ARS MATHEMATICA CONTEMPORANEA

Also available at http://amc-journal.eu
ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 10 (2016) 67–77

Commutators of cycles in permutation groups

Aleš Vavpetič *

Fakulteta za Matematiko in Fiziko, Univerza v Ljubljani,
Jadranska ulica 19, SI-1111 Ljubljana, Slovenija

Received 10 January 2013, accepted 26 September 2014, published online 27 May 2015

Abstract

We prove that for $n \geq 5$, every element of the alternating group A_n is a commutator of two cycles of A_n. Moreover we prove that for $n \geq 2$, a $(2n+1)$-cycle of the permutation group S_{2n+1} is a commutator of a p-cycle and a q-cycle of S_{2n+1} if and only if the following three conditions are satisfied (i) $n+1 \leq p, q$, (ii) $2n+1 \geq p, q$, (iii) $p+q \geq 3n+1$.

Keywords: Commutator, cycle, permutation, alternating group.

Math. Subj. Class.: 20B05

1 Introduction

In 1951 O. Ore [9] conjectured that in a finite simple non-abelian group every element is a commutator. In the same paper he proved that the conjecture holds for the alternating group A_n, where $n \geq 5$, but the result had already been proved by G. A. Miller half a century earlier [7]. After Ore published the paper there were many papers devoted to the Ore conjecture: R. C. Thompson proved the Ore conjecture for the projective special linear groups $PSL_n(q)$ [10], [11], [12], R. Gow proved it for the projective simplectic groups $PSp_{2n}(q)$, where $q \equiv 1 \pmod 4$ [4], O. Bonten for the exceptional groups of Lie type of low rank [2], J. Neubüser, H. Pahlings, E. Cleuvers proved it for the sporadic groups [8], E. W. Ellers, N. Gordeev handled the finite simple groups of Lie type over a finite field $\mathbb{F}_q$, whenever $q \geq 9$, ... M. W. Liebeck, E. A. O'Brien, A. Shalev, P. H. Tiep proved the Ore conjecture for the remaining cases [6] and the conjecture became the theorem. We refer the reader to the survey paper [5] for more historical notes about commutators and the Ore conjecture.

In this paper we prove a stronger version of the Ore conjecture for the simple alternating group A_n. In Section 2 it is shown that, for $n \geq 5$, every permutation of A_n is actually a

*This research was supported by the Slovenian Research Agency grants P1-0292-0101 and J1-5435-0101.
E-mail address: ales.vavpetic@fmf.uni-lj.si (Aleš Vavpetič)

commutator of two cycles of A_n. In particular, every even permutation of the symmetric group S_n is a product of two conjugate cycles. Namely, if $\rho = [\sigma,\tau] = \sigma^{-1}\tau^{-1}\sigma\tau$, then ρ is a product of $\sigma^{-1}\tau^{-1}\sigma$ and τ (and also a product of σ^{-1} and $\tau^{-1}\sigma\tau$). Note that permutations τ and τ^{-1} are conjugate in S_n. In [1] it is proved that a $(2n+1)$-cycle of A_{2n+1} is a product of two conjugate l-cycles of A_{2n+1} if and only if $l \geq n+1$. Hence this is a necessary condition for the existence of two l-cycles σ and τ such that $[\sigma,\tau]$ is a $(2n+1)$-cycle. In Section 3 it is shown that this is far from being a sufficient condition. More precisely, it is shown that, for $n \geq 2$, a $(2n+1)$-cycle of A_{2n+1} is a commutator of a p-cycle and a q-cycle of S_{2n+1} if and only if $n+1 \leq p,q$ and $p+q \geq 3n+1$. In particular, a $(2n+1)$-cycle of A_{2n+1} ($n \geq 2$) is a commutator of l-cycles of S_{2n+1} if and only if $l \geq \frac{3n+1}{2}$.

The image of an element a under a permutation σ is denoted by a^σ. Permutations are executed from left to right. The support $\operatorname{supp}\sigma$ of a permutation σ is the set of all elements which are not fixed by σ.

Let σ be a permutation, $a \in \operatorname{supp}\sigma$ and $x_1,\ldots,x_n \notin \operatorname{supp}\sigma$. We define permutations $\varphi(\sigma;a,x_1,\ldots,x_n)$ and $\varepsilon(\sigma;a)$ by

$$t^{\varphi(\sigma;a,x_1,\ldots,x_n)} = \begin{cases} x_1, & t=a,\\ x_{i+1}, & t\in\{x_1,\ldots,x_{n-1}\},\\ a^\sigma, & t=x_n,\\ t^\sigma, & t\notin\{a,x_1,\ldots,x_n\},\end{cases}$$

and

$$t^{\varepsilon(\sigma;a)} = \begin{cases} a, & t=a,\\ a^\sigma, & t=a^{\sigma^{-1}},\\ t^\sigma, & t\notin\{a,a^{\sigma^{-1}}\}.\end{cases}$$

If σ is the k-cycle $(a_1,\ldots,a_k)$, then $\varphi(\sigma;a_k,x_1,\ldots,x_n)$ is the $(k+n)$-cycle $(a_1,\ldots,a_k, x_1,\ldots,x_n)$ and $\varepsilon(\sigma;a_k)$ is the $(k-1)$-cycle $(a_1,\ldots,a_{k-1})$.

Let σ and τ be permutations such that $\operatorname{supp}\sigma\cap\operatorname{supp}\tau=\emptyset$. For $a\in\operatorname{supp}\sigma$ and $b\in\operatorname{supp}\tau$, let $\psi(\sigma,\tau;a,b)$ denote the permutation defined by

$$t^{\psi(\sigma,\tau;a,b)} = \begin{cases} t^\sigma, & t\in\operatorname{supp}\sigma-\{a\},\\ b^\tau, & t=a,\\ t^\tau, & t\in\operatorname{supp}\tau-\{b\},\\ a^\sigma, & t=b.\end{cases}$$

If τ is a k-cycle then $\psi(\sigma,\tau;a,b)=\varphi(\sigma;a,b^\tau,b^{\tau^2},\ldots,b^{\tau^k})$, and if σ is a k-cycle then $\psi(\sigma,\tau;a,b)=\varphi(\tau;b,a^\sigma,a^{\sigma^2},\ldots,a^{\sigma^k})$.

2 Permutations as commutators of cycles

The proof that every permutation of A_n ($n\geq 5$) is a commutator of two cycles is based on induction on the number and the lengths of cycles in the cycle decomposition of the permutation. In the following lemmas we describe how the application of φ, ψ, and ε modify commutators.

Lemma 2.1. *Let σ, τ be permutations, $x \in \operatorname{supp}\sigma$, $y \in \operatorname{supp}\tau$, and $(\operatorname{supp}\sigma \cup \operatorname{supp}\tau) \cap (\{x_1, \ldots, x_n\} \cup \{y_1, \ldots, y_m\}) = \emptyset$. Then for $t \notin \{x^\sigma, x^{\tau\sigma}, y^{\tau\sigma}, y^{\sigma^{-1}\tau\sigma}, x_1, \ldots, x_n, y_1, \ldots, y_m\}$ we have $t^{[\sigma,\tau]} = t^{[\varphi(\sigma;x,x_1,\ldots,x_n),\varphi(\tau;y,y_1,\ldots,y_m)]}$.*

Proof. Denote $\widetilde{\sigma} = \varphi(\sigma; x, x_1, \ldots, x_n)$ and $\widetilde{\tau} = \varphi(\tau; y, y_1, \ldots, y_m)$. For $t \notin \{x^\sigma, x^{\tau\sigma}, y^{\tau\sigma}, y^{\sigma^{-1}\tau\sigma}, x_1, \ldots, x_n, y_1, \ldots, y_m\}$ we have $t^{\sigma^{-1}} = t^{\widetilde{\sigma}^{-1}}$. Since $t \notin \{y^{\tau\sigma}, y_1, \ldots, y_m\}$, also $t^{\sigma^{-1}} \notin \{y^\tau, y_1, \ldots, y_m\}$ and therefore $t^{\sigma^{-1}\tau^{-1}} = t^{\widetilde{\sigma}^{-1}\widetilde{\tau}^{-1}}$. Since $t^{\sigma^{-1}\tau^{-1}} \notin \{x, x_1, \ldots, x_n\}$ we have $t^{\sigma^{-1}\tau^{-1}\sigma} = t^{\widetilde{\sigma}^{-1}\widetilde{\tau}^{-1}\widetilde{\sigma}}$. And finally $t^{\sigma^{-1}\tau^{-1}\sigma} \notin \{y, y_1, \ldots, y_m\}$, hence $t^{[\sigma,\tau]} = t^{[\widetilde{\sigma},\widetilde{\tau}]}$. □

We record the following immediate consequence.

