EXTRACTA MATHEMATICAE Vol. **30**, Núm. 2, 251 – 262 (2015)

Powers in Alternating Simple Groups [*]

J. Martínez Carracedo

Departamento de Matemáticas, Universidad de Oviedo
c/ Calvo Sotelo, s/n, 33007 Oviedo, Spain
martinezjorge@uniovi.es

Presented by Consuelo Martínez Received July 17, 2015

Abstract: C. Martínez and E. Zelmanov proved in [12] that for every natural number d and every finite simple group G, there exists a function $N = N(d)$ such that either $G^d = 1$ or $G = \{a_1^d \cdots a_N^d \,:\, a_i \in G\}$. In a more general context the problem of finding words ω such that the word map $(g_1, \dots, g_d) \longrightarrow \omega(g_1, \dots, g_d)$ is surjective for any finite non abelian simple group is a major challenge in Group Theory. In [8] authors give the first example of a word map which is surjective on all finite non-abelian simple groups, the commutator $[x, y]$ (Ore Conjecture). In [11] the conjecture that this is also the case for the word x^2y^2 is formulated. This conjecture was solved in [9] and, independently, in [6], using deep results of algebraic simple groups and representation theory. An elementary proof of this result for alternating simple groups is presented here.

Key words: Alternating groups, simple groups, power subgroups, word maps.

AMS *Subject Class.* (2010): 20D06, 20B35.

1. Introduction

In any group G, G^d the subgroup generated by d-th powers of elements in G and G' are normal subgroups. So, if G is a finite non-abelian simple group it is clear that $G = G'$ and if d is not divisible by $\exp(G)$, then $G = G^d$. So, every element of G can be expressed both, as a product of a finite number of commutators in G and as a product of finitely many p-th powers in G. But the existence of a bound for the number of factors in any element of G has important consequences, for instance in profinite groups.

In 1996, C. Martínez and E. Zelmanov [12] proved that for a natural number $d \geq 1$, there exists a function $N(d)$ such that for an arbitrary simple group G either $G^d = 1$ or $G = \{a_1^d \cdots a_N^d \,:\, a_i \in G\}$.

In particular, for alternating groups A_n, $n \geq 5$, Martínez and Zelmanov used a result by Bertran that says that any even permutation in A_n can

[*] This work was partially supported by BES-2011-044790 (research fellowship associated to project MTM2010-18370-C04-01).

be written as a product of two cycles, each one of length l, if and only if, $[3n/4] \leq l \leq n$.

Clearly, it seems that the bound depends on d. For instance, if $d = 2$ every element in A_n, $n \geq 5$, is a product of two squares in A_n. However, if $d = 210$, it is impossible to write every 7-cycle in A_7 as a product of two 210-th powers in A_7. But, for every natural number $m' < 210$, it can be proved that every element in A_7 can be written as a product of two m'-th powers.

Still, it is natural to ask if we can find a general constant N such that every element in an alternating group A_n, $n \geq 5$, can be written as a product of N d-th powers of elements in A_n. In this paper it is proved that this is the case for $d = p^r$, where p is a prime number and r is a natural number. And in this case, $N = 2$.

These ideas can be reformulated in an slightly different way. Given an arbitrary group G and a word in the free group of rank r, $\omega \in \mathbb{F}_r$, with r a natural number, we can consider the word map $\omega : G \times \overset{r}{\cdots} \times \ G \longrightarrow G$ that maps each tuple $(g_1, g_2, \dots, g_r)$ to $\omega(g_1, g_2, \dots, g_r)$. It has sense to ask if this word map is surjective.

Of course, there are words for which $\omega(G) \neq G$. For example, the word x^2 is not surjective on any finite non abelian simple group. Nevertheless, some word maps are surjective, and it is an interesting problem in Group Theory to determine which ones are.

The first non-trivial example of a word map which is surjective on all finite non-abelian simple groups is the commutator map $[x, y]$. It was proved in [8], giving a positive answer to a conjecture formulated by Ore, who had proved in 1951 [13] the result for alternating groups.

