On the number of conjugacy classes of finite nilpotent groups

Andrei Jaikin-Zapirain *

Abstract

We establish the first super-logarithmic lower bound for the number of conjugacy classes of a finite nilpotent group. In particular, for any constant c there are only finitely many finite p-groups of order p^m with at most $c \cdot m$ conjugacy classes. This answers a question of L. Pyber.

1 Introduction

Let p be a fixed prime number and G a finite p-group of order p^m. Since G is nilpotent there exists a central series of subgroups

$$G = G_0 > G_1 > \ldots > G_m = \{1\}$$

such that $|G_i : G_{i+1}| = p$. Since for each $0 \leq i \leq m-1$ there are at least $p-1$ conjugacy classes in $G_i \setminus G_{i+1}$, we obtain that the number of conjugacy classes $k(G)$ of G satisfies

$$k(G) \geq (p-1)m \geq \log_2 |G|.$$

A slight improvement of this elementary bound was given by P. Hall. We write m as $m = 2n + e$, where $e = 0, 1$. P. Hall showed (see, for example, [2, Chapter 5, Theorem 15.2]) that there exists a non-negative integer $a = a(G)$, which we call the abundance of G, such that

$$k(G) = p^e + (p^2 - 1)(n + a(p-1)). \tag{1}$$

*Supported by Spanish Ministry of Science and Innovation, grant MTM2008-06680.

This implies, in particular, that

$$k(G) > \frac{p^2-1}{2}m + (a-1)(p^2-1)(p-1). \tag{2}$$

In [8] J. Poland proved that if $a = 0$ then G is a p-group of maximal class of order at most p^{p+2} and so there are only finitely many finite p-groups of abundance 0 (for each prime p). Combining this with the bound (2) we obtain that

$$k(G) > \frac{p^2-1}{2}m \text{ for all } p\text{-groups except finitely many of them.} \tag{3}$$

Polland's results suggested that for a fixed prime p there are only finitely many finite p-groups G with a given value of $a(G)$ (this appears, for example, as Problem 4 in [10]). This problem was solved in [4]. It was shown that $a(G) \geq \frac{\sqrt{m}}{p^3}$. However note that this result did not improve the constant $\frac{p^2-1}{2}$ in the bound (3). In this paper we establish the first super-logarithmic lower bound for the number of conjugacy classes of a finite nilpotent group.

Theorem 1.1. *There exists a (explicitly computable) constant $C > 0$ such that every finite nilpotent group G of order $n \geq 8$ satisfies*

$$k(G) > C\frac{\log_2 \log_2 n}{\log_2 \log_2 \log_2 n} \cdot \log_2 n.$$

As an immediate consequence we obtain the answer on a question of L. Pyber posed in [9] (this question appears also as Problem 5 in [10]).

Corollary 1.2. *For any constant c there exists only a finite number of finite p-groups G of order p^m with at most $c \cdot m$ conjugacy classes.*

In his paper L. Pyber established a lower bound for $k(G)$ for an arbitrary finite group G. Recently T. Keller [7] has improved Pyber's bound. We hope that the techniques introduced in the proof of Theorem 1.1 may be also used in obtaining further improvements of the Pyber-Keller bound. Recall the main conjecture in this subject.

Conjecture. There exists a constant $C > 0$ such that a finite group G of order n satisfies $k(G) \geq C \log_2 n$.

Acknowledgments: I would like to thank Jon Gonzalez who carefully read the manuscript and made many useful suggestions.

2 Preliminaries

Our notation is standard. If M is a subset of G, then we denote by $k_G(M)$ the number of conjugacy classes that have a non-empty intersection with M. As usual, $d(G)$ denotes the minimal possible number of generators for G and $\exp(G)$ the exponent of G. For any natural number n, G^n is the subgroup of G generated by $\{g^n | g \in G\}$. If G is a p-group, then for any real r we denote by $\Omega_r(G)$ the subgroup generated by elements of order at most p^r. We will use log for the logarithm to base 2.

2.1 Powerful groups

Recall that a finite p-group K is powerful if p is odd and K/K^p is abelian, or $p = 2$ and K/K^4 is abelian. Throughout this paper we shall use various facts about powerful p-groups, which can be found in [6] and [1]. Some of them are recollected in the following proposition.

