Product of Conjugacy Classes in Some Finite Groups and Related Problems

Wei-Liang Sun
National Cheng Kung University

May 2012

Notation

Let G be a group and $c, g \in G$.

- $Z(G)$: the center of G
- $\mathbb{C}_G(c)$: the centralizer of c
- $c^G = \{c^g = g^{-1}cg \mid g \in G\}$, the conjugacy class of c
- $[c, g] = c^{-1}g^{-1}cg$: a commutator
- $K(G)$: the collection of all commutators of G
- G': the commutator subgroup which is generated by $K(G)$

Definition

A subset X of G is called normal (or G-invariant) if

$$X^g = g^{-1}Xg = X \text{ for all } g \in G.$$

Proposition

Every group G can be express as

$$G = {c_{\alpha_0}}^G \cup {c_\alpha}^G \cup {c_\beta}^G \cup {c_\gamma}^G \cup \cdots, c_{\alpha_0} = 1,$$

for some $c_\alpha, c_\beta, c_\gamma \in G$, $\alpha_0, \alpha, \beta, \gamma \in I$, an index set, such that ${c_s}^G \cap {c_t}^G = \varnothing$ for all $s, t \in I$. The decomposition is unique up to conjugation. In particular, I is finite when G is finite.

The number $|I|$ is called the class number of a finite group G.

Thus any subset of a group must be contained in a union of some conjugacy classes.

Proposition

Every group G can be express as

$$G = {c_{\alpha_0}}^G \cup {c_\alpha}^G \cup {c_\beta}^G \cup {c_\gamma}^G \cup \cdots, c_{\alpha_0} = 1,$$

for some $c_\alpha, c_\beta, c_\gamma \in G$, $\alpha_0, \alpha, \beta, \gamma \in I$, an index set, such that ${c_s}^G \cap {c_t}^G = \varnothing$ for all $s, t \in I$. The decomposition is unique up to conjugation. In particular, I is finite when G is finite.

The number $|I|$ is called the class number of a finite group G.
Thus any subset of a group must be contained in a union of some conjugacy classes.

Let G be a finite group and $\{c_i{}^G\}_{i\in I}$ be the collection of conjugacy classes. For any subset $X \subseteq G$, set

$$\eta(X) = \left|\{i \in I \mid X \cap c_i{}^G \neq \varnothing\}\right| < \infty.$$

Evidently, $\eta(G) = |I|$, the class number of G, and $\eta(c_i{}^G) = 1$ for all $i \in I$.

Conjecture (Z. Arad and M. Herzog, 1985)

Let G be a finite non-abelian simple group and a^G, b^G be two non-trivial conjugacy class. Then $a^G b^G \neq (ab)^G$, i.e., $\eta(a^G b^G) \neq 1$.

Some non-abelian groups which may not be simple behave similar.

Let G be a finite group and $\{{c_i}^G\}_{i \in I}$ be the collection of conjugacy classes. For any subset $X \subseteq G$, set

$$\eta(X) = \left|\{i \in I \mid X \cap {c_i}^G \neq \varnothing\}\right| < \infty.$$

Evidently, $\eta(G) = |I|$, the class number of G, and $\eta({c_i}^G) = 1$ for all $i \in I$.

Conjecture (Z. Arad and M. Herzog, 1985)

Let G be a finite non-abelian simple group and a^G, b^G be two non-trivial conjugacy class. Then $a^G b^G \neq (ab)^G$, i.e., $\eta(a^G b^G) \neq 1$.

Some non-abelian groups which may not be simple behave similar.

Let G be a finite group and $\{{c_i}^G\}_{i\in I}$ be the collection of conjugacy classes. For any subset $X \subseteq G$, set

$$\eta(X) = \left|\{i \in I \mid X \cap {c_i}^G \neq \varnothing\}\right| < \infty.$$

Evidently, $\eta(G) = |I|$, the class number of G, and $\eta({c_i}^G) = 1$ for all $i \in I$.