In [11] authors proved in the same article that every element of a sufficiently large finite simple group is a product of two squares and posed the conjecture that the word x^2y^2 is surjective. This conjecture was proved in [9], where authors also proved that if $p > 7$ is a prime number, then any element of a finite non-abelian simple group G is a product of two p-th powers.

At the same time, R. Guralnick and G. Mall got a new proof using some results about conjugacy classes. In [6], they proved that there always exist two conjugacy classes in a finite non abelian simple group such that every non trivial element of the group belongs to the product of these conjugacy classes. This result is used to prove that every element in a finite non abelian simple group can be written as a product of two p^k-th powers, with p a primer number.

We must emphasize that the proof of all these results is highly nontrivial.

Our aim here is to show a proof of the mentioned result for alternating groups A_n, $n \geq 5$, that uses only elementary techniques.

Let's mention an elementary fact that will be extensively used in what follows. Given a group G and a natural number $n \geq 1$, the mapping

$$\begin{aligned} \varphi_n : G &\longrightarrow G \\ g &\longmapsto g^n \end{aligned}$$

is bijective if an only if the greatest common divisor $gcd(n, \exp(G)) = 1$.

Indeed, if we take a prime divisor p of $\exp(G)$ and n, there exists an element in $g \in G$ of order p. So $\varphi(g) = \varphi(1) = 1$.

The next elementary result will very useful in this paper.

Theorem 1.1. *If G is a finite group, g is an element of G and $d \geq 1$ is an integer such that $\gcd(o(g), d) = 1$, then $g = (g^s)^d$ for some integer $s \geq 1$.*

Proof. It suffices to consider the cycle group $\langle g \rangle$. As the $\gcd(o(g), d) = 1$, we can apply the Bezout's Identity to get that there exist $t, s \in \mathbb{Z}$ such that $1 = o(g)t + sd$.

Then we have that

$$g = g^{o(g)t+sd} = g^{o(g)t} g^{sd} = (g^s)^d.$$

∎

In order to address our problem and study p^k-th powers in A_n, we will distinguish 3 different cases: $p = 2$, $p = 3$ and $p > 3$.

Before starting, we want to give an elementary definition.

Definition 1.2. Let σ be a permutation of a symmetric group S_n, $n \geq 1$. The support of σ is defined as

$$\operatorname{supp}(\sigma) = \big\{ i \in \{1, \ldots, n\} \,:\, \sigma(i) \neq i \big\}.$$

The following results will be an essential tool in the paper.

Lemma 1.3. *Let m be a positive integer and $n \geq 5$. Take $\sigma_1, \ldots, \sigma_k$ permutations in A_n such that $\sigma_i = \lambda_i^m$ for some $\lambda_i \in A_n$. If $\operatorname{supp}(\sigma_i) \cap \operatorname{supp}(\sigma_j) = \emptyset$ for every $i \neq j$, then there exists $\lambda \in A_n$, such that $\sigma_1 \cdots \sigma_k = \lambda^m$ and*

$$\operatorname{supp}(\lambda) = \bigcup_{i=1}^{k} \operatorname{supp}(\sigma_i)\,.$$

Proof. For each $i \in \{1, \ldots, k\}$, we have that there exists $\lambda_i \in A_n$ such that $\sigma_i = \lambda_i^m$.

We can assume, without loss of generality that $\mathrm{supp}(\lambda_i) = \mathrm{supp}(\sigma_i)$, and so, the supports of λ_i and λ_j are disjoint for every $i \neq j$ and we have that λ_i commutes with λ_j for every $i \neq j$.

Then, we have that

$$\prod_{i=1}^{k} \sigma_i = \prod_{i=1}^{k} (\lambda_i)^m = \left(\prod_{i=1}^{k} \lambda_i \right)^m .$$

It is enough to take $\lambda = \prod_{i=1}^{k} \lambda_i$.