Proposition 2.1. *Let K be a powerful p-group and $P = K^2$ (note that $P = K$ if $p > 2$). Then*

1. *The exponent of K coincides with the maximum of the orders of elements from any generating set.*
2. *For any $i, j \geq 0$, $[K^{p^i}, K^{p^j}] \leq K^{p^{i+j+1}}$.*
3. *For any i, j and k such that $k - 1 \leq i \leq j$, the map $K^{p^i}/K^{p^{i+k}} \to K^{p^j}/K^{p^{j+k}}$ which send $aK^{p^{i+k}}$ to $a^{p^{j-i}}K^{p^{j+k}}$ is a surjective homomorphism of abelian groups.*
4. *$\Omega_i(P)$ has exponent less than or equal to p^i.*
5. *$|\Omega_1(P)| = p^{d(P)}$ and $|\Omega_i(P)| \leq p^{d(P)i}$.*
6. *Any normal in K subgroup, which is contained in K^{2p}, is powerful.*

Let P be a powerful p-group. Consider a function

$$f_P \colon \{1, \ldots, d(P)\} \to \mathbb{N}$$

defined in the following way. We put

$$f_P(i) = k \text{ if } \ |P : \Omega_k(P)\Phi(P)| < p^i \text{ and } |P : \Omega_{k-1}(P)\Phi(P)| \geq p^i.$$

Example 2.2. Let $n_1 \geq n_2 \geq \ldots \geq n_k$ be k positive integers. Put $P = C_{p^{n_1}} \times \cdots \times C_{p^{n_k}}$. Then we have $d(P) = k$ and $f_P(i) = n_i$.

Lemma 2.3. *Let K be a powerful p-group and $P = K^2$. Then for every $k \leq \log_p \exp(P)$ we have that*

$$|P/\Omega_k(P)| = \prod_{f_P(i) \geq k} p^{f_P(i)-k}.$$

Proof. We will prove the lemma by induction on $|P|$. By Proposition 2.1(4), $\Omega_i(P/\Omega_1(P)) = \Omega_{i+1}(P)/\Omega_1(P)$. Thus, if $\bar{P} = P/\Omega_1(P)$, then $f_{\bar{P}}(i) = f_P(i) - 1$ when $i \in \{1, \ldots, d(\bar{P})\}$. Let us assume first that $k \geq 1$. Then applying the induction hypothesis we obtain that

$$|P/\Omega_k(P)| = |\bar{P}/\Omega_{k-1}(\bar{P})| = \prod_{f_{\bar{P}}(i) \geq k-1} p^{f_{\bar{P}}(i)-k+1} = \prod_{f_P(i) \geq k} p^{f_P(i)-k}.$$

Now consider the case $k = 0$. Using Proposition 2.1(5) and the induction hypothesis, we obtain that

$$\begin{aligned} |P| &= |\Omega_1(P)||\bar{P}| = p^{d(P)} \prod_{i=1}^{d(\bar{P})} p^{f_{\bar{P}}(i)} = p^{d(P)-d(\bar{P})} \prod_{f_P(i) \geq 1} p^{f_P(i)} \\ &= |\Omega_1(P)\Phi(P) : \Phi(P)| \prod_{f_P(i) \geq 1} p^{f_P(i)} = \prod_{i=1}^{d(P)} p^{f_P(i)}. \end{aligned}$$

□

Corollary 2.4. *Let K be a powerful p-group and $P = K^2$. Then for every $k \leq \log_p \exp(P)$ we have that*

$$|\Omega_k(P) : \Omega_{k-1}(P)| = p^{\max\{1 \leq i \leq d(P):\ f_P(i) \geq k\}}.$$

Proof. Applying the previous lemma we obtain that

$$|P/\Omega_k(P)| = \prod_{f_P(i) \geq k} p^{f_P(i)-k}$$

and

$$|P/\Omega_{k-1}(P)| = \prod_{f_P(i) \geq k-1} p^{f_P(i)-k+1} = \prod_{f_P(i) \geq k} p^{f_P(i)-k+1}.$$

Thus, since $f_P(i)$ is a monotonically decreasing function,

$$|\Omega_k(P) : \Omega_{k-1}(P)| = p^{\max\{1\leq i\leq d(P):\ f_P(i)\geq k\}}.$$

□

We also will need the following lemma.

