Applying combinatorial results to products of conjugacy classes

Rachel Deborah Camina
Fitzwilliam College, Cambridge, CB3 0DG, UK
rdc26@cam.ac.uk

Abstract

Let $K = x^G$ be the conjugacy class of an element $x$ of a group $G$ and suppose $K$ is finite. We study the increasing sequence of natural numbers $\{|K^n|\}_{n \geq 1}$ and consider restrictions on this sequence and the algebraic consequences. In particular, we prove that if $|K^2| < \frac{3}{7}|K|$ or if $|K^4| < 2|K|$ then $K^n$ is a coset of the normal subgroup $[x,G]$ for all $n \geq 2$ or 4, respectively. We then use these results to contribute to conjectures about the solubility of $\langle K \rangle$ when $K^n$ satisfies certain conditions.

1 Introduction

Suppose $K = x^G$ is the conjugacy class of an element $x$ in a group $G$ and suppose $K$ is finite. Let $n$ be a natural number. The study of $K^n = \{ x_1 \cdots x_n \mid x_i \in K \}$, the powers of the class $K$, has long interested mathematicians, see for example [1]. More recently Guralnick and Navarro [7] considered the case when $G$ is finite and $K^2$ is a conjugacy class, this led to the situation when $K^n$ is a conjugacy class, and $n$ is an integer at least 2, being studied in [3]. Note, assuming $G$ finite and $K^n$ a conjugacy class, then $K^n$ is equal to $(x^n)^G$ and since $|K^n| \geq |K|$ and $C_G(x) \leq C_G(x^n)$ (where $C_G(x)$ denotes the centraliser of $x$ in $G$) it follows that $|K^n| = |K|$. In this article instead of considering the sets $K^n$ we consider the increasing sequence of natural numbers $\{|K^n|\}_{n \geq 1}$ and see how restrictions on this sequence lead to algebraic consequences. For example if the sequence stops, that is $|K^m| = |K^{m+1}|$ for some $m \geq 1$, then $K^r = x^rN$ for all $r \geq m$ where
$N$ is the normal subgroup $[x, G] = \langle [x, g] | g \in G \rangle$. In particular if $|K^2| = |K|$ then $K = xN$. Applying the ‘Freiman Inverse Problem for $\kappa < \frac{3}{2}$’, allows us to generalise these ideas as the following theorem shows.

**Theorem A.** Suppose $K = x^G$ is a conjugacy class of an element $x$ of a group $G$ and $K$ is finite. Let $N$ denote the normal subgroup $[x, G]$.

(i) If $|K^2| = \mu |K|$ with $\mu < \frac{3}{2}$ then $K^r = x^rN$ for all $r \geq 2$.
(ii) If $|K^3| = \frac{3}{2}|K|$ then $K^r = x^rN$ for all $r \geq 2$.
(iii) If $|K^4| = \mu |K|$ with $\mu < 2$ then $K^r = x^rN$ for all $r \geq 4$.
(iv) If $|K^5| = 2|K|$ then $K^r = x^rN$ for all $r \geq 4$.

For example if $A_4$ is the alternating group of degree 4 and $K$ is the conjugacy class of the double transposition $x = (1, 2)(3, 4)$, then $|K^2| = 4 = \frac{4}{3}|K|$ and indeed $K^2 = KK^{-1} = [x, A_4]$ is a normal subgroup of $A_4$. An example for (ii) is given by the conjugacy class $K$ of the 3-cycle $x = (1, 2, 3)$ in $S_3$ the symmetric group of degree 3. In this case $K^2 = KK^{-1} = [x, S_3]$ is the normal subgroup of $S_3$ and $|K^3| = |K^2| = \frac{3}{2}|K|$. Note (i) is best possible in the following sense. Let $D_{2n}$ be the dihedral group of order $2n$ with rotation $r$ of order $n$ and suppose $n \geq 5$. Let $K$ be the conjugacy class of $r$ in $D_{2n}$, then $|K^2| = 3 = \frac{3}{2}|K|$ but $|K^r| > |K^2|$ for all $r \geq 3$. Consideration of the conjugacy class of a rotation of order 8 in $D_{16}$ illustrates (iv).