Corollary 2.2. *Let σ, τ be permutations. Suppose that $a, b \in \operatorname{supp}\sigma$ such that $a^\sigma = a^\tau = b$, and $(\operatorname{supp}\sigma \cup \operatorname{supp}\tau) \cap (\{x_1, \ldots, x_n\} \cup \{y_1, \ldots, y_m\}) = \emptyset$. Then for $t \notin \{b^\sigma, b^{\tau\sigma}, x_1, \ldots, x_n, y_1, \ldots, y_m\}$ we have $t^{[\sigma,\tau]} = t^{[\varphi(\sigma;b,x_1,\ldots,x_n),\varphi(\tau;b,y_1,\ldots,y_m)]}$.*

Lemma 2.3. *Let σ, τ be permutations and $a, b \in \operatorname{supp}\sigma$ such that $b = a^\sigma = a^\tau$ and $c, d \notin \operatorname{supp}\sigma \cup \operatorname{supp}\tau$. Then*

$$[\varphi(\sigma; b, c, d), \varphi(\tau; b, d, c)] = \varphi([\sigma, \tau]; b^{\tau\sigma}, c, d).$$

Proof. Denote $\widetilde{\sigma} = \varphi(\sigma; b, c, d)$ and $\widetilde{\tau} = \varphi(\tau; b, d, c)$. By Corollary 2.2, we have $t^{[\widetilde{\sigma},\widetilde{\tau}]} = t^{[\sigma,\tau]}$ for $t \notin \{b^\sigma, b^{\tau\sigma}, c, d\}$. Because

$$\begin{aligned}
(b^{\tau\sigma})^{[\widetilde{\sigma},\widetilde{\tau}]} &= (b^\tau)^{\widetilde{\tau}^{-1}\widetilde{\sigma}\widetilde{\tau}} = c^{\widetilde{\sigma}\widetilde{\tau}} = d^{\widetilde{\tau}} = c,\\
c^{[\widetilde{\sigma},\widetilde{\tau}]} &= b^{\widetilde{\tau}^{-1}\widetilde{\sigma}\widetilde{\tau}} = a^{\widetilde{\sigma}\widetilde{\tau}} = b^{\widetilde{\tau}} = d,\\
d^{[\widetilde{\sigma},\widetilde{\tau}]} &= c^{\widetilde{\tau}^{-1}\widetilde{\sigma}\widetilde{\tau}} = d^{\widetilde{\sigma}\widetilde{\tau}} = (b^\sigma)^{\widetilde{\tau}} = b^{\sigma\tau} = (b^{\tau\sigma})^{[\sigma,\tau]},\\
(b^\sigma)^{[\widetilde{\sigma},\widetilde{\tau}]} &= d^{\widetilde{\tau}^{-1}\widetilde{\sigma}\widetilde{\tau}} = b^{\widetilde{\sigma}\widetilde{\tau}} = c^{\widetilde{\tau}} = b^\tau = (a^\sigma)^\tau = (b^{\tau^{-1}})^{\sigma\tau} = (b^\sigma)^{[\sigma,\tau]},
\end{aligned}$$

we have $[\varphi(\sigma; b, c, d), \varphi(\tau; b, d, c)] = \varphi([\sigma, \tau]; b^{\tau\sigma}, c, d)$. □

Lemma 2.4. *Let σ, τ be permutations and $a, b \in \operatorname{supp}\sigma$ such that $b = a^\sigma = a^\tau$ and $c, d \notin \operatorname{supp}\sigma \cup \operatorname{supp}\tau$. Then*

$$\begin{aligned}
[\varphi(\sigma; b, c, d), \varphi(\tau; b, d)] &= \varphi([\sigma, \tau]; b^\sigma, c, d),\\
[\varphi(\sigma; b, d), \varphi(\tau; b, c, d)] &= \varphi([\sigma, \tau]; b^\sigma, d, c).
\end{aligned}$$

Proof. Denote $\widetilde{\sigma} = \varphi(\sigma; b, c, d)$ and $\widetilde{\tau} = \varphi(\tau; b, d)$. By Corollary 2.2, we have $t^{[\widetilde{\sigma},\widetilde{\tau}]} = t^{[\sigma,\tau]}$ for $t \notin \{b^\sigma, b^{\tau\sigma}, c, d\}$. Because

$$\begin{aligned}
(b^\sigma)^{[\widetilde{\sigma},\widetilde{\tau}]} &= d^{\widetilde{\tau}^{-1}\widetilde{\sigma}\widetilde{\tau}} = b^{\widetilde{\sigma}\widetilde{\tau}} = c^{\widetilde{\tau}} = c,\\
c^{[\widetilde{\sigma},\widetilde{\tau}]} &= b^{\widetilde{\tau}^{-1}\widetilde{\sigma}\widetilde{\tau}} = a^{\widetilde{\sigma}\widetilde{\tau}} = b^{\widetilde{\tau}} = d,\\
d^{[\widetilde{\sigma},\widetilde{\tau}]} &= c^{\widetilde{\tau}^{-1}\widetilde{\sigma}\widetilde{\tau}} = c^{\widetilde{\sigma}\widetilde{\tau}} = d^{\widetilde{\tau}} = b^\tau = (a^\sigma)^\tau = (b^{\tau^{-1}})^{\sigma\tau} = (b^\sigma)^{[\sigma,\tau]},\\
(b^{\tau\sigma})^{[\widetilde{\sigma},\widetilde{\tau}]} &= (b^\tau)^{\widetilde{\tau}^{-1}\widetilde{\sigma}\widetilde{\tau}} = d^{\widetilde{\sigma}\widetilde{\tau}} = (b^\sigma)^{\widetilde{\tau}} = b^{\sigma\tau} = (b^{\tau\sigma})^{[\sigma,\tau]},
\end{aligned}$$

we have $[\varphi(\sigma; b, c, d), \varphi(\tau; b, d)] = \varphi([\sigma, \tau]; b^\sigma, c, d)$.

Because $[\sigma,\tau]^{-1} = [\tau,\sigma]$ and $(b^\tau)^{[\tau,\sigma]} = b^\sigma$, we have

$$\begin{aligned}[\varphi(\sigma;b,d),\varphi(\tau;b,c,d)] &= ([\varphi(\tau;b,c,d),\varphi(\sigma;b,d)])^{-1} = \\ &= \varphi([\tau,\sigma];b^\tau,c,d)^{-1} = \\ &= \varphi([\sigma,\tau];b^\sigma,d,c).\end{aligned}$$

□

Corollary 2.5. *Let ρ be a $(2n+1)$-cycle and $n \geq 2$. For $p,q \in \mathbb{N}$ such that $p,q \leq 2n+1$ and $p+q \geq 3n+2$, there exist a p-cycle σ, a q-cycle τ, and $a \in \operatorname{supp}\sigma$ such that $[\sigma,\tau] = \rho$, $\operatorname{supp}\rho = \operatorname{supp}\sigma \cup \operatorname{supp}\tau$, and $a^\sigma = a^\tau$. In the case $q \neq 2n+1$ we arrange that $a^{\sigma\sigma} \notin \operatorname{supp}\tau$.*

Proof. If $n=2$ and $p \geq q$ then $(p,q) \in \{(5,5),(5,4),(5,3),(4,4)\}$ and we have

$$\begin{aligned}(a_1,a_2,a_3,a_4,a_5) &= [(a_1,a_4,a_2,a_3,a_5),(a_1,a_4,a_3,a_5,a_2)] = \\ &= [(a_1,a_4,a_2,a_5,a_3),(a_1,a_4,a_3,a_5)] = \\ &= [(a_1,a_2,a_4,a_5,a_3),(a_1,a_2,a_5)] = \\ &= [(a_1,a_5,a_2,a_3),(a_1,a_5,a_3,a_4)].\end{aligned}$$

If $n=2$ and $p<q$, then $q = 2n+1 = 5$ and we can use the equality $[\sigma,\tau]^{-1} = [\tau,\sigma]$. In all cases $a_1^\sigma = a_1^\tau$ and if $q \neq 5$, also $a_1^{\sigma\sigma} \notin \operatorname{supp}\tau$.

Let $n > 2$. The proof is divided into 3 cases.

Case 1: Suppose $q \leq 2n$. Let $p_1 = p-2$, $q_1 = q-1$, and $n_1 = n-1$. Then $p_1+q_1 = p-2+q-1 \geq 3n_1+2$ and $p_1,q_1 \leq 2n_1+1$. By the inductive hypothesis there exist a p_1-cycle σ, a q_1-cycle τ, and $a \in \operatorname{supp}\sigma$ such that $[\sigma,\tau]$ is a $(2n_1+1)$-cycle, $\operatorname{supp}\sigma \cup \operatorname{supp}\tau = \operatorname{supp}[\sigma,\tau]$, and $a^\sigma = a^\tau$. Let $x,y \notin \operatorname{supp}\sigma \cup \operatorname{supp}\tau$, $\widetilde{\sigma} = \varphi(\sigma;a^\sigma,x,y)$, and $\widetilde{\tau} = \varphi(\tau;a^\tau,y)$. Then $\widetilde{\sigma}$ is a p-cycle, $\widetilde{\tau}$ is a q-cycle, $a^{\widetilde{\sigma}} = a^\sigma = a^\tau = a^{\widetilde{\tau}}$, $a^{\widetilde{\sigma}\widetilde{\sigma}} = x \notin \operatorname{supp}\widetilde{\tau}$, and by Lemma 2.4, $[\widetilde{\sigma},\widetilde{\tau}]$ is a $(2n+1)$-cycle and $\operatorname{supp}\widetilde{\sigma} \cup \operatorname{supp}\widetilde{\tau} = \operatorname{supp}[\widetilde{\sigma},\widetilde{\tau}]$.