Lemma 2.5. *Let G be a finite p-group and P a maximal normal powerful subgroup of G. Then $C_G(P/P^{2p}) = P$. In particular, if $n = d(P)$ then*

$$|G/P| \leq \begin{cases} 2^{\frac{n(3n-1)}{2}} & p = 2 \\ p^{\frac{n(n-1)}{2}} & p > 2 \end{cases}$$

Proof. For simplicity we assume that p is odd. If $C_G(P/\Phi(P)) \neq P$ then there exists $a \notin P$ such that $aP \in Z(G/P) \cap (C_G(P/\Phi(P))/P)$. Put $R = \langle a, P\rangle$. Then $[R,R] \leq P^p \leq R^p$ and R is normal in G. We have a contradiction. Thus, G/P can be embedded in $\mathrm{GL}_n(\mathbf{F}_p)$. Therefore it's order is at most the order of a Sylow p-subgroup of $\mathrm{GL}_n(\mathbf{F}_p)$ which is equal to $p^{\frac{n(n-1)}{2}}$. □

2.2 The average order

If N is a normal subgroup of a finite group G and $x \in G$, we denote by $o_{G/N}(x) = o_{G/N}(xN)$ the order of xN in G/N. Then we put

$$o(G/N) = \frac{1}{|G|}\sum_{x\in G} o_{G/N}(x).$$

The number $o(G)$ is called the average order of G. For example, we may estimate the average order a powerful p-group. This result appears in the proof of [10, Lemma 4.7].

Lemma 2.6. *Let P be a powerful p-group of exponent p^k. Then*

$$p^k \geq o(P) \geq (p-1)p^{k-1}.$$

Proof. By Proposition 2.1(1), $\Omega_{k-1}(P)$ is a proper normal subgroup of P. If $x \in P \setminus \Omega_{k-1}(P)$, then $o(x) = p^k$. Thus,

$$o(P) \geq \frac{1}{|P|}\sum_{x\in P\setminus\Omega_{k-1}(P)} |o(x)| \geq (p-1)p^{k-1}.$$

This proves the second inequality. The first inequality is obvious. □

In the following lemma we show that the average order of a finite group is at least the average order of its center.

Lemma 2.7. *Let G be a finite group. Then $o(G) \geq o(Z(G))$.*

Proof. Let $x \in G$ and

$$m = m(x) = \min\{o_G(y) : \ y \in xZ(G)\}.$$

Then there exists $y \in xZ(G)$ such that $y^m = 1$. Take $a \in Z(G)$. Then $(ya)^m = a^m \in Z(G)^m$. Hence $l = o_{G/Z(G)^m}(ya)$ divides m. On the other hand, there exists $z \in Z(G)$ such that $(ya)^l = z^m$. Therefore $(yaz^{-m/l})^l = 1$, and so by the choice of m, $l \geq m$. Thus, $m = o_{G/Z(G)^m}(ya)$.

Since $o_{G/Z(G)^m}(ya)$ divides $o_G(ya)$, we obtain that

$$o_G(ya) = m \cdot o_G((ya)^m) = m \cdot o_G(a^m) = m \cdot \frac{o_G(a)}{(m, o_G(a))} \geq o_G(a).$$

Now, calculating the average order of elements of $xZ(G)$ we see that

$$\frac{1}{|Z(G)|} \sum_{g \in xZ(G)} o_G(g) = \frac{1}{|Z(G)|} \sum_{a \in Z(G)} o_G(ya) \geq \frac{1}{|Z(G)|} \sum_{a \in Z(G)} o_G(a) = o(Z(G)).$$

Hence $o(G) \geq o(Z(G))$. □

It would be very interesting to understand the relation between $o(G)$ and $o(N)$, where N is a normal subgroup of G. We pose the following question.

Question. *Let G be a finite (p-) group and N a normal (abelian) subgroup of G. Is it true that $o(G) \geq o(N)^{1/2}$?*

The following lemma is proved in [5]. We include the proof for the convenience of the reader.