Conjecture (Z. Arad and M. Herzog, 1985)

Let G be a finite non-abelian simple group and a^G, b^G be two non-trivial conjugacy class. Then $a^G b^G \neq (ab)^G$, i.e., $\eta(a^G b^G) \neq 1$.

Some non-abelian groups which may not be simple behave similar.

Let G be a finite group and $\{{c_i}^G\}_{i\in I}$ be the collection of conjugacy classes. For any subset $X \subseteq G$, set

$$\eta(X) = \left|\{i \in I \mid X \cap {c_i}^G \neq \varnothing\}\right| < \infty.$$

Evidently, $\eta(G) = |I|$, the class number of G, and $\eta({c_i}^G) = 1$ for all $i \in I$.

Conjecture (Z. Arad and M. Herzog, 1985)

Let G be a finite non-abelian simple group and a^G, b^G be two non-trivial conjugacy class. Then $a^G b^G \neq (ab)^G$, i.e., $\eta(a^G b^G) \neq 1$.

Some non-abelian groups which may not be simple behave similar.

Denote $\min(G) = \{\eta(a^G b^G) \mid a, b \in G \setminus Z(G)\}$.

Theorem (E. Adan-Bante, J. M. Harris and H. Verrill, 2008-2009)

For $n \geq 6$	*For* $n, q \geq 2$
$\min(S_n) = 2$ *or* 3	$\min(\mathrm{GL}(n,q)) \geq q-1$
$\min(A_n) = 2$, 4 *or* 5	$\min(\mathrm{SL}(n,q)) \geq \lceil \frac{q}{2} \rceil$

But results for $\mathrm{GL}(n,q)$ and $\mathrm{SL}(n,q)$ are not optimal for general n and q. For example, they checked $\min(\mathrm{GL}(2,2^m)) = 2^m - 1$ for $m > 1$. Using GAP, they checked that $\min(\mathrm{GL}(2,q)) = q-1$ for $q \in \{3,5,7,9,11,13\}$, but $\min(\mathrm{GL}(3,3)) = 4 > 2$.

Denote $\min(G) = \{\eta(a^G b^G) \mid a, b \in G \setminus Z(G)\}$.

Theorem (E. Adan-Bante, J. M. Harris and H. Verrill, 2008-2009)

For $n \geq 6$	*For* $n, q \geq 2$
$\min(S_n) = 2$ *or 3*	$\min(\mathrm{GL}(n,q)) \geq q - 1$
$\min(A_n) = 2,$ *4 or 5*	$\min(\mathrm{SL}(n,q)) \geq \lceil \frac{q}{2} \rceil$

But results for $\mathrm{GL}(n,q)$ and $\mathrm{SL}(n,q)$ are not optimal for general n and q. For example, they checked $\min(\mathrm{GL}(2,2^m)) = 2^m - 1$ for $m > 1$. Using GAP, they checked that $\min(\mathrm{GL}(2,q)) = q - 1$ for $q \in \{3,5,7,9,11,13\}$, but $\min(\mathrm{GL}(3,3)) = 4 > 2$.

Denote $\min(G) = \{\eta(a^G b^G) \mid a, b \in G \setminus Z(G)\}$.

Theorem (E. Adan-Bante, J. M. Harris and H. Verrill, 2008-2009)

For $n \geq 6$	*For* $n, q \geq 2$
$\min(S_n) = 2$ *or 3*	$\min(\mathrm{GL}(n,q)) \geq q - 1$
$\min(A_n) = 2$, *4 or 5*	$\min(\mathrm{SL}(n,q)) \geq \lceil \frac{q}{2} \rceil$

But results for $\mathrm{GL}(n,q)$ and $\mathrm{SL}(n,q)$ are not optimal for general n and q. For example, they checked $\min(\mathrm{GL}(2,2^m)) = 2^m - 1$ for $m > 1$. Using GAP, they checked that $\min(\mathrm{GL}(2,q)) = q - 1$ for $q \in \{3,5,7,9,11,13\}$, but $\min(\mathrm{GL}(3,3)) = 4 > 2$.