In [3] the authors propose the following conjecture.

**Conjecture.** [3, Conjecture 2] Let $G$ be a finite group and $K$ a conjugacy class. If $K^n = D \cup D^{-1}$ for some natural number $n \geq 2$ and $D$ a conjugacy class, then $\langle K \rangle$ is soluble.

The authors prove that in this scenario $|D| = |K|/2$ or $|D| = |K|$. For the cases when $D = D^{-1}$ or $|D| = |K|/2$ they prove that $\langle K \rangle$ is soluble. They also show that if $K^2 = K \cup K^{-1}$ then $\langle K \rangle$ is soluble and $x$ is a $p$-element for some prime $p$. More recently Beltrán and Felipe [4, Theorem B] have shown that if $K^n = K \cup K^{-1}$ then $\langle K \rangle$ is soluble. Examples of when these situations arise are given in [3, Example 3] and [4, Example 3.2]. By applying Theorem A and [4, Theorem A] we prove the following, giving more evidence for the conjecture above.

**Theorem B.** Suppose $G$ is a finite group and $K$ a conjugacy class such that $K^n = D \cup D^{-1}$ for some conjugacy class $D$ and $n \geq 4$, then $\langle K \rangle$ is soluble.

We also show that in the situation above $D^3 \subseteq D \cup D^{-1}$.
In [5] the authors consider the product $KK^{-1}$ for $K$ a conjugacy class of a finite group $G$. In particular they study when $KK^{-1} = \{1\} \cup D \cup D^{-1}$ and when $KK^{-1} = \{1\} \cup D$ for $D$ a conjugacy class. They prove that in these cases $G$ is not a nonabelian simple group [5, Theorem A] and they conjecture that $\langle K \rangle$ is soluble. Applying a combinatorial result of Tao [8], which considers when $XX^{-1}$ is a group given that $X$ is a finite subset of a nonabelian group, gives the following which adds to this line of research.

Theorem C. Suppose $K = x^G$ is a conjugacy class of an element $x$ of a finite group $G$ and

(i) $KK^{-1} = \{1\} \cup D$ for a conjugacy class $D$ and $|D| + 1 < \frac{3}{2}|K|$ or

(ii) $KK^{-1} = \{1\} \cup D \cup D^{-1}$ for a conjugacy class $D$ and $2|D| + 1 < \frac{3}{2}|K|$.

Then $\langle D \rangle$ is $p$-elementary abelian for a prime $p$ and $\langle K \rangle = \langle x \rangle \langle D \rangle$ is metabelian.

2 The sequence $\{|K^n|\}_{n \geq 1}$.

Recall, the kernel of a finite subset $S$ of a group $G$ is defined to be

$$\ker(S) = \{x \in G : xS = S\}.$$ 

Clearly $\ker(S)$ is a subgroup of $G$ and as $S$ is a union of cosets of $\ker(S)$ its order divides $|S|$. If $S$ is a normal subset then $\ker(S)$ is a normal subgroup. Furthermore, a recent result [7, Theorem B(a)] gives that if $S$ is a conjugacy class then $\ker(S)$ is soluble. The notion of a kernel has appeared in the literature many times, under various different names.

The following lemma is a first illustration of how a restriction on the sequence $\{|K^n|\}_{n \geq 1}$ determines structural properties of $K$. The ideas are known but are presented here for completeness.

Lemma 1. Suppose $K = x^G$ is a conjugacy class of a group $G$ and $K$ is finite. Suppose $|K^n| = |K^m|$ for some $n < m$. Then $K^r = x^rN$ for all $r \geq n$ where $N = [x,G]$ is a normal subgroup of $G$. If $|K^n| = |K^m| < |G|$ then $N$ is a proper normal subgroup.