Lemma 2.8. *Let G be a finite p-group and M a normal subgroup of G. Then for any $x \in G$*

$$|C_G(x)| \geq o_{G/M}(x)|C_M(x)|.$$

Moreover, if M is elementary abelian and $o_{G/M}(x) \leq t \leq \ln |M|$ then

$$|C_G(x)| \geq t|M|^{1/t}.$$

Proof. Since $C_M(x) = M \cap C_G(x)$,

$$|C_G(x)/C_M(x)| = |C_G(x)M/M| \geq o_{G/M}(x).$$

Hence $|C_G(x)| \geq o_{G/M}(x)|C_M(x)|$.

Now, if M is elementary abelian we may consider M as a $\mathbb{F}_p[x]$-module. Then M is a direct sum of principal submodules of order $\leq p^{o_{G/M}(x)}$. Hence $|C_M(x)| \geq |M|^{1/o_{G/M}(x)}$.

Consider the function $f(z) = z|M|^{1/z}$. Then f decreases in the interval $1 \leq z \leq \ln|M|$. Hence we have that

$$|C_G(x)| \geq o_{G/M}(x)|C_M(x)| \geq o_{G/M}(x)|M|^{1/o_{G/M}(x)} \geq t|M|^{1/t}.$$

□

3 Proof of Theorem 1.1

Without loss of generality we may assume that G in Theorem 1.1 is a p-group. In this case Theorem 1.1 is a consequence of the following result.

Theorem 3.1. *There exists a constant $c > 0$ such that a finite p-group G of order $p^m \geq p^4$ satisfies*

$$k(G) \geq c \cdot p \cdot \frac{m \cdot \log m}{\log \log m}.$$

Proof. For simplicity we assume that p is odd. The same proof with few changes works also when $p = 2$.

Fix a maximal powerful normal subgroup P of G and let $d = d(P)$.

Claim 3.2. *The theorem holds if $m \geq d(d^2 + 1)$.*

Proof. Let p^k be the exponent of P. Since P is powerful, by Proposition 2.1 (5), $|P| \leq p^{d(P)k} = p^{dk}$. Thus, by Lemma 2.6,

$$k(P) \geq o(P) \geq (p-1)p^{k-1} \geq \frac{p-1}{p}|P|^{1/d}$$

By Lemma 2.5, $|G/P| \leq p^{\frac{d(d-1)}{2}}$. Therefore,

$$k(G) \geq \frac{k(P)}{|G:P|} \geq \frac{p-1}{p} \frac{|P|^{1/d}}{p^{d(d-1)/2}} \geq p^{\frac{m}{d} - \frac{d(d-1)}{2d} - \frac{d(d-1)}{2} - 1} = p^{\frac{m}{d} - \frac{d^2+1}{2}}.$$

Now, let us assume that $m \geq d(d^2+1)$. In this case we obtain that

$$k(G) \geq p^{\frac{m}{d}-\frac{d^2+1}{2}} \geq p^{\frac{m}{2d}} \geq p \cdot p^{\frac{m^{\frac{2}{3}}-2}{2}} \geq c \cdot p \cdot m^2$$

for some constant $c > 0$.

□

Claim 3.3. *The theorem holds if $d \leq 2^{12}$.*

Proof. By Claim 3.2, we may assume that $m < d(d^2+1)$. Thus, if $d \leq 2^{12}$, then $m < 2^{37}$. Since $k(G) \geq (p-1)m$, we are done. □

So, from now on, we will assume that $m < d(d^2+1)$ and $d > 2^{12}$.