Case 2: Suppose $q = 2n+1$ and $p \neq 2n+1$. This case follows from the previous case and equality $[\sigma,\tau]^{-1} = [\tau,\sigma]$.

Case 3: Suppose $p = q = 2n+1$. By the inductive hypothesis there exist $(2n-1)$-cycles σ, τ, and $a \in \operatorname{supp}\sigma$ such that $[\sigma,\tau]$ is a $(2n-1)$-cycle, $\operatorname{supp}\sigma = \operatorname{supp}\tau = \operatorname{supp}[\sigma,\tau]$, and $a^\sigma = a^\tau$. Let $x,y \notin \operatorname{supp}\sigma$, $\widetilde{\sigma} = \varphi(\sigma;a^\sigma,x,y)$, and $\widetilde{\tau} = \varphi(\tau;a^\tau,y,x)$. Then $\widetilde{\sigma}$ and $\widetilde{\tau}$ are $(2n+1)$-cycles, $a^{\widetilde{\sigma}} = a^\sigma = a^\tau = a^{\widetilde{\tau}}$, and by Lemma 2.3, $[\widetilde{\sigma},\widetilde{\tau}]$ is a $(2n+1)$-cycle and $\operatorname{supp}\widetilde{\sigma} = \operatorname{supp}\widetilde{\tau} = \operatorname{supp}[\widetilde{\sigma},\widetilde{\tau}]$. □

Lemma 2.6. *Let σ,τ be permutations and $a,b \in \operatorname{supp}\sigma$ such that $b = a^\sigma = a^\tau$, $b^\sigma \notin \operatorname{supp}\tau$, and $c \notin \operatorname{supp}\sigma \cup \operatorname{supp}\tau$. Then*

$$[\sigma,\varphi(\tau;b,c)] = \varepsilon([\sigma,\tau];b^\sigma)(c,b^\sigma).$$

Proof. Let $\widetilde{\tau} = \varphi(\tau;b,c)$. By Corollary 2.2, we get $t^{[\sigma,\widetilde{\tau}]} = t^{[\sigma,\tau]}$ for $t \notin \{b^\sigma,b^{\tau\sigma},c\}$. From

$$(b^\sigma)^{[\sigma,\widetilde{\tau}]} = b^{\widetilde{\tau}^{-1}\sigma\widetilde{\tau}} = a^{\sigma\widetilde{\tau}} = b^{\widetilde{\tau}} = c,$$

$$c^{[\sigma,\widetilde{\tau}]} = c^{\widetilde{\tau}^{-1}\sigma\widetilde{\tau}} = b^{\sigma\widetilde{\tau}} = b^\sigma,$$

$$(b^{\tau\sigma})^{[\sigma,\widetilde{\tau}]} = (b^\tau)^{\widetilde{\tau}^{-1}\sigma\widetilde{\tau}} = c^{\sigma\widetilde{\tau}} = c^{\widetilde{\tau}} = b^\tau,$$

and

$$(b^{\tau\sigma})^{[\sigma,\tau]} = b^{\sigma\tau} = b^{\sigma},$$
$$(b^{\sigma})^{[\sigma,\tau]} = b^{\tau^{-1}\sigma\tau} = a^{\sigma\tau} = b^{\tau},$$

it follows $[\sigma, \varphi(\tau; b, c)] = \varepsilon([\sigma, \tau]; b^{\sigma})(c, b^{\sigma})$. □

Corollary 2.7. *Let $n_1, n_2 \in \mathbb{N}$ and let ρ be a product of two disjoint cycles of lengths $2n_1$ and $2n_2$, respectively. If $p, q \leq 2(n_1 + n_2) - 1$ and $p + q \geq 3(n_1 + n_2)$ then there exist a p-cycle σ, a q-cycle τ, and $a \in \operatorname{supp} \sigma$ such that $\rho = [\sigma, \tau]$, $\operatorname{supp} \rho = \operatorname{supp} \sigma \cup \operatorname{supp} \tau$, and $a^{\sigma} = a^{\tau}$.*

If $n_1 = n_2 = 1$ then there exist no cycles σ and τ such that the length of one of them is strictly greater than $2(n_1 + n_2) - 1 = 3$, $[\sigma, \tau]$ is a product of two disjoint transpositions, $\operatorname{supp}[\sigma, \tau] = \operatorname{supp} \sigma \cup \operatorname{supp} \tau$, where $a^{\sigma} = a^{\tau}$ for some $a \in \operatorname{supp} \sigma$. That means that in the Corollary in this case the upper bound requirement on the length of the cycles is sharp. If $n_1 + n_2 \geq 3$ the upper bound requirement is not sharp (it can be increased to $2(n_1 + n_2)$) but the bound in the Corollary is in almost all cases sufficient for our purposes. Namely, in the case $n_1 + n_2 \geq 4$, we get $2(2(n_1 + n_2) - 2) \geq 3(n_1 + n_2)$ and therefore the Corollary provides two cycles whose lengths can be required to be (independently) either odd or even: both odd ($p = q = 2(n_1 + n_2) - 1$), both even ($p = q = 2(n_1 + n_2) - 2$), the first even and the second odd ($p = 2(n_1 + n_2) - 2, q = 2(n_1 + n_2) - 1$), the first odd and the second even.

Proof. One may assume that $n_1 \geq n_2$. The proof is by induction on n_2.

Let $n_2 = 1$. If $n_1 = 1$ then the only possibility for p and q is $p = q = 3$. In this case $[(a_1, a_2, a_3), (a_1, a_2, a_4)] = (a_1, a_2), (a_3, a_4)$. Let $n_1 \geq 2$. Because $p + (q - 1) \geq 3(n_1 + 1) - 1 = 3n_1 + 2$ and $p, q \leq 2(n_1 + 1) - 1 = 2n_1 + 1$, Corollary 2.5 provides a p-cycle σ, a $(q - 1)$-cycle τ, and $a \in \operatorname{supp} \sigma$ such that $[\sigma, \tau]$ is a $(2n_1 + 1)$-cycle, $\operatorname{supp} \sigma \cup \operatorname{supp} \tau = \operatorname{supp}[\sigma, \tau]$, $a^{\sigma} = a^{\tau}$, and $a^{\sigma\sigma} \notin \operatorname{supp} \tau$. Let $c \notin \operatorname{supp} \sigma \cup \operatorname{supp} \tau$ and $\widetilde{\tau} = \varphi(\tau; a^{\tau}, c)$. Then $\widetilde{\tau}$ is a q-cycle, $a^{\sigma} = a^{\tau} = a^{\widetilde{\tau}}$, and by Lemma 2.6, $[\sigma, \widetilde{\tau}] = \varepsilon([\sigma, \tau]; a^{\sigma\sigma})(a^{\sigma\sigma}, c)$ and $\operatorname{supp} \sigma \cup \operatorname{supp} \widetilde{\tau} = \operatorname{supp}[\sigma, \widetilde{\tau}]$. Note that $a^{\sigma\widetilde{\tau}\sigma} = c$ is in the support of the 2-cycle.

For the proof by induction, suppose that for all $n < n_2$ the assumptions $p, q \leq 2(n_1 + n) - 1$ and $p + q \geq 3(n_1 + n)$ guarantee the existence of a p-cycle σ, a q-cycle τ, and $a \in \operatorname{supp} \sigma$ such that the following hold: $[\sigma, \tau]$ is a product of two disjoint cycles of lengths $2n_1$ and $2n$, $\operatorname{supp}[\sigma, \tau] = \operatorname{supp} \sigma \cup \operatorname{supp} \tau$, $a^{\sigma} = a^{\tau}$, and $a^{\sigma\tau\sigma}$ is in the support of the $2m$-cycle in the cycle decomposition of $[\sigma, \tau]$.

We prove that the same holds for $n = n_2$. The proof is divided into 3 cases.