Let us notice that $\mathrm{supp}(\lambda) = \bigcup_{i=1}^{k} \mathrm{supp}(\sigma_i)$. ∎

Theorem 1.4. *Let $\sigma_1, \ldots, \sigma_t$ permutations in A_n such that $\sigma_i = \lambda_{i1}^d \cdots \lambda_{iN}^d$ for some $N, d \geq 1$. If σ_i and σ_j are disjoint when $i \neq j$ and $\mathrm{supp}(\sigma_i) = \bigcup_{j=1}^{N} \mathrm{supp}(\lambda_{ij})$, then there exist permutations $\lambda_1, \ldots, \lambda_N$ such that*

$$\sigma_1 \cdots \sigma_t = \lambda_1^d \cdots \lambda_N^d .$$

Proof. It suffices to take $\lambda_1 = \lambda_{11} \cdots \lambda_{t1}, \ldots,\ \lambda_N = \lambda_{1N} \cdots \lambda_{tN}$ and take into account that λ_{ij} commutes with λ_{hl} if $i \neq h$. Then, we can use Lemma 1.3 to get the result.

Notice that again $\bigcup_{i=1}^{N} \mathrm{supp}(\lambda_i) = \bigcup_{j=1}^{t} \mathrm{supp}(\sigma_j)$. ∎

In this paper n will be an integer greater than or equal to 5 and k will be an integer greater than or equal to 1.

The main result of this paper is the next theorem.

Theorem 1.5. *Let p be a prime number. Every element in an alternating group A_n can be written as a product of two p^k-th powers in A_n.*

2. The case $p = 2$

We will start with the case of $p = 2$. We will consider first those permutations of A_n that can be written as products of cycles of odd length.

Lemma 2.1. *Let σ be a permutation that can be written as a product of disjoint cycles of odd length. Then there exists λ in A_n such that $\sigma = \lambda^{2^k}$.*

Proof. Suppose that $\sigma = (a_1, \ldots, a_k)$ is a cycle of length odd, $k \geq 3$.

Since $\gcd(2, o(\sigma)) = 1$, we can apply Lemma 1.1 to get that $\sigma = (\sigma^s)^{2^k}$ for some $s \geq 1$. Clearly, $\mathrm{supp}(\sigma) = \mathrm{supp}(\sigma^s)$. ▮

Lemma 2.2. *Let σ be a permutation in A_n that can be written as a product of an even number of disjoint cycles of even length. Then there exist μ, η in A_n such that $\sigma = \mu^{2^k}\eta^{2^k}$.*

Proof. Suppose initially that $\sigma = (a_1, \ldots, a_{2i})(a_{2i+1}, \ldots, a_{2r})$ is a permutation in A_n that is a product of two cycles of even length. It is enough to rewrite σ as $\sigma = \xi_1\eta_1$, where $\xi_1 = (a_1, a_2, \ldots, a_{2i+1})$ and $\eta_1 = (a_{2i}, a_{2i+1}, \ldots, a_{2r})$.

By Lemma 2.1 there exist elements ξ and η in A_n such that $\xi_1 = \xi^{2^k}$, $\eta_1 = \eta^{2^k}$. So

$$\sigma = \xi^{2^k}\eta^{2^k}.$$

Notice that we can always assume that $\mathrm{supp}(\xi) \cup \mathrm{supp}(\eta) \subset \mathrm{supp}(\sigma)$.

Lemma 2.2 is now a direct consequence of Lemma 2.1. ▮

Since every even permutation σ in A_n can be written as a product of two disjoint permutations $\sigma = \sigma_1\sigma_2$, where σ_1 satisfies the assumptions of Lemma 2.1 and σ_2 satisfies the assumptions of Lemma 2.2, a direct application of Theorem 1.4 gives Theorem 1.5 in the case $p = 2$.

3. The case $p \geq 5$

In this section we will address the case $p \geq 5$. We will start considering cycles of odd length.

Lemma 3.1. *Let σ be a permutation in A_n that can be written as a product of disjoint cycles of odd length, then there exist λ and μ in A_n such that $\sigma = \lambda^{p^k}\mu^{p^k}$.*

Proof. Let's consider first the case in which σ is a single cycle. Suppose that $\sigma = (a_1, \ldots, a_r)$, with $r \geq 3$ odd. We will distinguish two different cases:

(i) If p is not a divisor of $o(\sigma)$, the result follows from Lemma 2.1, since $\sigma = (\sigma^s)^{p^k}$ for some integer s.