Claim 3.4. *Assume $|G/P| = p^{xd}$. Then $k(G) \geq dp^x$.*

Proof. Let $\bar{G} = G/P$. By Lemma 2.5, the nilpotency class of $\bar{G}$ is at most d. Define $p^{a_i} = |\gamma_i(\bar{G}) : \gamma_{i+1}(\bar{G})|$. Thus, $k_G(\gamma_i(G)P \setminus \gamma_{i+1}(G)P) \geq p^{a_i} - 1$. On the other hand $k_G(P) \geq (p-1)\log_p |P| \geq d$. Hence

$$\begin{aligned} k(G) &\geq k_G(P) + \textstyle\sum_{i=1}^{d} k_G(\gamma_i(G)P \setminus \gamma_{i+1}(G)P) \geq d + \sum_{i=1}^{d}(p^{a_i}-1) \\ &= \textstyle\sum_{i=1}^{d} p^{a_i} \geq d\sqrt[n]{p^{\sum_i a_i}} = d(|\bar{G}|^{1/d}) = dp^x. \end{aligned}$$

□

We put $S = P^p$. Since P is powerful, by Proposition 2.1, S is also powerful.

Claim 3.5. *We have that $k(G/S) > \frac{p \cdot d \log d}{24}$.*

Proof. Without loss of generality we may assume in the proof of this claim that $S = P^p = \{1\}$. Thus $|P| = p^d$.

Let H be a subgroup of G. Put $t_H = \frac{d}{2\log_p |G:H| + \log d + 1}$ and denote by $A(H)$ the following subset of H:

$$A = A(H) = \{x \in H : \ o_{G/P}(x) \geq t_H\}.$$

Note that if $x \in H \setminus A(H)$ then, by Lemma 2.8,

$$\begin{aligned} |C_G(x)| &\geq o_{G/P}(x)|P|^{\frac{1}{o_{G/P}(x)}} \geq t_H|P|^{1/t_H} \geq \frac{d \cdot p^{2\log_p |G:H| + \log d + 1}}{2\log_p |G:H| + \log d + 1} \\ &\geq \frac{p|G:H|^2 d^2}{2\log_p |G:H| + \log d + 1} \geq \frac{p|G:H| d \log d}{2}. \end{aligned}$$

Since $k_G(H) \geq \frac{1}{|G|}\sum_{x\in H\setminus A(H)}|C_G(x)|$, we have

$$k_G(H) \geq \frac{p|G:H||H\setminus A(H)|d\log d}{2|G|} = \frac{p|H\setminus A(H)|d\log d}{2|H|}.$$

Thus, if $|A(H)| < \frac{|H|}{2}$, then $k_G(H) > \frac{p\cdot d\log d}{4}$. Thus we may assume that $|A(H)| \geq \frac{|H|}{2}$ for any $H \leq G$.

Note that by Lemma 2.8,

$$k(G) = \frac{1}{|G|}\sum_{x\in G}|C_G(x)| \geq \frac{1}{|G|}\sum_{x\in G} o_{G/P}(x)|C_P(x)|.$$

Let $\chi(x) = |C_P(x)|$ be the permutation character associated with the action of G on P (see [3, p.68]). Then the last inequality can be rewritten as

$$k(G) \geq \langle o_{G/P}, \chi\rangle.$$

For each $0 \leq i \leq d-1$ we fix an element $m_i \in P$ in the following way:

First, let $1 \neq m_0 \in Z(G)\cap P$. Now, suppose we have chosen $m_0,\ldots,m_k$. Then let $m_{k+1}\in P$, $m_{k+1}\notin\langle m_0,\cdots,m_k\rangle$ and $[G,m_{k+1}]\subseteq\langle m_0,\cdots,m_k\rangle$. It is clear that the elements $\{m_i^\alpha|\alpha = 0,\ldots,p-1\}$ lie in different conjugacy classes of G. Put $N_i = C_G(m_i)$. Note that since $|[G,m_i]| \leq p^i$, the index of N_i in G is at most p^i.

If Λ is a set of representatives of the G-conjugacy classes in P, then it is known that $\chi = \sum_{m\in\Lambda} 1_{C_G(m)}^G$. In particular, $\chi(x) \geq (p-1)\sum_{i=0}^{d-1} 1_{N_i}^G(x)$ for every $x \in G$.