Proof. As $|K^n| = |K^m|$ it follows that $|K^n| = |K^{n+1}|$. So, $xK^n = K^{n+1} = x^gK^n$ for all $g \in G$ and thus $N = \langle [x,g] \rangle = [x,G] \leq \ker(K^n)$ and $|N|$ divides $|K^n|$. In particular, when $|K^n| < |G|$ it follows that $N$ is proper. Note $K \subseteq xN$ so $K^n \subseteq x^nN$. But $|N| \leq |K^n| \leq |N|$, so $K^n = x^nN$. As $|K^r| \geq |K^n|$ for all $r \geq n$ but also $K^r \subseteq x^rN$ it follows that $K^r = x^rN$ as required. □
The following useful result is due to Freiman. Although originally proved in 1973, [6] gives a more recent exposition.

**Theorem 1.** (Freiman inverse problem for κ < \( \frac{3}{2} \)) [6] Suppose \( A \) is a finite subset of a nonabelian group \( G \) and \( |A^2| < \frac{3}{2}|A| \), then the following hold.

(a) The set \( H = A^{-1}A = AA^{-1} \) is an \( A \)-invariant subgroup of \( G \) and \( A^2 \) is a coset of \( H \).

(b) If \( A^2 \cap H \neq \emptyset \) then \( A^2 = H \).

We apply this to conjugacy classes. Note if \( K = x^G \) is a conjugacy class then \( KK^{-1} = K^{-1}K \). This is because if \( ab \in KK^{-1} \) with \( a \in K \) and \( b \in K^{-1} \) then \( ba \in K^{-1}K \) and as \( K^{-1}K \) is normal \( ab = (ba)^{-1} \in K^{-1}K \). Further if \( KK^{-1} \) is a subgroup then \( KK^{-1} = [x,G] \). Also if \( G \) is abelian the following result is trivially true.

**Proposition 1.** Suppose \( K = x^G \) is a finite conjugacy class of a group \( G \) and \( |K^2| = \mu |K| \) with \( \mu < \frac{3}{2} \). Then \( N = KK^{-1} = [x,G] \) is a normal subgroup of \( G \) with \( |N| = \mu |K| \) and \( K^r = x^rN \) for all \( r \geq 2 \).

**Proof.** By the previous theorem \( N = KK^{-1} \) is a subgroup, so \( N = [x,G] \), and \( |N| = |K^2| \). As \( K \subseteq xN \) it follows that \( K^2 \subseteq x^2N \) and, by orders, \( K^2 = x^2N \). As \( |K^r| \geq |K^2| \) for all \( r \geq 2 \) but also \( K^r \subseteq x^rN \) we have \( K^r = x^rN \) for all \( r \geq 2 \).

Motivated by the situation described in the introduction, that is when \( K'' = D \cup D^{-1} \) where both \( K \) and \( D \) are conjugacy classes and \( |D| = |K| \), we now investigate the case when \( |K''| = 2|K| \). First a lemma which is adapted from [2, page 29].

**Lemma 2.** Let \( K \) be a finite conjugacy class of a group \( G \) and suppose \( |KK^{-1}K| < 2|K| \). Then \( H = KK^{-1} \) is a normal subgroup of \( G \).

**Proof.** Clearly \( 1 \in KK^{-1} \). Suppose \( h,g \in H \) then as \( |HK| < 2|K| \) it follows that \( hK \cap gK \neq \emptyset \) and so there exists \( a, b \in K \) such that \( ha = gb \). Thus \( g^{-1}h = ba^{-1} \in KK^{-1} = H \), it follows that \( H \) is a subgroup.

We apply this lemma to our situation.

**Proposition 2.** Suppose \( K = x^G \) is a finite conjugacy class of a group \( G \).

(i) If \( |K^4| = \mu |K| \) for some \( \mu < 2 \) then \( N = KK^{-1} \) is a normal subgroup of \( G \) with \( |N| = \mu |K| \) and \( K^r = x^rN \) for all \( r \geq 4 \).

(ii) If \( |K^m| = 2|K| \) for some \( m \geq 5 \) then \( N = [x,G] \) is a normal subgroup of \( G \) with \( N = 2|K| \) and \( K^r = x^rN \) for all \( r \geq 4 \).
Proof. (i) First note that if $G$ is abelian then $\mu = 1$ and the result trivially holds. So assume $G$ not abelian. Now $|K^2| \leq |K^4| = \mu|K|$, so $|K^2| = \lambda|K|$ for some $\lambda \leq \mu$. If $\lambda < \frac{3}{2}$ then the result follows from Proposition 1. So we assume $\frac{3}{2}|K| \leq |K^2| < 2|K|$.