(ii) If p is a divisor of $o(\sigma)$, then we can rewrite σ as

$$\sigma = (a_1, a_2, a_3)(a_3, a_4, \ldots, a_r)$$

as a product of a 3-cycle and a $(r-2)$-cycle.

But p does not divide neither to 3 nor to $(r-2)$. So, using the previous case, there exist α and β elements in A_n such that

$$(a_1, a_2, a_3) = \alpha^{p^k} \qquad \text{and} \qquad (a_3, \ldots, a_r) = \beta^{p^k}.$$

So

$$\sigma = (a_1, a_2, a_3)(a_3, a_4, \ldots, a_r) = \alpha^{p^k} \beta^{p^k}.$$

Notice that $\operatorname{supp}(\alpha) \cup \operatorname{supp}(\beta) \subset \operatorname{supp}(\sigma)$

Theorem 1.4 immediately extends the previous result to permutations that are product of disjoint cycles of odd length. ▮

Now, let's consider products of disjoint cycles of even length.

Lemma 3.2. *Let σ be a permutation in A_n that is a product of an even number of disjoint cycles of even length. Then σ can be written as a product of two p^k-th powers in $A_{\operatorname{supp}(\sigma)}$.*

Proof. To start, consider $\sigma = \sigma_1 \sigma_2$ a permutation in A_n, where $\sigma_1 = (a_1, \ldots, a_{2i})$ and $\sigma_2 = (a_{2i+1}, \ldots, a_{2r})$. We will consider two different cases:

(i) If p is not a divisor of $o(\sigma)$, by Lemma 1.1, we have that $\sigma = (\sigma^s)^{p^k}$ for some $s \geq 1$.

(ii) If p is a divisor of $o(\sigma)$, let's distinguish two different cases:

(a) If p divides both $o(\sigma_1)$ and $o(\sigma_2)$, then we can rewrite σ as follows:

$$\sigma = (a_1, a_2)(a_{2i+1}, a_{2i+2})(a_2, \ldots, a_{2i})(a_{2i+2}, \ldots, a_{2r}).$$

Denoting $(a_1, a_2)(a_{2i+1}, a_{2i+2}) = \lambda_1$ and $(a_2, \ldots, a_{2i})(a_{2i+2}, \ldots, a_{2r}) = \lambda_2$, it is clear that $\lambda_1 = \lambda_1^{p^k}$ because of $o(\lambda_1) = 2$.

On the other hand, we have that p is neither a divisor of $o(\sigma_1) - 1$ nor of $o(\sigma_2) - 1$. So, by Lema 1.1, we have that λ_2 is a p^k-th power in A_n.

That is, there exist permutations λ and μ in A_n such that $\lambda_1 = \lambda^{p^k}$, $\lambda_2 = \mu^{p^k}$. So

$$\sigma = \lambda^{p^k} \mu^{p^k}.$$

(b) Suppose that p is a divisor of $o(\sigma_2)$ and not of $o(\sigma_1)$ (the case $p \mid o(\sigma_1)$ and $p \dagger o(\sigma_2)$ is similar). We can rewrite σ as

$$\sigma = \sigma_1(a_{2i+1}, a_{2i+2})(a_{2i+2}, \dots, a_{2r})\,.$$

Denoting $\lambda_1 = \sigma_1(a_{2i+1}, a_{2i+2})$ and $\lambda_2 = (a_{2i+2}, \dots, a_{2r})$, we have that p is not a divisor of $o(\lambda_1)$ and that p is not a divisor of $o(\lambda_2) = o(\sigma_2) - 1$.

So, applying Lemma 1.1 to λ_1 and to λ_2 we have that there exist λ and μ permutations in A_n such that $\lambda_1 = \lambda^{p^k}$, $\lambda_2 = \mu^{p^k}$.