Note that, by Frobenius Reciprocity,

$$\begin{aligned}\langle o_{G/P}, 1_{N_i}^G\rangle &= \langle o_{N_i/P}, 1_{N_i}\rangle = o(N_i/P) \geq \tfrac{|A(N_i)|t_{N_i}}{|N_i|} \geq \tfrac{t_{N_i}}{2}\\ &= \tfrac{d}{4\log_p|G:N_i|+2\log d+2} \geq \tfrac{d}{4i+2\log d+2}.\end{aligned}$$

Hence

$$\begin{aligned}k(G) &\geq \langle o_{G/P},\chi\rangle \geq \langle o_{G/P},(p-1)\textstyle\sum_{i=0}^{d-1}1_{N_i}^G\rangle \geq (p-1)d\textstyle\sum_{i=0}^{d-1}\tfrac{1}{4i+2\log d+2}\\ &\geq \tfrac{p\cdot d}{4}\textstyle\sum_{i=0}^{d-1}\tfrac{1}{2i+\log d+1} > \tfrac{p\cdot d}{8}\ln\tfrac{2d+\log d-1}{\log d+1} \geq \tfrac{p\cdot d\log d}{24}.\end{aligned}$$

□

Remark. The proofs of Claims 3.4 and 3.5 essentially repeat the argument of the proof of [5, Theorem 1.10]. The main new ingredients in the proof of Theorem 3.1 are Claims 3.6 and 3.7.

Claim 3.6. *Let* $s \in \{1, \ldots, d(S)\}$. *Then*

$$k(G) \geq p^{(f_S(s)-1)/3} s.$$

Remark. It may be helpful in the first reading of the proof of this claim assume that S is abelian. In this case the function f_S is described in Example 2.2.

Proof. It is clear that without loss of generality we may assume that $f_S(s+1) \leq f_S(s)-1$ or $s = d(S)$. Put $k = f_S(s)$, $T = \Omega_k(S)$ and let t be the integer part of $(k+1)/3$. Since T is a normal subgroup of P and it is contained in $S = P^p$, Proposition 2.1(6) implies that T is powerful. Let $A = T^{p^{k-2t}}$ and $B = T^{p^{k-t}}$. Note that A and B are characteristic subgroups of P and so they are normal in G. Since, T is powerful, Proposition 2.1(2) implies that $[A, B] = 1$. Moreover, by Proposition 2.1(3), the map $\alpha\colon A/B \to B$ which sends aB to a^{p^t} is a surjective homomorphism of abelian groups. Since α commutes with G-action, α is also a homomorphism of G-modules. In particular, $A/\ker\alpha \cong B$ as G-modules.

Note that $\Omega_{k-1}(T) = \Omega_{k-1}(S)$. Since we assume that $f_S(s+1) \leq f_S(s)-1$ or $s = d(S)$, Corollary 2.4 implies that

$$|T/\Omega_{k-1}(T)| = |\Omega_k(S) : \Omega_{k-1}(S)| = p^s.$$

Since G is a p-group, there are at least $(p-1)s$ non-trivial G-conjugacy classes in $T/\Omega_{k-1}(T)$. Hence the claim holds if $k = 1$. So, we assume now that $k \geq 2$. In this case $t \geq 1$.

Choose $m_1, \ldots, m_{(p-1)s} \in T \setminus \Omega_{k-1}(T)$ such that $\{m_i\Omega_{k-1}(T)\}$ lie in different G-conjugacy classes. Consider the map $\beta\colon T/T^p \to T^{p^{k-t}}/T^{p^{k-t+1}}$ which sends xT^p to $x^{p^{k-t}}T^{p^{k-t+1}}$. Applying again Proposition 2.1(3) we conclude that β is a homomorphism of G-modules. Let $x \in \ker\beta$ be an arbitrary element of $\ker\beta$. This means that $x^{p^{k-t}} \in T^{p^{k-t+1}}$. On the other hand, by Proposition 2.1(4),

$$T^{p^{k-t+1}} = \Omega_k(S)^{p^{k-t+1}} \leq \Omega_{t-1}(S) = \Omega_{t-1}(T).$$

Proposition 2.1(4) also implies that $\Omega_{t-1}(T)^{p^{t-1}} = 1$, and so

$$x^{p^{k-1}} = (x^{p^{k-t}})^{p^{t-1}} = 1.$$

Hence we conclude that $\ker\beta \le \Omega_{k-1}(T)$. Thus we obtain that

$$T/\Omega_{k-1}(T) \cong T^{p^{k-t}}/\Omega_{k-1}(T)^{p^{k-t}} T^{p^{k-t+1}}, \qquad (4)$$

as G-modules.