Now $|K^4| = \nu|K^2|$ for some $\nu$ and as $|K^2| \geq \frac{3}{2}|K|$ it follows that $2|K| > \nu|K^2| \geq \frac{3\nu}{2}|K|$ and so $\nu < \frac{4}{3} < \frac{3}{2}$. Thus $H = K^2K^{-2}$ is a finite group of order $\nu|K^2|$ by Theorem 1. Note that $KK^{-1} = K^{-1}K$ and so $H = KK^{-1}KK^{-1}$ and $|KK^{-1}| \leq |H| < 2|K|$. So, $KK^{-1} = N$ is a group by Lemma 2. Moreover $N = H$. As $K \subseteq xN$ for $x \in K$ this forces $K^n \subseteq x^nN$ for all $n$, and by orders, $K^r = x^rN$ for all $r \geq 4$.

(ii) If $|K^4| < 2|K|$ then by (i) it follows that $|K^n| < 2|K|$ for all $n \geq 4$. Thus $|K^4| = 2|K|$ and the result follows from Lemma 1. □

Proof of Theorem A. (i) follows from Proposition 1. Suppose $|K^3| = \frac{3}{2}|K|$. If $|K^2| < |K^3|$, then applying (i) gives that $|K^3| = |K^2| < \frac{3}{2}|K|$, a contradiction. So $|K^2| = |K^3|$ and applying Lemma 1 gives (ii). Finally, (iii) and (iv) follow from Proposition 2(i) and (ii) respectively. □

We return to considering $K^n = D \cup D^{-1}$ with $K$ and $D$ conjugacy classes, $D \neq D^{-1}$ and $|K| = |D|$. We have two cases (i) when $|K^{n-1}| < 2|K|$ and (ii) when $|K^m| = 2|K|$ for some $m < n$. The previous proposition says that if $n > 4$ then we are in the second case. The next lemma says this also holds if $n = 4$.

Lemma 3. Suppose $K$ is a conjugacy class of a finite group $G$ and $K^4 = D \cup D^{-1}$ with $D$ a conjugacy class, $D \neq D^{-1}$ and $|K| = |D|$. Then $|K^2| = 2|K|$.

Proof. Note $|K| < |K^2|$ by Lemma 1. It follows that $K^2$ is not a single conjugacy class, since if it were $K^2 = (x^2)^G$ but then $|K^2| \leq |K|$ as $C_G(x) \leq C_G(x^2)$. Suppose $|K| < |K^2| < 2|K|$. As $K^2$ is not a single conjugacy class there exists $y \in K^2$ with $|y^G| < |K|$, thus $|C_G(y)| > |C_G(x)|$. Now, $y^2 \in K^4$ so $|(y^2)^G| = |K|$. This implies $|C_G(y^2)| = |C_G(x)| < |C_G(y)|$ which contradicts $C_G(y) \leq C_G(y^2)$. □

Note the above proof also shows that in this case $K^2$ is a union of two conjugacy classes of size $|K|$.

We have the following theorem.

Theorem 2. Let $K = x^G$ be a conjugacy class of a finite nontrivial group $G$, let $N$ denote the normal subgroup $[x^G]$ and let $n \geq 4$ be an integer. Suppose $K^n = D \cup D^{-1}$ with $D$ a conjugacy class, $D \neq D^{-1}$ and $|D| = |K|$.
(i) If \( n > 4 \), then \( K^r = x^r N \) for all \( r \geq 4 \) and \( N \) is proper.
(ii) If \( n = 4 \), then \( K^r = x^r N \) for all \( r \geq 2 \) and \( N \) is proper.

**Proof.** Note that \( K^n = D \cup D^{-1} \neq G \). So (i) follows from Proposition 2(ii). For (ii), applying Lemma 3 gives that \( |K^2| = 2|K| = |K^4| \) and the result follows from Lemma 1. \( \square \)

This yields Theorem B which confirms [3, Conjecture 2] for \( n \geq 4 \).