So, we have that

$$\sigma = (\lambda)^{p^k}(\mu)^{p^k}.$$

∎

Since every even permutation σ in A_n can be written as a product of two disjoint permutations $\sigma = \sigma_1\sigma_2$, where σ_1 satisfies the assumptions of Lemma 3.1 and σ_2 satisfies the assumptions of Lemma 3.2, a direct application of Theorem 1.4 gives Theorem 1.5 in the case $p \geq 5$.

4. The case $p = 3$

We will prove that for every natural number $k \geq 1$, every element in A_n, can be written as a product of two 3^k-th powers.

Let's start with the study of cycles of odd length.

Lemma 4.1. *Every cycle σ in A_n with odd length $s \geq 3$ can be written as a product of two 3^k-th powers in A_n*

Proof. Take $\sigma = (a_1, \dots, a_s)$, with $s \geq 3$ odd. We distinguish three different cases:

(i) If 3 does not divide to $o(\sigma)$ we can apply Lemma 1.1 to get that $\sigma = (\sigma^t)^{3^k}$ for some $t \geq 1$.

(ii) If $3 \mid o(\sigma) = s$ and $s \geq 9$, we can rewrite σ as a product of two cycles

$$\sigma := (a_1, \dots, a_5)(a_5, \dots, a_s)\,,$$

one of length 5 and the other one of length $s - 4$. Clearly 3 does not divide $s - 4$. Denoting $\lambda_1 = (a_1, \dots, a_5)$ and $\lambda_2 = (a_5, \dots, a_s)$, we have that $\lambda_1 = (\lambda_1^r)^{3^k}$ and $\lambda_2 = (\lambda_2^t)^{3^k}$ for some $r, t \geq 1$. So,

$$\sigma = (\lambda_1^r)^{3^k}(\lambda_2^t)^{3^k}.$$

Notice that $\lambda_1, \lambda_2 \in A_{\mathrm{supp}(\sigma)}$.

(iii) Suppose $s = 3$. Assume $\sigma = (a_1, a_2, a_3)$ and take the permutation $x := (a_1, a_5, a_3, a_4, a_2)$ and $y := (a_1, a_3, a_5, a_2, a_4)$ in A_n (remember that $n \geq 5$). Then we have that $\sigma = yx$, and, by the first case, there exist λ_1 and λ_2 in A_n such that $x = \lambda_1^{3^k}$ and $y = \lambda_2^{3^k}$, that is

$$\sigma = \lambda_2^{3^k} \lambda_1^{3^k}.$$

∎

Remark. If σ is a 3-cycle, $A_{\mathrm{supp}(\sigma)} \simeq A_3 \leq A_4$, it is impossible to write σ as a product of two 3^k-th powers neither in A_3 nor A_4.

Indeed, A_3 is an abelian group of order 3 and $A_4^3 = V$, where V is the 4-Klein group that consists of the identity and all products of two disjoint transpositions.

We will need, at least, 5 symbols to write a 3-cycle as a product of two 3^k-powers, for every $k \geq 1$. That's why we have to be careful when using Lemma 1.3, in case that a 3-cycle is involved in a permutation σ.

The problem does not appear if only cycles of odd length greater than or equal to 5 appear.

Corollary 4.2. *Let σ be a permutation in A_n that can be written as a product of disjoint cycles of odd length greater than 3. Then there exist λ and μ in A_n such that $\sigma = \lambda^{3^k} \mu^{3^k}$.*

Lemma 4.3. *Let σ be a permutation in A_n that is a product of r disjoint 3-cycles, $r \geq 2$. Then there exist λ and μ in $A_{\mathrm{supp}\,(\sigma)}$ such that $\sigma = \lambda^{3^k} \mu^{3^k}$.*

Proof. Suppose $\sigma = \sigma_1 \cdots \sigma_r$, such that σ_i is a 3-cycle for every $i \in \{1, \ldots, r\}$, $r \geq 2$ and σ_i, σ_j disjoint if $i \neq j$.

(i) If $r = 2$, suppose that

$$\sigma = (a_1, a_2, a_3)(a_4, a_5, a_6).$$

Then σ can be rewritten as

$$\sigma = \xi_1 \xi_2,$$

where $\xi_1 = (a_1, a_2)(a_4, a_5)$ and $\xi_2 = (a_2, a_3)(a_5, a_6)$.