We modified their GAP code and checked:

$\min(\mathrm{GL}(2,q)) = q-1$ for $q \in \{17, 19, 23, 25, 27, 29, 31, 37\}$, $\min(\mathrm{GL}(3,2)) = 3 > 1$, $\min(\mathrm{GL}(3,4)) = 5 > 3$, $\min(\mathrm{SL}(3,3)) = 4 > 2$ and $\min(\mathrm{SL}(3,4)) = 8 > 2$. Furthermore, we find some matrices $A, B \in G \setminus Z(G)$, $G = \mathrm{GL}(3,q)$, such that $\eta(A^G B^G) = q+1$ for $q \in \{5, 7, 8, 9, 11\}$. We conjecture that:

Conjecture

- $\min(\mathrm{GL}(2,q)) = q-1$ for all q.
- $\min(\mathrm{GL}(3,q)) = q+1$ for all q.
- For fixed n, there is a $a_n \in \mathbb{Z}$ such that $\min(\mathrm{GL}(n,q)) = q + a_n$ for all q.

We modified their GAP code and checked:
$\min(\mathrm{GL}(2,q)) = q-1$ for $q \in \{17, 19, 23, 25, 27, 29, 31, 37\}$, $\min(\mathrm{GL}(3,2)) = 3 > 1$, $\min(\mathrm{GL}(3,4)) = 5 > 3$, $\min(\mathrm{SL}(3,3)) = 4 > 2$ and $\min(\mathrm{SL}(3,4)) = 8 > 2$. Furthermore, we find some matrices $A, B \in G \setminus Z(G)$, $G = \mathrm{GL}(3,q)$, such that $\eta(A^G B^G) = q+1$ for $q \in \{5, 7, 8, 9, 11\}$. We conjecture that:

Conjecture

- $\min(\mathrm{GL}(2,q)) = q-1$ for all q.
- $\min(\mathrm{GL}(3,q)) = q+1$ for all q.
- For fixed n, there is a $a_n \in \mathbb{Z}$ such that $\min(\mathrm{GL}(n,q)) = q + a_n$ for all q.

We modified their GAP code and checked:
$\min(\mathrm{GL}(2,q)) = q-1$ for $q \in \{17,19,23,25,27,29,31,37\}$,
$\min(\mathrm{GL}(3,2)) = 3 > 1$, $\min(\mathrm{GL}(3,4)) = 5 > 3$,
$\min(\mathrm{SL}(3,3)) = 4 > 2$ and $\min(\mathrm{SL}(3,4)) = 8 > 2$. Furthermore, we find some matrices $A, B \in G \setminus Z(G)$, $G = \mathrm{GL}(3,q)$, such that $\eta(A^G B^G) = q+1$ for $q \in \{5,7,8,9,11\}$. We conjecture that:

Conjecture

- $\min(\mathrm{GL}(2,q)) = q-1$ for all q.
- $\min(\mathrm{GL}(3,q)) = q+1$ for all q.
- For fixed n, there is a $a_n \in \mathbb{Z}$ such that $\min(\mathrm{GL}(n,q)) = q + a_n$ for all q.

We call $c^{-1}c^G = \{c^{-1}c^g \mid g \in G\} = \{[c, g] \mid g \in G\}$ is a c-commutator set, denoted by $[c, G]$.

Lemma

$\eta(a^G b^G) = \eta(ab^G) = \eta(a^G b).$

Lemma (E. Adan-Bante, 2006)

Let G be a group and $c \in G$. If $[c, G]$ is a subgroup of G, then it is normal.

We call $c^{-1}c^G = \{c^{-1}c^g \mid g \in G\} = \{[c,g] \mid g \in G\}$ is a c-commutator set, denoted by $[c,G]$.

Lemma

$\eta(a^G b^G) = \eta(ab^G) = \eta(a^G b)$.

Lemma (E. Adan-Bante, 2006)

Let G be a group and $c \in G$. If $[c,G]$ is a subgroup of G, then it is normal.