**Proof of Theorem B.** If \( D = D^{-1} \) the result follows from [3, Theorem A]. By [3, Theorem C] either \( |D| = |K|/2 \) or \( |D| = |K| \) and in the first case the result follows. So we assume \( D \neq D^{-1} \) and \( |D| = |K| \). By the previous theorem \( K^n = x^n N = D \cup D^{-1} \) where \( N = [x, G] \). Applying [4, Theorem A] gives that \( N \) is soluble. As \( \langle K \rangle = \langle x \rangle N \) it follows that \( \langle K \rangle \) is also soluble. \( \square \)

We also have the following structural information.

**Proposition 3.** Suppose \( K \) and \( D \) are conjugacy classes of a finite group satisfying \( K^n = D \cup D^{-1} \) with \( |D| = |K| \) and \( n \geq 4 \). Then \( D^3 \subseteq D \cup D^{-1} \).

**Proof.** If \( D = D^{-1} \) then \( D^3 = D \) by [3, Theorem 4], so assume \( D \neq D^{-1} \). As \( n \geq 4 \) by Theorem 2 it follows that \( K^n = x^n N = D \cup D^{-1} = x^{-n} N \), where \( N = [x, G] \). Thus
\[
K^{2n} = x^{2n} N = N = (D \cup D^{-1})(D \cup D^{-1}) = D^2 \cup D^{-1} D \cup D^{-2},
\]
as \( DD^{-1} = D^{-1} D \). Without loss of generality we assume \( D = (x^n)^G \). As \( D^{-1} D \subseteq N \) it follows that \( DN = x^n N \). Thus \( D^3 \subseteq DN = x^n N = D \cup D^{-1} \). \( \square \)

## 3 The normal subset \( KK^{-1} \).

In [5] the authors consider the product \( KK^{-1} \) for \( K \) a conjugacy class. In particular they study when \( KK^{-1} = \{1\} \cup D \cup D^{-1} \) and when \( KK^{-1} = \{1\} \cup D \) for \( D \) a conjugacy class. For example consider the conjugacy class of a 3-cycle in the symmetric group of degree 3, this satisfies \( KK^{-1} = \{1\} \cup K \). More examples are given in [5] and they prove the following result.

**Theorem 3.** [5, Theorem C] Let \( K \) be a conjugacy class of a finite group \( G \) and suppose \( KK^{-1} = \{1\} \cup D \) where \( D \) is a conjugacy class of \( G \). Then \( |D| \) divides \( |K|(|K| - 1) \) and \( \langle K \rangle / \langle D \rangle \) is cyclic. In addition,

(1) If \( |D| = |K| - 1 \) then \( \langle K \rangle \) is metabelian. More precisely, \( \langle D \rangle \) is \( p \)-elementary abelian for some prime \( p \).
If $|D| = |K|$ then $\langle K \rangle$ is soluble with derived length at most 3.

If $|D| = |K|(|K| - 1)$ then $\langle K \rangle$ is abelian.

We apply the following combinatorial result, which appears in [8], to show that the situation in (1) is more common than the above implies.

**Lemma 4.** [8] Let $X$ be a finite subset of a nonabelian group $G$. If $|X^{-1}X| < \frac{3}{2}|X|$ then $XX^{-1}$ and $X^{-1}X$ are both finite groups which are conjugate to each other. In particular, $X$ is contained in the right-coset (or left-coset) of a group of order less than $\frac{3}{2}|X|$.

**Proof of Theorem C.** $K$ is the conjugacy class $x^G$ and the hypotheses ensure that $|KK^{-1}| < \frac{3}{2}|K|$. So, by the previous lemma, $KK^{-1}$ is a finite group. Thus either $\langle D \rangle = \{1\} \cup D$ or $\langle D \rangle = \{1\} \cup D \cup D^{-1}$ respectively. It follows that $\langle D \rangle$ is $p$-elementary abelian (as it is a minimal normal subgroup). Further, $\langle K \rangle = \langle x \rangle[x,G] = \langle x \rangle \langle D \rangle$ and thus $K$ is metabelian. □

**Acknowledgements.** The author would like to thank the Isaac Newton Trust for supporting her sabbatical during which time this research took place.

**References**