Since $o(\xi_1) = 2 = o(\xi_2)$ it follows from Lemma 1.1 that

$$\sigma = (\xi_1^{s_1})^{3^k}(\xi_2^{s_2})^{3^k}.$$

Notice that $\xi_1, \xi_2 \in A_{\mathrm{supp}(\sigma)}$.

(ii) For r even, the result follows immediately from Theorem 1.4 and the case $r = 2$.

(iii) If $r = 3$,

$$\sigma = (a_1, a_2, a_3)(a_4, a_5, a_6)(a_7, a_8, a_9)\,.$$

Now, we can rewrite $\sigma = \lambda_1\lambda_2$, with $\lambda_1 = (a_1, a_6, a_9, a_5, a_8, a_2, a_3)$ and $\lambda_2 = (a_1, a_8, a_6, a_4, a_9, a_7, a_5)$. Since $o(\lambda_1) = 7 = o(\lambda_2)$, by Lemma 1.1 $\lambda_1 = (\lambda_1^{l_1})^{3^k}$ and $\lambda_2 = (\lambda_2^{l_2})^{3^k}$. So

$$\sigma = (\lambda_1^{l_1})^{3^k}(\lambda_2^{l_2})^{3^k}.$$

Notice that $\lambda_1, \lambda_2 \in A_{\mathrm{supp}(\sigma)}$.

(iv) If r is odd, $r \geq 5$, then we can consider the product of the first three 3-cycles and the rest of the 3-cycles in pairs. Now the result for σ follows immediately from Theorem 1.4 and the previous cases.

∎

Lemma 4.4. *Let σ be a permutation that is a product of disjoint cycles of odd length.Then there exist λ and μ in A_n such that $\sigma = \lambda^{3^k}\mu^{3^k}$.*

Proof. If at least two 3-cycles appear, it follows from Theorem 1.4, Lemma 4.1 and Lemma 4.3. So let us assume that only one 3-cycle appears, in the expression of σ as product of cycles of odd length.

Let's write $\sigma = \sigma_1\alpha_1 \cdots \alpha_r$, with $\sigma_1 = (a_1, a_2, a_3)$ a 3-cycle and α_i a cycle of odd length greater than 3 for every $i \in \{1, \ldots, r\}$.

We can apply Lemma 4.1 and Theorem 1.4 to $\alpha_2 \cdots \alpha_r$ to get that there exist β, γ in A_n such that $\mathrm{supp}(\beta, \gamma) \subset \bigcup_{i=2}^{r} \mathrm{supp}(\alpha_i)$ such that

$$\alpha_2 \cdots \alpha_r = \beta^{3^k}\gamma^{3^k}.$$

Consider now $\sigma_1\alpha_1 = (a_1, a_2, a_3)(a_4, a_5, \ldots, a_s)$, with $s \geq 8$ even. We distinguish two cases:

(i) If 3 does not divide to $s-4$, we can rewrite $\sigma_1\alpha_1$ as follows:

$$\sigma_1\alpha_1 = (a_1, a_2)(a_4, a_5)(a_2, a_3)(a_5, \dots, a_s)\,.$$

If we denote $\lambda_1 = (a_1, a_2)(a_4, a_5)$ and $\lambda_2 = (a_2, a_3)(a_5, \dots, a_s)$, we have that 3 does not divide neither to $o(\lambda_1) = 2$ nor to $o(\lambda_2) = s-4$. By Lemma 1.1, $\lambda_1 = (\lambda_1^{m_1})^{3^k}$ and $\lambda_2 = (\lambda_2^{m_2})^{3^k}$, for some $m_1, m_2 \geq 1$. So, we have that

$$\sigma_1\alpha_1 = \lambda_1\lambda_2 = (\lambda_1^{m_1})^{3^k}(\lambda_2^{m_2})^{3^k}.$$

(ii) If 3 is a divisor of $s-4$, we can rewrite $\sigma_1\alpha_1$ as follows:

$$\sigma_1\alpha_1 = \lambda_1\lambda_2\,,$$

where $\lambda_1 = (a_1, a_2, a_3, a_4, a_5)$ and $\lambda_2 = (a_3, a_5, a_6, \dots, a_s)$. Then 3 does not divide neither to $o(\lambda_1) = 5$ nor to $o(\lambda_2) = (s-3)$.