Theorem (E. Adan-Bante, 2006)

Let G be a finite group, a^G and b^G be conjugacy classes of G. Assume that $\mathbb{C}_G(a) = \mathbb{C}_G(b)$. Then $a^G b^G = (ab)^G$ if and only if $[ab, G] = [a, G] = [b, G]$ and $[ab, G]$ is a normal subgroup of G. In particular, given any conjugacy class a^G of G, then $a^G a^G = (a^2)^G$ if and only if $[a, G]$ is a normal subgroup of G.

Corollary (E. Adan-Bante, 2006)

Let G be a finite non-abelian simple group, a^G and b^G be conjugacy classes of G. Assume that $\mathbb{C}_G(a) = \mathbb{C}_G(b)$. Then $a^G b^G = (ab)^G$ if and only if $a = b = 1_G$. In particular, $a^G a^G = (a^2)^G$ if and only if $a = 1_G$.

Theorem (Sun)

Let G be a finite group, a^G and b^G be conjugacy classes of G. Then the following are equivalent:

- $|\mathbb{C}_G(ab)| \geq \max\{|\mathbb{C}_G(a)|, |\mathbb{C}_G(b)|\}$ *and* $a^G b^G = (ab)^G$,
- $[ab, G] = [a, G] = [b, G] \trianglelefteq G$.

This is equivalent to

Theorem (Sun)

Let G be a finite group, a^G and b^G be conjugacy classes of G. Then the following are equivalent:

- $|(ab)^G| \leq \min\{|a^G|, |b^G|\}$ *and* $a^G b^G = (ab)^G$,
- $[ab, G] = [a, G] = [b, G] \trianglelefteq G$.

Corollary (Sun)

Let G be a finite non-abelian simple group, a^G and b^G be conjugacy classes of G. Then the following are equivalent:

- $|\mathbb{C}_G(ab)| \geq \max\{|\mathbb{C}_G(a)|, |\mathbb{C}_G(b)|\}$ *and* $a^G b^G = (ab)^G$,
- $|(ab)^G| \leq \min\left\{|a^G|, |b^G|\right\}$ *and* $a^G b^G = (ab)^G$,
- $a = b = 1_G$.

Proposition (E. Adan-Bante, 2006)

Let G be a finite group, a^G and b^G be conjugacy classes with $\mathbb{C}_G(a) = \mathbb{C}_G(b)$ and $|a^G| = 2$. Then $\eta(a^G b^G) = 2$. In particular, $\eta(a^G a^G) = 2$.

Proposition (Sun)

Let G be a finite group, a^G and b^G be conjugacy classes with $|a^G| = 2$. Then $\eta(a^G b^G) \leq 2$.

- *If $\eta(a^G b^G) = 1$, then either $\mathbb{C}_G(a) \nsubseteq \mathbb{C}_G(b)$ or $\mathbb{C}_G(b) \nsubseteq \mathbb{C}_G(a)$.*
- *If $\eta(a^G b^G) = 2$, then $\mathbb{C}_G(b) \subseteq \mathbb{C}_G(a)$ and so $2 \mid |b^G|$.*

In particular, $\eta(a^G a^G) = 2$ and $\eta(a^G (a^{-1})^G) = 2$.

Theorem (Sun)

Let G be a (finite) group and $c \in G$. Then the following are equivalent:

- $[c, G]$ *is a subgroup of* G,
- $[c, G] = [c', G]$ *for all* $c' \in c^G$,
- $[c, G]$ *is normal,*
- $[c, G] = c^{-1}c^G = (c^{-1})^G c^G$.

The existence for which $[c, G]$ is a subgroup of G.

Proposition (Sun)

Let G be a non-trivial finite group. Then the following are equivalent:

- $G = H \cup C$ *where H is a proper normal subgroup and C is a conjugacy class.*
- $G = [c, G] \cup c^G$ *for some $c \in G$.*

Example

- $S_3 = A_3 \cup (1\,2)^{S_3} = [(1\,2), S_3] \cup (1\,2)^{S_3}$.
- Every finite non-abelian group of order $2p$, p is an odd prime, can be decomposed the such form.

The existence for which $[c, G]$ is a subgroup of G.