Case 1: Let $q < 2(n_1 + n_2) - 1$. Define $\widetilde{p} = p - 2$, $\widetilde{q} = q - 1$, and $m = n_2 - 1$. Because $\widetilde{p} + \widetilde{q} \geq 3(n_1 + m)$ and $\widetilde{p}, \widetilde{q} \leq 2(n_1 + m) - 1$, the inductive hypothesis yields a $\widetilde{p}$-cycle σ, a $\widetilde{q}$-cycle τ, and $a \in \operatorname{supp} \sigma$ such that $[\sigma, \tau] = \rho_1\rho_2$, where $\operatorname{supp} \rho_1 \cap \operatorname{supp} \rho_2 = \emptyset$, ρ_1 is a $2n_1$-cycle, ρ_2 is a $2m$-cycle, $a^{\sigma} = a^{\tau}$, and $a^{\sigma\tau\sigma} \in \operatorname{supp} \rho_2$. Let $x, y \notin \operatorname{supp} \sigma \cup \operatorname{supp} \tau$, $\widetilde{\sigma} = \varphi(\sigma; a^{\sigma}, x, y)$, and $\widetilde{\tau} = \varphi(\tau; a^{\tau}, y)$. Then $\widetilde{\sigma}$ is a p-cycle, $\widetilde{\tau}$ is a q-cycle, $a^{\widetilde{\sigma}} = a^{\sigma} = a^{\tau} = a^{\widetilde{\tau}}$, and by Lemma 2.4, $[\widetilde{\sigma}, \widetilde{\tau}] = \varphi(\rho_1\rho_2; a^{\sigma\sigma}, x, y) = \rho_1\varphi(\rho_2; a^{\sigma\sigma}, x, y)$ and $a^{\widetilde{\sigma}\widetilde{\tau}\widetilde{\sigma}} = a^{\sigma\sigma} \in \operatorname{supp} \varphi(\rho_2; a^{\sigma\sigma}, x, y)$.

Case 2: Let $p \neq 2(n_1 + n_2) - 1$ and $q = 2(n_1 + n_2) - 1$. This case follows from the previous case and the equality $[\sigma, \tau]^{-1} = [\tau, \sigma]$.

Case 3: Let $p = q = 2(n_1+n_2)-1$. Define $\widetilde{p} = \widetilde{q} = 2(n_1+n_2)-3$ and $m = n_2-1$. From $\widetilde{p}, \widetilde{q} \le 2(n_1+m)-1$ and $n_1 > 1$ we get $\widetilde{p}+\widetilde{q} \ge 3(n_1+m)$. By the inductive hypothesis there exist $\widetilde{p}$-cycles σ, τ, and $a \in \operatorname{supp}\sigma$ such that $[\sigma,\tau] = \rho_1\rho_2$, where $\operatorname{supp}\rho_1 \cap \operatorname{supp}\rho_2 = \emptyset$, ρ_1 is a $2n_1$-cycle, ρ_2 is a $2m$-cycle, $a^\sigma = a^\tau$, and $a^{\sigma\tau\sigma} \in \operatorname{supp}\rho_2$. Let $x, y \notin \operatorname{supp}\sigma \cup \operatorname{supp}\tau$, $\widetilde{\sigma} = \varphi(\sigma; a^\sigma, x, y)$, and $\widetilde{\tau} = \varphi(\tau; a^\tau, y, x)$. Then $\widetilde{\sigma}$ and $\widetilde{\tau}$ are p-cycles, $a^{\widetilde{\sigma}} = a^\sigma = a^\tau = a^{\widetilde{\tau}}$, and by Lemma 2.3, $[\widetilde{\sigma},\widetilde{\tau}] = \varphi(\rho_1\rho_2; a^{\sigma\tau\sigma}, x, y) = \rho_1\varphi(\rho_2; a^{\sigma\tau\sigma}, x, y)$ and $a^{\widetilde{\sigma}\widetilde{\tau}\widetilde{\sigma}} = a^{\sigma\sigma} \in \operatorname{supp}\varphi(\rho_2; a^{\sigma\tau\sigma}, x, y)$. □

Lemma 2.8. *Let σ, τ be permutations and $a, b \in \operatorname{supp}\sigma$ such that $b = a^\sigma = a^\tau$, and $x, y, z \notin \operatorname{supp}\sigma \cup \operatorname{supp}\tau$. Then*

$$[\varphi(\sigma; b, x, y, z), \varphi(\tau; b, y, z)] = [\sigma,\tau](x, y, z).$$

Proof. Let $\widetilde{\sigma} = \varphi(\sigma; b, x, y, z)$ and $\widetilde{\tau} = \varphi(\tau; b, y, z)$. By Corollary 2.2, we have $t^{[\widetilde{\sigma},\widetilde{\tau}]} = t^{[\sigma,\tau]}$ for $t \notin \{b^\sigma, b^{\tau\sigma}, x, y, z\}$. As

$$\begin{aligned}
(b^\sigma)^{[\widetilde{\sigma},\widetilde{\tau}]} &= z^{\widetilde{\tau}^{-1}\widetilde{\sigma}\widetilde{\tau}} = y^{\widetilde{\sigma}\widetilde{\tau}} = z^{\widetilde{\tau}} = b^\tau = (a^\sigma)^\tau = (b^{\tau^{-1}})^{\sigma\tau} = (b^\sigma)^{[\sigma,\tau]},\\
(b^{\tau\sigma})^{[\widetilde{\sigma},\widetilde{\tau}]} &= (b^\tau)^{\widetilde{\tau}^{-1}\widetilde{\sigma}\widetilde{\tau}} = z^{\widetilde{\sigma}\widetilde{\tau}} = b^{\sigma\widetilde{\tau}} = b^{\sigma\tau} = (b^{\tau\sigma})^{[\sigma,\tau]},\\
x^{[\widetilde{\sigma},\widetilde{\tau}]} &= b^{\widetilde{\tau}^{-1}\widetilde{\sigma}\widetilde{\tau}} = a^{\widetilde{\sigma}\widetilde{\tau}} = b^{\widetilde{\tau}} = y,\\
y^{[\widetilde{\sigma},\widetilde{\tau}]} &= x^{\widetilde{\tau}^{-1}\widetilde{\sigma}\widetilde{\tau}} = x^{\widetilde{\sigma}\widetilde{\tau}} = y^{\widetilde{\tau}} = z,\\
z^{[\widetilde{\sigma},\widetilde{\tau}]} &= y^{\widetilde{\tau}^{-1}\widetilde{\sigma}\widetilde{\tau}} = b^{\widetilde{\sigma}\widetilde{\tau}} = x^{\widetilde{\tau}} = x,
\end{aligned}$$

we have $[\widetilde{\sigma},\widetilde{\tau}] = [\sigma,\tau](x, y, z)$. □

Lemma 2.9. *Let $\sigma_1, \sigma_2, \tau_1, \tau_2$ be cycles such that $(\operatorname{supp}\sigma_1 \cup \operatorname{supp}\tau_1) \cap (\operatorname{supp}\sigma_2 \cup \operatorname{supp}\tau_2) = \emptyset$. Suppose there exist $a \in \operatorname{supp}\sigma_1$ and $b \in \operatorname{supp}\sigma_2$ such that $a^{\sigma_1} = a^{\tau_1}$ and $b^{\sigma_2} = b^{\tau_2}$. Then $[\psi(\sigma_1, \sigma_2; a^{\sigma_1}, b^{\sigma_2}), \psi(\tau_1, \tau_2; a^{\tau_1}, b^{\tau_2})] = [\sigma_1, \tau_1][\sigma_2, \tau_2]$.*

Proof. Let $\sigma = \psi(\sigma_1, \sigma_2; a^{\sigma_1}, b^{\sigma_2})$ and $\tau = \psi(\tau_1, \tau_2; a^{\tau_1}, b^{\tau_2})$. Set $c = a^{\sigma_1} = a^{\tau_1}$ and $d = b^{\sigma_2} = b^{\tau_2}$. From Corollary 2.2 and equalities $\sigma = \varphi(\sigma_1; c, b^{\sigma_2^2}, \dots, b, b^{\sigma_2})$ and $\tau = \varphi(\tau_1; c, b^{\tau_2^2}, \dots, b, b^{\tau_2})$, we get $t^{[\sigma,\tau]} = t^{[\sigma_1,\tau_1]} = t^{[\sigma_1,\tau_1][\sigma_2,\tau_2]}$ for $t \notin \{c^{\sigma_1}, c^{\tau_1\sigma_1}\} \cup \operatorname{supp}\sigma_2 \cup \operatorname{supp}\tau_2$. From Corollary 2.2 and equalities $\sigma = \varphi(\sigma_2; d, a^{\sigma_1^2}, \dots, a, a^{\sigma_1})$ and $\tau = \varphi(\tau_2; d, a^{\tau_1^2}, \dots, a, a^{\tau_1})$, we get $t^{[\sigma,\tau]} = t^{[\sigma_2,\tau_2]} = t^{[\sigma_1,\tau_1][\sigma_2,\tau_2]}$ for $t \notin \{d^{\sigma_2}, d^{\tau_2\sigma_1}\} \cup \operatorname{supp}\sigma_2 \cup \operatorname{supp}\tau_2$. Therefore $t^{[\sigma,\tau]} = t^{[\sigma_1,\tau_1][\sigma_2,\tau_2]}$ for $t \notin \{c^{\sigma_1}, c^{\tau_1\sigma_1}, d^{\sigma_2}, d^{\tau_2\sigma_1}\}$. From