Again by Lemma 1.1 we get that $\lambda_1 = (\lambda_1^{n_1})^{3^k}$ and that $\lambda_2 = (\lambda_2^{n_2})^{3^k}$, for some $n_1, n_2 \geq 1$. Consequently

$$\sigma_1\alpha_1 = \lambda_1\lambda_2 = (\lambda_1^{m_1})^{3^k}(\lambda_2^{m_2})^{3^k}.$$

Theorem 1.4 finishes the proof of this lemma. ∎

It remains to consider products of cycles of even length.

Lemma 4.5. *Let σ be a permutation in A_n that is a product of an even number of disjoint cycles of even length. Then there exist μ, η in A_n such that $\sigma = \mu^{3^k}\eta^{3^k}$.*

Proof. The proof follows the same lines of the proof of Lemma 3.2. ∎

If σ is a permutation in A_n, we can write it as

$$\sigma = \sigma_1 \cdots \sigma_r \gamma_1 \cdots \gamma_s (\alpha_1\alpha_2) \cdots (\alpha_{2l-1}\alpha_{2l})\,,$$

where each σ_i is a 3-cycle, $i \in \{1, \dots, 2r\}$, γ_j is a cycle of odd length greater or equal than 5, $j \in \{1, \dots, s\}$, and α_k is a cycle of even length for every k, $k \in \{1, \dots, 2l\}$.

Theorem 1.5 follows from Theorem 1.4 together with Lemma 4.3 and Lemma 4.4 except in the case $s = 0$, $r = 1$ and $l \geq 1$. Notice that in this case σ_1 is a product of two 3^k-powers, but we need to involve two symbols that do not appear in $\operatorname{supp}(\sigma_1)$, so Theorem 1.4 can not be directly applied.

To finish the result we only need the following lemma.

Lemma 4.6. *Let σ be a permutation in A_n that is a product of a single 3-cycle and two disjoint cycles of even length. Then there exist μ, η in A_n such that $\sigma = \mu^{3^k}\eta^{3^k}$.*

Proof. Suppose that σ can be written as follows:

$$\sigma = \sigma_1(\alpha_1\alpha_2)\,,$$

with $\sigma_1 = (a_1, a_2, a_3)$ a 3-cycle and α_1, α_2 are cycles of even length, $\alpha_1 = (b_1, \dots, b_{2i})$, $\alpha_2 = (b_{2i+1}, \dots, b_{2t})$.

We distinguish four different cases:

(i) If 3 divides to both $o(\alpha_1)$ and $o(\alpha_2)$, or equivalently $3 \mid i$ and $3 \mid t$, we rewrite σ as $\sigma = \lambda_1\lambda_2$, where $\lambda_1 = (a_1, a_2)(b_1, b_2)(b_{2i+1}, \dots, b_{2t-1})$ and $\lambda_2 = (a_2, a_3)(b_{2t-1}, b_{2t})(b_2, \dots, b_{2i})$.

But 3 does not divide neither to $o(\lambda_1) = 2(2(t-i)-1)$ nor to $o(\lambda_2) = 2(2i-1)$. So Lemma 1.1 gives the result, since $\lambda_1 = (\lambda_1^p)^{3^k}$ and $\lambda_2 = (\lambda_2^q)^{3^k}$, for some $p, q \in \mathbb{Z}$.

(ii) If 3 divides to $o(\alpha_1)$ but does not divide to $o(\alpha_2)$, that is $3 \mid i$, but $3 \dagger t$, we rewrite σ as follows:

$$\sigma = \lambda_1\lambda_2\,,$$

where $\lambda_1 = (a_1, a_2, a_3, b_1)(b_{2i+1}, \dots, b_{2t})$ and $\lambda_2 = (a_3, b_1, b_2, \dots, b_{2i})$.