Put $a_i = m_i^{p^{k-2t}}$ and $b_i = m_i^{p^{k-t}} = a_i^{p^t}$. The isomorphism (4) implies that $\{b_i\}$ lie in different G-conjugacy classes in B. Note that

$$o_B(b_i) = \frac{o_G(m_i)}{p^{k-t}} = \frac{p^k}{p^{k-t}} = p^t.$$

Let χ be the permutation character corresponding to the action of G on B. Thus, $\chi(g) = |C_B(g)|$. Since $\{b_i\}$ lie in different G-conjugacy classes in B, we obtain that $\chi(g) \ge \sum_{i=1}^{(p-1)s} 1_{C_G(b_i)}^G(g)$ for all $g \in G$. Therefore we have the following.

$$\begin{aligned} k(G) &= \tfrac{1}{|G|}\textstyle\sum_{g\in G} |C_G(g)| \ge \tfrac{1}{|G|}\sum_{g\in G} o_{G/B}(g)|C_B(g)| && \text{Lemma 2.8}\\ &= \langle o_{G/B}, \chi\rangle \ge \langle o_{G/B}, \textstyle\sum_{i=1}^{(p-1)s} 1_{C_G(b_i)}^G\rangle \\ &= \textstyle\sum_{i=1}^{(p-1)s} \langle o_{C_G(b_i)/B}, 1_{C_G(b_i)}\rangle = \sum_{i=1}^{(p-1)s} o(C_G(b_i)/B) \\ &\ge \textstyle\sum_{i=1}^{(p-1)s} o(C_G(b_i)/\ker\alpha) \ge \sum_{i=1}^{(p-1)s} o(Z(C_G(b_i)/\ker\alpha)) && \text{Lemma 2.7.} \end{aligned}$$

Since $[A,B]=1$, $A \le C_G(b_i)$. As we observed already $\alpha\colon A/B \to B$ is a surjective homomorphism of G-modules. Therefore since $\alpha(a_iB) = b_i$, we obtain that $C_G(a_i \ker\alpha) = C_G(b_i)$ and so $a_i \ker\alpha \in Z(C_G(b_i)/\ker\alpha)$. Thus the exponent of $Z(C_G(b_i)/\ker\alpha)$ is at least $o_{A/\ker\alpha}(a_i) = o_B(b_i) = p^t$. Hence, by Lemma 2.6, $o(Z(C_G(b_i)/\ker\alpha)) \ge (p-1)p^{t-1}$. Finnaly we conclude that

$$k(G) \ge \sum_{i=1}^{(p-1)s} o(Z(C_G(b_i)/\ker\alpha)) \ge (p-1)s(p-1)p^{t-1} \ge sp^{(f_P(s)-1)/3}.$$

□

Claim 3.7. *Assume $|S/\Omega_{9\log\log d+4}(S)| = p^{yd}$. Then there exists $s \in \{1,\dots,d(S)\}$ such that*

$$sp^{(f_S(s)-4)/3} > y \cdot d\log d.$$

In particular, $k(G) > p \cdot y \cdot d\log d$.

Proof. Let $M = y \cdot d \log d$. Since we assume that $m < d(d^2+1)$, we have $y < d^2 + 1$. Thus,

$$M < d^4. \tag{5}$$

By the way of contradiction let us assume that $sp^{(f_S(s)-4)/3} \leq M$ for all $s \in \{1, \ldots, d(S)\}$. Thus,

$$f_S(s) \leq 3 \log_p \frac{M}{s} + 4 < 3 \log M + 4. \tag{6}$$

By Lemma 2.3,

$$\begin{aligned} M &= (\log_p |S/\Omega_{9 \log \log_p n + 4}(S)|) \log d \\ &= \log d \sum_{f_S(i) \geq 9 \log \log_p d + 4} (f_S(i) - 9 \log \log_p d - 4) \\ &\leq 3 \log d \cdot \log M \cdot |\{i : \ f_S(i) \geq 9 \log \log_p d + 4\}|. \end{aligned}$$

Note that if $f_S(i) \geq 9 \log \log_p d + 4$, then, using the inequality (6), we obtain that

$$3 \log_p \frac{M}{i} + 4 \geq f_S(i) \geq 9 \log \log_p d + 4 \geq 9 \log_p \log d + 4$$

and so $i \leq \frac{M}{(\log d)^3}$. Thus, using (5), we obtain

$$M \leq 3 \log d \cdot \log M \frac{M}{(\log d)^3} = M \frac{3 \log M}{(\log d)^2} \leq M \frac{12}{\log d}.$$

Since we assume that $d > 2^{12}$, we obtain that $M < M$. We have a contradiction.

