **129** (2002), 119–123.
- [11] N. Itô, On finite groups with given conjugate types I, *Nagoya Mathematical Journal*, **6** (1953), 17–28.