Now, 3 does not divide to $(2i+1) = o(\lambda_2)$, so we can apply Lemma 1.1.

Similarly, 3 does not divide to $4(t-i) = o(\lambda_1)$. we can use again Lemma 1.1. So,

$$\sigma = (\lambda_1^v)^{3^k}(\lambda_2^u)^{3^k},$$

for some integers u, v.

(iii) If 3 divides to $o(\alpha_2)$ but 3 does not divide to $o(\alpha_1)$, the proof is similar.

(iv) If 3 does not divide neither to $o(\alpha_2)$ nor to $o(\alpha_1)$, we rewrite σ as follows

$$\sigma = (a_1, a_2, a_3, b_1, b_2)(a_3, b_2, \dots, b_{2i})(b_{2i+1}, \dots, b_{2t})\,.$$

Denote $\lambda_1 = (a_1, a_2, a_3, b_1, b_2)$ and $\lambda_2 = (a_3, b_2, \dots, b_{2i})(b_{2i+1}, \dots, b_{2t})$. Since 3 does not divide to $o(\lambda_1) = 5$ and 3 does not divide to $o(\lambda_2) = \mathrm{mcm}(2i, 2t-2i)$, the result follows immediately from Lemma 1.1.

This finishes the proof of Lemma 4.6 and gives Theorem 1.5 in the case $p = 3$.

∎

References

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

[2] E. Bertran, Powers of cycle-classes in symmetric groups, *J. Combin. Theory Ser. A* **94** (1) (2001), 87 – 99.

[3] V.I. Chernousov, E.W. Ellers, N.L. Gordeev, Gauss decomposition with prescribed semisimple part: short proof, *J. Algebra* **229** (1) (2000), 314 – 332.

[4] E.W. Ellers, N.L. Gordeev, On the conjectures of J. Thompson and O. Ore, *Trans. Amer. Math. Soc.* **350** (9) (1998), 3657 – 3671.

[5] W.J. Ellision, Warings's problem, *Amer. Math. Monthly* **78** (1) (1971), 10 – 36.

[6] R. Guralnick, G. Malle, Products of conjugacy classes and fixed point spaces, *J. Amer. Math. Soc.* **25** (1) (2012), 77 – 121.

[7] M. Larsen, A. Shalev, Word maps and Waring type problems, *J. Amer. Math. Soc.* **22** (2) (2009), 437 – 466.

[8] M.W. Liebeck, E.A. O'Brien, A. Shalev, P.H. Tiep, The Ore conjecture, *J. Eur. Math. Soc. (JEMS)* **12** (4) (2010), 939 – 1008.

[9] M.W. Liebeck, E.A. O'Brien, A. Shalev, P.H. Tiep, Products of squares in finite simple groups, *Proc. Amer. Math. Soc.* **140** (1) (2012), 21 – 33.

[10] M.W. Liebeck, A. Shalev, Diameters of finite simple groups: sharp bounds and applications, *Ann. of Math. (2)* **154** (2) (2001), 383 – 406.

[11] M.J. Larsen, A. Shalev, P.H. Tiep, The Waring problem for finite simple groups, *Ann. of Math. (2)* **174** (3) (2011), 1885 – 1950.

[12] C. Martinez, E.I. Zelmanov, Products of powers in finite simple groups, *Israel J. Math.* **96** (1996), part B, 469 – 479.

[13] O. Ore, Some remarks on commutators, *Proc. Amer. Math. Soc.* **2** (1952), 307 – 314.

[14] J. Saxl, J.S. Wilson, A note on powers in simple groups, *Math. Proc. Cambridge Philos. Soc.* **122** (1) (1997), 91 – 94.

[15] J.S. Wilson, First-order group theory, in "Infinite groups 1994", Proceedings of the International Conference held in Ravello, May 23-27, 1994 (edited by F. de Giovanni and M.L. Newell), Walter de Gruyter & Co., Berlin, 1996, 301 – 314.