Thus, there exists $s \in \{1, \ldots, d(S)\}$ such that $sp^{(f_S(s)-4)/3} > y \cdot d \log d$. By Claim 3.6, $k(G) \geq p \cdot y \cdot d \log d$. □

Now we are ready to finish the proof. Note that since P is powerful, Proposition 2.1(5) implies that

$$|\Omega_{9 \log \log d + 4}(S)| \leq |\Omega_{9 \log \log d + 4}(P)| \leq p^{d(9 \log \log d + 4)}.$$

Thus,

$$\begin{aligned} m &= \log_p |G| = \log_p |G/P| + \log_p |P/S| + \log_p |S/\Omega_{9 \log \log d + 4}(S) \\ &+ \log_p |\Omega_{9 \log \log d + 4}(S)| \leq d(x + y + 9 \log \log d + 5). \end{aligned}$$

If $x = \max\{x, y, 3\log\log d+2\}$, then $m \le 5xd$ and $\log d \le p^{(x-2)/3}$. Applying Claim 3.4, we obtain that

$$k(G) \ge p^x d \ge p \cdot x \cdot d \log d \log x \ge \frac{p}{15} m \log m.$$

If $y = \max\{x, y, 3\log\log d + 2\}$, then $m \le 5yd$. Since we suppose that $m < d(d^2+1)$, $y < d^2 + 1$ and since we assume that $d > 2^{12}$, $\log d > 12$. Applying Claim 3.7 we obtain that

$$k(G) \ge p \cdot y \cdot d \log d \ge \frac{p}{4} \cdot y \cdot d(\log d + \log y + 3) \ge \frac{p}{20} m \log m.$$

Finally, if $3\log\log d+2 = \max\{x, y, 3\log\log d+2\}$, then $m \le d(15\log\log d + 9)$. Hence, by Claim 3.5,

$$k(G) \ge \frac{p}{24} d \log d \ge \frac{p \cdot m \log m}{800 \cdot \log\log m}.$$

□

References

[1] J. González-Sánchez, A. Jaikin-Zapirain, On the structure of normal subgroups of potent p-groups, *J. Algebra* 276 (2004), no. 1, 193–209.

[2] B. Huppert, *Endliche Gruppen I*, Springer, Berlin-Heidelberg-New York, 1982.

[3] M. Isaacs, *Character theory of finite groups* (Dover Publications, Inc., New York, 1994).

[4] A. Jaikin Zapirain, On the abundance of finite p-groups, *Journal Group Theory* 3 (2000) 225–231.

[5] A. Jaikin-Zapirain, On the number of conjugacy classes in finite p-groups, *J. London Math. Soc.* (2) 68 (2003), no. 3, 699–711.

[6] A. Lubotzky and A. Mann, Powerful p-groups. I. Finite groups, *J. Algebra*, **105** (1987), 484-505.

[7] T. Keller, Finite groups have even more conjugacy classes, arXiv:0812.2590, to appear in Israel Journal of Math..

[8] J. Poland, Two problems with finite groups with k conjugate classes, *J. Austr. Math. Soc.*(Ser. A), **8** (1968), 49-55.

[9] L. Pyber, Finite groups have many conjugacy classes, *J. London Math. Soc.* (2) 46 (1992), no. 2, 239–249.

[10] A. Shalev, 'Finite p-groups', *Finite and locally finite groups (Istanbul, 1994)*, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 471 (1995) 401–450.

Departamento de Matemáticas, Universidad Autonoma de Madrid and
Instituto de Ciencias Matemáticas, CSIC-UAM-UC3M-UCM
andrei.jaikin@uam.es