Proposition (Sun)

Let G be a non-trivial finite group. Then the following are equivalent:

- $G = H \cup C$ *where H is a proper normal subgroup and C is a conjugacy class.*
- $G = [c, G] \cup c^G$ *for some $c \in G$.*

Example

- $S_3 = A_3 \cup (1\,2)^{S_3} = [(1\,2), S_3] \cup (1\,2)^{S_3}$.
- Every finite non-abelian group of order $2p$, p is an odd prime, can be decomposed the such form.

Conjecture

Let p be an odd prime and let $n \in \mathbb{N}$. Then there is a positive integer $m_n \geq n$ such that there exist m_n non-isomorphic finite non-abelian groups G with order $2p^n$ such that $G = [c, G] \cup c^G$ for some $c \in G$. In particular, p and m_n are independent, i.e. m_n is fixed when n is fixed, for any odd prime p.

We have checked some cases by GAP:

- For $n = 1$, $m_1 = 1$ for all odd primes by Example.
- For $n = 2$, $m_2 = 2$ for odd primes $p \leq 101$.
- For $n = 3$, $m_3 = 3$ for odd primes $p \leq 7$.
- For $n = 4$, $m_4 = 5$ for odd primes $p \leq 7$.
- For $n = 5$, $m_5 = 7$ for odd primes $p \leq 5$.

Conjecture (J. Thompson, unknown)

Let G be a finite non-abelian simple group. Then there exists a non-trivial conjugacy class c^G of G such that $G = c^G c^G$. In particular, $c^G = (c^{-1})^G$.

Conjecture (Ore, 1951, solved in 2010)

Every element in a finite non-abelian simple group is a commutator.

J. Thompson's conjecture can imply Ore's conjecture. However, Ore's conjecture is solved by M. W. Liebeck, E. A. O'Brien, A. Shalev, and P. H. Tiep in 2010.

Conjecture (J. Thompson, unknown)

Let G be a finite non-abelian simple group. Then there exists a non-trivial conjugacy class c^G of G such that $G = c^G c^G$. In particular, $c^G = (c^{-1})^G$.

Conjecture (Ore, 1951, solved in 2010)

Every element in a finite non-abelian simple group is a commutator.

J. Thompson's conjecture can imply Ore's conjecture. However, Ore's conjecture is solved by M. W. Liebeck, E. A. O'Brien, A. Shalev, and P. H. Tiep in 2010.

Recall that $K(G) = \{[g, h] \mid g, h \in G\}$ consists all commutators of G and $G' = \langle K(G) \rangle$ is the commutator subgroup of G. For small order of groups, $K(G) = G'$, but not for larger order. For example, the smallest order of the group such that $K(G) \neq G'$ is 96, J. J. Rotman states that the group is found via the computer.

Definition

Let X be a subset of G. We say that X is real if $x^{-1} \in X$ for all $x \in X$; X is "commutative" if $(gX)(hX) = (hX)(gX)$ for all $g, h \in G$, i.e., the product is commutative.

Note that if X is normal, then $(gX)(hX) = (gh)XX$.

Recall that $K(G) = \{[g,h] \mid g,h \in G\}$ consists all commutators of G and $G' = \langle K(G) \rangle$ is the commutator subgroup of G. For small order of groups, $K(G) = G'$, but not for larger order. For example, the smallest order of the group such that $K(G) \neq G'$ is 96, J. J. Rotman states that the group is found via the computer.

Definition

Let X be a subset of G. We say that X is real if $x^{-1} \in X$ for all $x \in X$; X is "commutative" if $(gX)(hX) = (hX)(gX)$ for all $g, h \in G$, i.e., the product is commutative.

Note that if X is normal, then $(gX)(hX) = (gh)XX$.

Theorem (well-known)

Let G be a group and let N be a normal subgroup of G. Then G/N is abelian if and only if $G' \leq N$.

Lemma (Sun)

Let G be a group and let X be a normal and real subset of G. If X is "commutative", then $K(G) \subseteq XX = X^2$.