$$\begin{aligned}
(c^{\sigma_1})^{[\sigma,\tau]} &= d^{\tau^{-1}\sigma\tau} = b^{\sigma\tau} = d^\tau = c^{\tau_1} = a^{\sigma_1\tau_1} = c^{\tau_1^{-1}\sigma_1\tau_1} = (c^{\sigma_1})^{[\sigma_1,\tau_1]},\\
(c^{\tau_1\sigma_1})^{[\sigma,\tau]} &= (c^{\tau_1})^{\tau^{-1}\sigma\tau} = d^{\sigma\tau} = (c^{\sigma_1})^\tau = c^{\sigma_1\tau_1} = (c^{\tau_1\sigma_1})^{[\sigma_1,\tau_1]},\\
(d^{\sigma_2})^{[\sigma,\tau]} &= c^{\tau^{-1}\sigma\tau} = a^{\sigma\tau} = c^\tau = d^{\tau_2} = b^{\sigma_2\tau_2} = d^{\tau_2^{-1}\sigma_2\tau_2} = (d^{\sigma_2})^{[\sigma_2,\tau_2]},\\
(d^{\tau_2\sigma_2})^{[\sigma,\tau]} &= (d^{\tau_2})^{\tau^{-2}\sigma\tau} = c^{\sigma\tau} = (d^{\sigma_2})^\tau = d^{\sigma_2\tau_2} = (d^{\tau_2\sigma_2})^{[\sigma_2,\tau_2]},
\end{aligned}$$

we get $[\sigma,\tau] = [\sigma_1,\tau_1][\sigma_2,\tau_2]$. □

Theorem 2.10. *Let $\rho \in A_n$. If $n \ge 5$ or ρ is not a 3-cycle then ρ is a commutator of two cycles of A_n.*

Proof. If $\rho = (a_1, a_2, a_3)$ is a 3-cycle then $n \geq 5$ and $\rho = [(a_1, a_3, x), (a_1, a_2, y)]$ for some $x, y \notin \operatorname{supp} \rho$.

Suppose that ρ is not a 3-cycle. We show that there exist cycles σ and τ of odd lengths and $a \in \operatorname{supp} \sigma$ such that $\rho = [\sigma, \tau]$, $\operatorname{supp} \rho = \operatorname{supp} \sigma \cup \operatorname{supp} \tau$, and $a^\sigma = a^\tau$. The proof is by induction on the number of cycles in the cycle decomposition of ρ, which we denote by $c(\rho)$.

If $c(\rho) = 1$, ρ is a cycle of odd length $l \geq 5$. The statement follows from Corollary 2.5.

If $c(\rho) = 2$, then let $\rho = \rho_1\rho_2$, where ρ_1 and ρ_2 are disjoint cycles. The lengths of these cycles are of the same parity. If the lengths are even, the statement follows from Corollary 2.7. In the case of odd lengths, 3 cases are considered.

Case 1: Suppose both lengths are 3. Then $[(a_1, a_2, a_6, a_5, a_3), (a_1, a_2, a_4, a_6, a_5)] = (a_1, a_2, a_3)(a_4, a_5, a_6)$.

Case 2: Suppose exactly one of the lengths is 3. One may assume $\rho_2 = (x, y, z)$ is the 3-cycle. Let ρ_1 be a cycle of length $2l + 1$, where $l \geq 2$. By Corollary 2.5, there exist a $2l$-cycle σ, a $(2l + 1)$-cycle τ, and $a \in \operatorname{supp} \sigma$ such that $\rho_1 = [\sigma, \tau]$, $\operatorname{supp} \rho_1 = \operatorname{supp} \sigma \cup \operatorname{supp} \tau$, and $a^\sigma = a^\tau$. By Lemma 2.8, we have $\rho = [\varphi(\sigma; a^\sigma, x, y, z), \varphi(\tau; a^\tau, y, z)]$, where $\varphi(\sigma; a^\sigma, x, y, z)$ and $\varphi(\tau; a^\tau, y, z)$ are $(2l + 3)$-cycles.

Case 3: Suppose both lengths are greater than 3. Let ρ_i be a cycle of length $2l_i + 1$, $l_i \geq 2$. By Corollary 2.5, there exist $(2l_1 + 1)$-cycles σ_1, τ_1, $(2l_2)$-cycles σ_2, τ_2, $a_1 \in \operatorname{supp} \sigma_1$, and $a_2 \in \operatorname{supp} \sigma_2$ such that $\rho_i = [\sigma_i, \tau_i]$, $\operatorname{supp} \rho_i = \operatorname{supp} \sigma_i \cup \operatorname{supp} \tau_i$, and $a_i^{\sigma_i} = a_i^{\tau_i}$. Then $\psi(\sigma_1, \sigma_2; a_1^{\sigma_1}, a_2^{\sigma_2})$ and $\psi(\tau_1, \tau_2; a_1^{\tau_1}, a_2^{\tau_2})$ are $(2(l_1 + l_2) + 1)$-cycles and by Lemma 2.9, $\rho = [\psi(\sigma_1, \sigma_2; a_1^{\sigma_1}, a_2^{\sigma_2}), \psi(\tau_1, \tau_2; a_1^{\tau_1}, a_2^{\tau_2})]$.

If $c(\rho) \geq 3$, the following 4 cases are considered.

Case 1: Suppose $\rho = \rho_1\rho_2$, where ρ_2 is a $(2l+1)$-cycle, $l \geq 2$, and $\operatorname{supp} \rho_1 \cap \operatorname{supp} \rho_2 = \emptyset$. By Corollary 2.5, there exist $(2l)$-cycles σ_2, τ_2 and $b \in \operatorname{supp} \sigma_2$, such that $\rho_2 = [\sigma_2, \tau_2]$, $\operatorname{supp} \rho_2 = \operatorname{supp} \sigma_2 \cup \operatorname{supp} \tau_2$, and $b^{\sigma_2} = b^{\tau_2}$. Because $2 \leq c(\rho_1) \leq c(\rho) - 1$, the inductive hypothesis yields cycles σ_1, τ_1 of odd lengths, as well as $a \in \operatorname{supp} \sigma_1$, such that $\rho_1 = [\sigma_1, \tau_1]$, $\operatorname{supp} \rho_1 = \operatorname{supp} \sigma_1 \cup \operatorname{supp} \tau_1$, and $a^{\sigma_1} = a^{\tau_1}$. By Lemma 2.9, we have $\rho = [\psi(\sigma_1, \sigma_2; a^{\sigma_1}, b^{\sigma_2}), \psi(\tau_1, \tau_2; a^{\tau_1}, b^{\tau_2})]$, where $\psi(\sigma_1, \sigma_2; a^{\sigma_1}, b^{\sigma_2})$ and $\psi(\tau_1, \tau_2; a^{\tau_1}, b^{\tau_2})$ are cycles of odd lengths.

Case 2: Suppose $\rho = \rho_1\rho_2$, where $\rho_2 = (a_1, a_2, a_3)(a_4, a_5, a_6)$ and $\operatorname{supp} \rho_1 \cap \operatorname{supp} \rho_2 = \emptyset$. If $\rho_1 = (a_7, a_8, a_9)$ then $\rho = [(a_1, a_2, a_7, a_8, a_9, a_4, a_5, a_3, a_6), (a_1, a_2, a_8, a_9, a_5, a_3, a_4)]$. If ρ_1 is not a 3-cycle, the inductive hypothesis yields cycles σ_1, τ_1 of odd lengths, as well as $a \in \operatorname{supp} \sigma_1$, such that $\rho_1 = [\sigma_1, \tau_1]$, $\operatorname{supp} \rho_1 = \operatorname{supp} \sigma_1 \cup \operatorname{supp} \tau_1$, and $a^{\sigma_1} = a^{\tau_1} = b$. Then $\sigma = \varphi(\varphi(\sigma_1; b, a_1, a_2, a_3); b, a_4, a_5, a_6)$ and $\tau = \varphi(\varphi(\tau_1; b, a_2, a_3); b, a_5, a_6)$ are cycles of odd lengths and, using Lemma 2.8 twice, we get $\rho = [\sigma, \tau]$.

Case 3: Suppose $\rho = \rho_1\rho_2$, where ρ_2 is a disjoint product of cycles of lengths $2l_1$ and $2l_2$, such that $l_1 + l_2 \geq 3$, and $\operatorname{supp} \rho_1 \cap \operatorname{supp} \rho_2 = \emptyset$.