By Ore's "Theorem", we have

Lemma (Sun)

Let G be a finite non-abelian simple group and C be a real conjugacy class of G. Then C is "commutative" if and only if $G = C^2$.

Theorem (well-known)

Let G be a group and let N be a normal subgroup of G. Then G/N is abelian if and only if $G' \leq N$.

Lemma (Sun)

Let G be a group and let X be a normal and real subset of G. If X is "commutative", then $K(G) \subseteq XX = X^2$.

By Ore's "Theorem", we have

Lemma (Sun)

Let G be a finite non-abelian simple group and C be a real conjugacy class of G. Then C is "commutative" if and only if $G = C^2$.

Theorem (well-known)

Let G be a group and let N be a normal subgroup of G. Then G/N is abelian if and only if $G' \leq N$.

Lemma (Sun)

Let G be a group and let X be a normal and real subset of G. If X is "commutative", then $K(G) \subseteq XX = X^2$.

By Ore's "Theorem", we have

Lemma (Sun)

Let G be a finite non-abelian simple group and C be a real conjugacy class of G. Then C is "commutative" if and only if $G = C^2$.

Given a conjugacy class number $\eta(G)$, how many non-isomorphic finite groups satisfy that?

Fix $\eta(G) = n$, $G = {c_1}^G \cup {c_2}^G \cup \cdots \cup {c_n}^G$, $c_1 = 1$, thus

$$|G| = |{c_1}^G| + |{c_2}^G| + \cdots + |{c_n}^G|,$$

so

$$1 = \frac{1}{m_1} + \frac{1}{m_2} + \cdots + \frac{1}{m_n} \quad (1)$$

where $m_i = \frac{|G|}{|{c_i}^G|} = |\mathbb{C}_G(c_i)|$.

In 1903, E. Landau proved Equation (1) has only finitely many solutions over the positive integers for each n.

Given a conjugacy class number $\eta(G)$, how many non-isomorphic finite groups satisfy that?

Fix $\eta(G) = n$, $G = {c_1}^G \cup {c_2}^G \cup \cdots \cup {c_n}^G$, $c_1 = 1$, thus

$$|G| = |{c_1}^G| + |{c_2}^G| + \cdots + |{c_n}^G|,$$

so

$$1 = \frac{1}{m_1} + \frac{1}{m_2} + \cdots + \frac{1}{m_n} \tag{1}$$

where $m_i = \frac{|G|}{|{c_i}^G|} = |\mathbb{C}_G(c_i)|$.

In 1903, E. Landau proved Equation (1) has only finitely many solutions over the positive integers for each n.

Given a conjugacy class number $\eta(G)$, how many non-isomorphic finite groups satisfy that?

Fix $\eta(G) = n$, $G = {c_1}^G \cup {c_2}^G \cup \cdots \cup {c_n}^G$, $c_1 = 1$, thus

$$|G| = |{c_1}^G| + |{c_2}^G| + \cdots + |{c_n}^G|,$$

so

$$1 = \frac{1}{m_1} + \frac{1}{m_2} + \cdots + \frac{1}{m_n} \tag{1}$$

where $m_i = \frac{|G|}{|{c_i}^G|} = |\mathbb{C}_G(c_i)|$.

In 1903, E. Landau proved Equation (1) has only finitely many solutions over the positive integers for each n.

$\eta(G)$	
≤ 5	Miller and Burnside, complete
6, 7	Sigley, incomplete for $\eta(G) = 6$; $Z(G) \neq 1$ for $\eta(G) = 7$
6, 7	Poland, complete
8	Kosvintsev, valid solutions proposed by a computer
9	Odincov and Starostin, complete
≤ 12	Aleksandrov and Komissarcik, all finite simple groups

How many groups satisfy that $|G| = |{c_1}^G| + |{c_2}^G| + \cdots + |{c_n}^G|$ where $|{c_i}^G| \neq |{c_j}^G|$ for $i \neq j$?

Conjecture (F. M. Markel, 1973)

$G \cong S_3$.

That is called S_3-conjecture.

Thank you for your attention!