If $\rho_1 = (a_1, a_2, a_3)$ then by Corollary 2.7, there exist a $(2(l_1 + l_2) - 2)$-cycle σ_2, a $(2(l_1 + l_2) - 1)$-cycle τ_2, and $a \in \operatorname{supp} \sigma_2$, such that $\rho_2 = [\sigma_2, \tau_2]$, $\operatorname{supp} \rho_2 = \operatorname{supp} \sigma_2 \cup \operatorname{supp} \tau_2$, and $a^{\sigma_2} = a^{\tau_2} = b$. Then $\sigma = \varphi(\sigma_2; b, a_1, a_2, a_3)$ and $\tau = \varphi(\tau_2; b, a_2, a_3)$ are $(2(l_1 + l_2) + 1)$-cycles and by Lemma 2.8, we get $\rho = [\sigma, \tau]$.

If ρ_1 is not a 3-cycle then by the inductive hypothesis there exist cycles σ_1, τ_1 of odd lengths and $a \in \operatorname{supp} \sigma_1$, such that $\rho_1 = [\sigma_1, \tau_1]$, $\operatorname{supp} \rho_1 = \operatorname{supp} \sigma_1 \cup \operatorname{supp} \tau_1$, and $a^{\sigma_1} = a^{\tau_1}$. If $l_1 + l_2 = 3$ then $\rho_2 = (a_1, a_2, a_3, a_4)(a_5, a_6)$ and for $\sigma_2 = (a_1, a_5, a_2, a_4, a_6, a_3)$ and $\tau_2 = (a_1, a_5, a_3, a_4)$ we get $\rho_2 = [\sigma_2, \tau_2]$ and for $b = a_1$ we get $b^{\sigma_1} = b^{\tau_1}$. If $l_1 + l_2 > 3$ Corollary 2.7 provides $(2(l_1 + l_2) - 2)$-cycles σ_2 and τ_2, as well as $b \in \operatorname{supp} \sigma_2$, such that

$\rho_2 = [\sigma_2, \tau_2]$, $\operatorname{supp}\rho_2 = \operatorname{supp}\sigma_2 \cup \operatorname{supp}\tau_2$, and $b^{\sigma_2} = b^{\tau_2}$. Then $\sigma = \psi(\sigma_1, \sigma_2; a^{\sigma_1}, b^{\sigma_2})$ and $\tau = \psi(\tau_1, \tau_2; a^{\tau_1}, b^{\tau_2})$ are cycles of odd length and by Lemma 2.9, we get $\rho = [\sigma, \tau]$.

Case 4: Suppose ρ is a disjoint product of transpositions and at most one 3-cycle. If there are at most four transpositions in the cycle decomposition of ρ we have 3 possibilities:

$$[(a_1,a_3,a_5,a_6,a_2,a_4,a_7),(a_1,a_3,a_6,a_4,a_7,a_2,a_5)] = (a_1,a_2)(a_3,a_4)(a_5,a_6,a_7),$$
$$[(a_1,a_2,a_4,a_8,a_6,a_3,a_5),(a_1,a_2,a_3,a_8,a_4,a_6,a_7)] = (a_1,a_2)(a_3,a_4)(a_5,a_6)(a_7,a_8),$$
$$[(a_1,a_2,a_5,a_3,a_4,a_9,a_{10},a_7,a_{11}),(a_1,a_2,a_6,a_3,a_4,a_{10},a_7,a_9,a_8)] =$$
$$=(a_1,a_2)(a_3,a_4)(a_5,a_6)(a_7,a_8)(a_9,a_{10},a_{11}).$$

Otherwise $\rho = \rho_1\rho_2$, where $\rho_2 = (a_1,a_2)(a_3,a_4)(a_5,a_6)(a_7,a_8)$, $2 \le c(\rho_1) < c(\rho)$, and $\operatorname{supp}\rho_1 \cap \operatorname{supp}\rho_2 = \emptyset$. By the inductive hypothesis there exist cycles σ_1, τ_1 of odd lengths and $a \in \operatorname{supp}\sigma_1$, such that $\rho_1 = [\sigma_1, \tau_1]$, $\operatorname{supp}\rho_1 = \operatorname{supp}\sigma_1 \cup \operatorname{supp}\tau_1$, and $a^{\sigma_1} = a^{\tau_1}$. For $\sigma_2 = (a_1,a_8,a_3,a_2,a_4,a_6,a_7,a_5)$ and $\tau_2 = (a_1,a_8,a_4,a_3,a_5,a_6)$ we have $\rho_2 = [\sigma_2, \tau_2]$. Then $\sigma = \psi(\sigma_1, \sigma_2; a^{\sigma_1}, a_1^{\sigma_2})$ and $\tau = \psi(\tau_1, \tau_2; a^{\tau_1}, a_1^{\tau_2})$ are cycles of odd lengths and by Lemma 2.9, we get $\rho = [\sigma, \tau]$. □

3 Cycles as commutators of cycles

From the previous section we know that a $(2n+1)$-cycle is a commutator of a p-cycle and a q-cycle if $p + q \ge 3n + 2$ (and $p, q \le 2n + 1$). But this sufficient condition is not necessary. Note that in the previous section we were interested in pairs of cycles σ and τ, for which there exists $a \in \operatorname{supp}\sigma$ such that $a^\sigma = a^\tau$. We needed that for "concatenation" of cycles in Lemma 2.9. With that assumption withdrawn, the result is obtained by using a more stringent hypothesis as shown in the next corollary.

Lemma 3.1. *Let σ, τ be permutations, $x, y \notin \operatorname{supp}\sigma \cup \operatorname{supp}\tau$, $a_1, a_2 \in \operatorname{supp}\sigma \cap \operatorname{supp}\tau$, $b \in \operatorname{supp}\sigma - \operatorname{supp}\tau$, and $c \in \operatorname{supp}\tau - \operatorname{supp}\sigma$, such that $a_1^\sigma = b$, $b^\sigma = a_2$, $a_1^\tau = c$, and $c^\tau = a_2$. Then*

$$[\varphi(\sigma; b, c, x), \varphi(\tau; c, y)] = \varphi([\sigma, \tau]; c, y, x).$$

Proof. Let $\widetilde{\sigma} = \varphi(\sigma; b, c, x)$ and $\widetilde{\tau} = \varphi(\tau; c, y)$. If $t \notin \{x, a_2, c\}$ then $t^{\sigma^{-1}} = t^{\widetilde{\sigma}^{-1}}$. If $t \notin \{y, a_2^\sigma\}$ then $t^{\sigma^{-1}} \notin \{y, a_2\}$ and $t^{\sigma^{-1}\tau^{-1}} = t^{\sigma^{-1}\widetilde{\tau}^{-1}}$. If $t \notin \{x, a_2^\sigma, a_2\}$ then $t^{\sigma^{-1}\tau^{-1}} \notin \{x, c, b\}$ and $t^{\sigma^{-1}\tau^{-1}\sigma} = t^{\sigma^{-1}\tau^{-1}\widetilde{\sigma}}$. If $t \notin \{y, a_2^\sigma\}$ then $t^{\sigma^{-1}\tau^{-1}\sigma} \notin \{y, c\}$ and $t^{\sigma^{-1}\tau^{-1}\sigma\tau} = t^{\sigma^{-1}\tau^{-1}\widetilde{\sigma}\widetilde{\tau}}$. Hence for $t \notin \{x, y, c, a_2, a_2^\sigma\}$ we get $t^{[\sigma,\tau]} = t^{[\widetilde{\sigma},\widetilde{\tau}]}$. Because

$$\begin{aligned}
c^{[\sigma,\tau]} &= c^{\tau^{-1}\sigma\tau} = a_1^{\sigma\tau} = b^\tau = b,\\
c^{[\widetilde{\sigma},\widetilde{\tau}]} &= b^{\widetilde{\tau}^{-1}\widetilde{\sigma}\widetilde{\tau}} = b^{\widetilde{\sigma}\widetilde{\tau}} = c^{\widetilde{\tau}} = y,\\
y^{[\widetilde{\sigma},\widetilde{\tau}]} &= y^{\widetilde{\tau}^{-1}\widetilde{\sigma}\widetilde{\tau}} = c^{\widetilde{\sigma}\widetilde{\tau}} = x^{\widetilde{\tau}} = x,\\
x^{[\widetilde{\sigma},\widetilde{\tau}]} &= c^{\widetilde{\tau}^{-1}\widetilde{\sigma}\widetilde{\tau}} = a_1^{\widetilde{\sigma}\widetilde{\tau}} = b^{\widetilde{\tau}} = b,\\
a_2^{[\widetilde{\sigma},\widetilde{\tau}]} &= x^{\widetilde{\tau}^{-1}\widetilde{\sigma}\widetilde{\tau}} = x^{\widetilde{\sigma}\widetilde{\tau}} = a_2^{\widetilde{\tau}} = a_2^\tau = b^{\sigma\tau} = b^{\tau^{-1}\sigma\tau} = a_2^{[\sigma,\tau]},\\
(a_2^\sigma)^{[\widetilde{\sigma},\widetilde{\tau}]} &= a_2^{\widetilde{\tau}^{-1}\widetilde{\sigma}\widetilde{\tau}} = y^{\widetilde{\sigma}\widetilde{\tau}} = y^{\widetilde{\tau}} = a_2 = c^\tau = c^{\sigma\tau} = a_2^{\tau^{-1}\sigma\tau} = (a_2^\sigma)^{[\sigma,\tau]},
\end{aligned}$$

we get $[\widetilde{\sigma}, \widetilde{\tau}] = \varphi([\sigma, \tau]; c, y, x)$. □

Corollary 3.2. *Let ρ be a $(2n+1)$-cycle and $n \geq 2$. For $p, q \in \mathbb{N}$ such that $p, q \leq 2n$ and $p + q = 3n + 1$, there exist a p-cycle σ and a q-cycle τ, such that $[\sigma, \tau] = \rho$ and* $\operatorname{supp}\rho = \operatorname{supp}\sigma \cup \operatorname{supp}\tau$.

Proof. By induction on n we prove that whenever $p, q \leq 2n$ and $p + q = 3n + 1$, there exist a p-cycle σ, a q-cycle τ, $a_1, a_2 \in \operatorname{supp}\sigma \cap \operatorname{supp}\tau$, $b \in \operatorname{supp}\sigma - \operatorname{supp}\tau$, and $c \in \operatorname{supp}\tau - \operatorname{supp}\sigma$, such that $a_1^\sigma = b$, $b^\sigma = a_2$, $a_1^\tau = c$, $c^\tau = a_2$, $[\sigma, \tau]$ is a $(2n+1)$-cycle, and $\operatorname{supp}[\sigma, \tau] = \operatorname{supp}\sigma \cup \operatorname{supp}\tau$.

Because $[\tau, \sigma] = [\sigma, \tau]^{-1}$ we may assume $p \geq q$.

If $n = 2$ then $p = 4$, $q = 3$ and we have $[(a_1, b, a_2, d), (a_1, c, a_2)] = (a_1, c, b, d, a_2)$.

Let $n > 2$. For $p, q \leq 2n$ and $p + q = 3n + 1$ we define $\widetilde{p} = p - 2$ and $\widetilde{q} = q - 1$. Then $\widetilde{p} + \widetilde{q} = 3(n-1) + 1$ and $\widetilde{p} \leq 2(n-1)$. From $q \leq p$ we get $q \neq 2n$ and therefore $\widetilde{q} \leq 2(n-1)$. By the inductive hypothesis there exist a $\widetilde{p}$-cycle $\widetilde{\sigma}$, a $\widetilde{q}$-cycle $\widetilde{\tau}$, $a_1, a_2 \in \operatorname{supp}\widetilde{\sigma} \cap \operatorname{supp}\widetilde{\tau}$, $b \in \operatorname{supp}\widetilde{\sigma} - \operatorname{supp}\widetilde{\tau}$, and $c \in \operatorname{supp}\widetilde{\tau} - \operatorname{supp}\widetilde{\sigma}$, such that $a_1^{\widetilde{\sigma}} = b$, $b^{\widetilde{\sigma}} = a_2$, $a_1^{\widetilde{\tau}} = c$, $c^{\widetilde{\tau}} = a_2$, $[\widetilde{\sigma}, \widetilde{\tau}]$ is a $(2n-1)$-cycle, and $\operatorname{supp}[\widetilde{\sigma}, \widetilde{\tau}] = \operatorname{supp}\widetilde{\sigma} \cup \operatorname{supp}\widetilde{\tau}$. Let $x, y \notin \operatorname{supp}\widetilde{\sigma} \cup \operatorname{supp}\widetilde{\tau}$. Then $\sigma = \varphi(\widetilde{\sigma}; b, c, x)$ is a p-cycle, $\tau = \varphi(\widetilde{\tau}; c, y)$ is a q-cycle, $c, a_2 \in \operatorname{supp}\sigma \cap \operatorname{supp}\tau$, $x \in \operatorname{supp}\sigma - \operatorname{supp}\tau$, $y \in \operatorname{supp}\tau - \operatorname{supp}\sigma$, $c^\sigma = x$, $x^\sigma = a_2$, $c^\tau = y$, $y^\tau = a_2$, and by Lemma 3.1, $[\sigma, \tau]$ is a $(2n+1)$-cycle. □

Let σ and τ be permutations. An equivalence relation on the set $\operatorname{supp}\sigma \cap \operatorname{supp}\tau$ is defined in the following way. Elements $a, b \in \operatorname{supp}\sigma \cap \operatorname{supp}\tau$ are equivalent if and only if there exist $a_0, \ldots, a_n \in \operatorname{supp}\sigma \cap \operatorname{supp}\tau$ and $\rho_1, \ldots, \rho_n \in \{\sigma, \sigma^{-1}, \tau, \tau^{-1}\}$, such that $a = a_0$, $b = a_n$, and $a_i = a_{i-1}^{\rho_i}$ for $i = 1, \ldots, n$. This is obviously an equivalence relation.

Definition 3.3. Permutations σ and τ are **braided** if all elements of $\operatorname{supp}\sigma \cap \operatorname{supp}\tau$ are equivalent to each other.

Lemma 3.4. *Let σ and τ be cycles such that the commutator $[\sigma, \tau]$ is a cycle and* $\operatorname{supp}[\sigma, \tau] = \operatorname{supp}\sigma \cup \operatorname{supp}\tau$. *Then σ and τ are braided.*

Proof. Let $\rho = [\sigma, \tau]$ and $a_0 \in \operatorname{supp}\sigma \cap \operatorname{supp}\tau$. For $n \geq 0$ we inductively define $a_{4n+1} = a_{4n}^{\sigma^{-1}}$, $a_{4n+2} = a_{4n+1}^{\tau^{-1}}$, $a_{4n+3} = a_{4n+2}^{\sigma}$, and $a_{4n+4} = a_{4n+3}^{\tau}$. Let us show that if $a_{4m} = a_0^{\rho^m} \in \operatorname{supp}\sigma \cap \operatorname{supp}\tau$, then a_{4m} is equivalent to a_0. Let $b_1 = a_0$ and $i_1 = \max\{i \mid i \leq 4m, a_i = a_0\}$. For $k \geq 1$ and $i_k < 4m$ we let $i_{k+1} = \max\{i \mid i_k < i \leq 4m, a_i = a_{i_k+1}\}$, $b_{k+1} = a_{i_{k+1}}$, and $\rho_k \in \{\sigma, \sigma^{-1}, \tau, \tau^{-1}\}$, where ρ_k is uniquely defined by $b_k^{\rho_k} = b_{k+1}$. If we show that $b_k \in \operatorname{supp}\sigma \cap \operatorname{supp}\tau$ for all k, then by definition, $a_0 = b_1$ is equivalent to $a_{4m} = b_l$. For $1 \leq k < l$ we have $b_{k+1} \in \operatorname{supp}\rho_k$. Suppose $b_{k+1} \notin \operatorname{supp}\widetilde{\rho}$, where $\widetilde{\rho}$ is the cycle in $\{\sigma, \tau\} - \{\rho_k, \rho_k^{-1}\}$. Because $a_{i_k}^{\rho_k} = a_{i_k+1}$ and $\rho_k \neq \widetilde{\rho}^{\pm 1}$, necessarily also $a_{i_k+1}^{\widetilde{\sigma}} = a_{i_k+2}$ or $a_{i_k+1}^{\widetilde{\sigma}^{-1}} = a_{i_k+2}$. Because $a_{i_k+2}^{\rho_k^{-1}} = a_{i_k+3}$ and $a_{i_k+1} \notin \operatorname{supp}\widetilde{\sigma}$, we get $a_{i_k} = a_{i_k+3}$. This contradicts the definition of i_k. Hence $b_k \in \operatorname{supp}\sigma \cap \operatorname{supp}\tau$.

Let $b \in \operatorname{supp}\sigma \cap \operatorname{supp}\tau$. Because ρ is a cycle and $b \in \operatorname{supp}\rho$, there exists m such that $b = a_0^{\rho^m}$. Thus b is equivalent to a_0, and hence σ and τ are braided. □

Lemma 3.5. *Let σ and τ be permutations such that* $\operatorname{supp}[\sigma, \tau] = \operatorname{supp}\sigma \cup \operatorname{supp}\tau$. *Then* $|\operatorname{supp}\sigma - \operatorname{supp}\tau|, |\operatorname{supp}\tau - \operatorname{supp}\sigma| \leq |\operatorname{supp}\sigma \cap \operatorname{supp}\tau|$.

Proof. Suppose there exist $x, y \in \operatorname{supp}\sigma - \operatorname{supp}\tau$, such that $x = y^\sigma$. Then $x^{[\sigma, \tau]} = x$, and consequently $x \notin \operatorname{supp}[\sigma, \tau]$, which is a contradiction. Hence the map $(\operatorname{supp}\sigma -$

$\operatorname{supp}\tau) \to (\operatorname{supp}\sigma \cap \operatorname{supp}\tau)$, defined by $x \mapsto x^\sigma$, is an injection. Therefore $|\operatorname{supp}\sigma - \operatorname{supp}\tau| \leq |\operatorname{supp}\sigma \cap \operatorname{supp}\tau|$.

Because $\operatorname{supp}[\tau,\sigma] = \operatorname{supp}[\sigma,\tau]$, the other inequality follows from the above paragraph. □

Lemma 3.6. *Let σ and τ be cycles such that $[\sigma,\tau]$ is a cycle and $\operatorname{supp}[\sigma,\tau] = \operatorname{supp}\sigma \cup \operatorname{supp}\tau$. Then $|\operatorname{supp}\sigma - \operatorname{supp}\tau| + |\operatorname{supp}\tau - \operatorname{supp}\sigma| \leq |\operatorname{supp}\sigma \cap \operatorname{supp}\tau| + 1$.*

Proof. Let $k = |\operatorname{supp}\sigma \cap \operatorname{supp}\tau|$, $|\operatorname{supp}\sigma| = k+p$, and $|\operatorname{supp}\tau| = k+q$. If $p = 0$, then by Lemma 3.5 we have

$$|\operatorname{supp}\sigma - \operatorname{supp}\tau| + |\operatorname{supp}\tau - \operatorname{supp}\sigma| = |\operatorname{supp}\tau - \operatorname{supp}\sigma| < |\operatorname{supp}\sigma \cap \operatorname{supp}\tau| + 1.$$

Analogously for $q = 0$. Let $p, q > 0$. Let $\operatorname{supp}\sigma - \operatorname{supp}\tau = \{a_1,\ldots,a_p\}$. Let $m_i \in \mathbb{N} \cup \{0\}$ be the largest number such that $a_i^{\sigma^j} \in \operatorname{supp}\sigma \cap \operatorname{supp}\tau$ for all $j \in \{1,\ldots,m_i\}$. We claim that all m_i are positive. Indeed, suppose that there exist $x, y \in \operatorname{supp}\sigma - \operatorname{supp}\tau$, such that $x^\sigma = y$. Then $y^{[\sigma,\tau]} = y$ which is a contradiction since $\operatorname{supp}\sigma \subset \operatorname{supp}[\sigma,\tau]$. Hence the set $M_i = \{a_i^\sigma,\ldots,a_i^{\sigma^{m_i}}\}$ is nonempty for all i. Because σ is a cycle and $p > 0$, for every $x \in \operatorname{supp}\sigma \cap \operatorname{supp}\tau$ there exists the smallest $i \in \mathbb{N}$ such that $x^{\sigma^{-i}} = a_k$ for some k, which means that $x \in M_k$. Therefore, $(\operatorname{supp}\sigma \cap \operatorname{supp}\tau) = M_1 \coprod \ldots \coprod M_p$. Similarly, $(\operatorname{supp}\sigma \cap \operatorname{supp}\tau) = N_1 \coprod \ldots \coprod N_q$, where $\operatorname{supp}\tau - \operatorname{supp}\sigma = \{b_1,\ldots,b_q\}$, $N_i = \{b_i^\tau,\ldots,b_i^{\tau^{n_i}}\} \subset \operatorname{supp}\tau \cap \operatorname{supp}\sigma$, and $b_i^{\tau^{n_i+1}} \notin \operatorname{supp}\sigma$.

By Lemma 3.4, the cycles σ and τ are braided. Hence there exist $i_2 \in \{2,\ldots,p\}$, $d_2 \in M_1$, $c_2 \in M_{i_2}$, and $\tau_2 \in \{\tau,\tau^{-1}\}$ such that $d_2 = c_2^{\tau_2}$. For $j > 2$ there exist $i_j \in \{2,\ldots,p\} - \{i_2,\ldots,i_{j-1}\}$, $d_j \in M_1 \cup (\cup_{l=2}^{j-1} M_{i_l})$, $c_j \in M_{i_j}$, and $\tau_j \in \{\tau,\tau^{-1}\}$ such that $d_j = c_j^{\tau_j}$. Let us show that for each i, the set $\widetilde{N}_i = N_i - \{c_2,\ldots,c_p\}$ is nonempty. By construction, the elements $c_2,\ldots,c_p$ are different, $d_j \neq c_k$ for $j \leq k$, and every pair $\{c_j, d_j\}$ is a subset of N_l for some l. Suppose $N_i \cap \{c_2,\ldots,c_p\} = \{c_{k_1},\ldots,c_{k_r}\}$, where $k_1 < \ldots < k_r$. Then $d_{k_1} \in N_i$ and $d_{k_1} \notin \{c_{k_1},\ldots,c_{k_r}\}$, so $d_{k_1} \in \widetilde{N}_i \neq \emptyset$. Hence in the union of the q nonempty sets $\widetilde{N}_1,\ldots,\widetilde{N}_q$ there are exactly $k-(p-1)$ elements. This means that $|\operatorname{supp}\tau - \operatorname{supp}\sigma| = q \leq k-(p-1) = |\operatorname{supp}\sigma \cap \operatorname{supp}\tau| - |\operatorname{supp}\sigma - \operatorname{supp}\tau| + 1$. □

Theorem 3.7. *Let $n \geq 2$ and let ρ be a $(2n+1)$-cycle. There exist a p-cycle σ and a q-cycle τ such that $\rho = [\sigma,\tau]$ and $\operatorname{supp}\rho = \operatorname{supp}\sigma \cup \operatorname{supp}\tau$ if and only if the following three conditions are satisfied (i) $n+1 \leq p, q$, (ii) $2n+1 \geq p, q$, (iii) $p+q \geq 3n+1$.*

Proof. Suppose there exist a p-cycle σ and a q-cycle τ such that $\rho = [\sigma,\tau]$ and $\operatorname{supp}\rho = \operatorname{supp}\sigma \cup \operatorname{supp}\tau$. Let $k = |\operatorname{supp}\sigma \cap \operatorname{supp}\tau|$, $p = k + \widetilde{p}$, and $q = k + \widetilde{q}$. By Lemma 3.5, we have $\widetilde{q} \leq k$, therefore $2\widetilde{q} \leq k + \widetilde{q} = q \leq 2n+1$ which implies $\widetilde{q} \leq n$. Then $2n+1 = |\operatorname{supp}\rho| = |\operatorname{supp}\sigma \cup \operatorname{supp}\tau| = p + \widetilde{q} \leq p + n$, hence $n+1 \leq p$. By Lemma 3.6, we have $\widetilde{p} + \widetilde{q} \leq k+1$. Therefore $2n+1 = k + \widetilde{p} + \widetilde{q} \leq 2k+1$ and $p+q = 2n+1+k \geq 3n+1$.

If $p+q \geq 3n+2$ the theorem follows from Corollary 2.5. If $p+q = 3n+1$, the theorem follows from Corollary 3.2. □

References

[1] E. Bertram, Even permutations as a product of two conjugate cycles, *J. Combin. Theory* **12** (1972), 368–380.

[2] O. Bonten, *Über Kommutatoren in endlichen einfachen Gruppen*, Aachener Beiträge zur Math. **7**, Verlag der Augustinus-Buchhandlung, Aachen, 1993.

[3] E. W. Ellers, N. Gordeev, On the conjectures of J. Thompson and O. Ore, *Trans. Amer. Math. Soc.* **350** (1998), no. 9, 3657–3671.

[4] R. Gow, Commutators in the symplectic group, *Arch. Math. (Basel)* **50** (1988), no. 3, 204–209.

[5] L. C. Kappe, R. S. Morse, *On commutators in groups*, Groups St. Andrews 2005. Vol. 2, 531–558, *London Math. Soc. Lecture Note Ser.*, 340, Cambridge Univ. Press, Cambridge, 2007.

[6] M. W. Liebeck, E. A. O'Brien, A. Shalev, P. H. Tiep, The Ore conjecture, *J. Eur. Math. Soc. (JEMS)* **12** (2010), no. 4, 939–1008.

[7] G. A. Miller, On the commutators of a given group, *Bull. Amer. Math. Soc.* **6** (1899) 105–109.

[8] J. Neubüser, H. Pahlings, E. Cleuvers, Each sporadic finasig G has a class C such that $CC = G$, *Abstracts Amer. Math. Soc.* **34**, 6 (1984).

[9] O. Ore, Some remarks on commutators, *Proc. Amer. Math. Soc.* **272** (1951), 307–314.

[10] R. C. Thompson, Commutators in the special and general linear groups, *Trans. Amer. Math. Soc.* **101** (1961), 16–33.

[11] R. C. Thompson, Commutators of matrices with coefficients from the field of two elements, *Duke Math. J.* **29** (1962), 367–373.

[12] R. C. Thompson, On matrix commutators, *Portugal. Math.* **21** (1962), 143–153.