ALTERNATING AND SYMMETRIC GROUPS WITH EULERIAN GENERATING GRAPH

ANDREA LUCCHINI[1] and CLAUDE MARION[2]

[1] Dipartimento di Matematica Tullio Levi-Civita, Università degli Studi di Padova,
35121-I Padova, Italy;
email: lucchini@math.unipd.it

[2] Dipartimento di Matematica Tullio Levi-Civita, Università degli Studi di Padova,
35121-I Padova, Italy;
email: marion@math.unipd.it

Abstract

Given a finite group G, the generating graph $\Gamma(G)$ of G has as vertices the (nontrivial) elements of G and two vertices are adjacent if and only if they are distinct and generate G as group elements. In this paper we investigate properties about the degrees of the vertices of $\Gamma(G)$ when G is an alternating group or a symmetric group of degree n. In particular, we determine the vertices of $\Gamma(G)$ having even degree and show that $\Gamma(G)$ is Eulerian if and only if $n \geqslant 3$ and n and $n-1$ are not equal to a prime number congruent to 3 modulo 4.

1. Introduction

Given a finite group G, the generating graph $\Gamma(G)$ of G has as vertices the (nontrivial) elements of G and two vertices are adjacent if and only if they are distinct and generate G as group elements.

When G is simple and $|G| > 2$ many deep results on generation of G in the literature can be translated to results about $\Gamma(G)$. For example, the property that G can be generated by two elements [1, 18, 21] amounts to saying that $\Gamma(G)$ has at least one edge. The fact due to Guralnick and Kantor in [11] that every nontrivial element of G belongs to a generating pair of elements of G is equivalent to saying

that $\Gamma(G)$ has no isolated vertices. More recently, Breuer *et al.* proved in [4] that G has spread at least 2, or in other words $\Gamma(G)$ has diameter at most 2.

More generally, one can try to characterize finite groups G for which a given graph-theoretical property holds in $\Gamma(G)$. As an illustration, recall that a graph Γ is Hamiltonian (respectively, Eulerian) if it contains a cycle going through every vertex (respectively, edge) of Γ exactly once. In [5], Breuer *et al.* and the first author have investigated the finite groups G for which $\Gamma(G)$ is Hamiltonian. For example they showed that every finite simple group of large enough order has a Hamiltonian generating graph and proposed (in correspondence with [4, Conjecture 1.8]) an interesting conjecture characterizing the finite groups having a Hamiltonian generating graph.

It is natural to investigate the finite groups G for which $\Gamma(G)$ is Eulerian. A famous result going back to Euler states that a connected graph Γ is Eulerian if and only if every vertex of Γ is of even degree.

In this paper we study properties of finite groups G relative to the degrees of the vertices of $\Gamma(G)$. Given an element $g \in G$, we let $|g|$ be the order of g in G, and furthermore if $g \neq 1$ we let $\delta(g)$ be the degree of g in $\Gamma(G)$. Also G^{ab} denotes the abelianization of G, that is, $G^{ab} = G/G'$ where $G' = [G, G]$ is the commutator subgroup of G.

Given a finite group G, our first result is a criterion for a vertex of $\Gamma(G)$ to be of even degree.

PROPOSITION 1. *Let G be a finite group and $1 \neq g \in G$. Let $\epsilon \in \{1, 2\}$ be such that $\epsilon = 1$ if and only if G^{ab} is of odd order. If 2^{ϵ} divides $|N_G(\langle g \rangle)|$ then $\delta(g)$ is even.*

For an integer $n \geqslant 3$, let Alt_n and Sym_n denote the alternating and the symmetric group on n letters, respectively. The rest of the paper concentrates on $G = \mathrm{Alt}_n$ or $G = \mathrm{Sym}_n$. As $\Gamma(\mathrm{Alt}_3)$ and $\Gamma(\mathrm{Alt}_4)$ have diameters 1 and 2 respectively, these graphs are both connected. Thus the result of [4] mentioned above yields that $\Gamma(\mathrm{Alt}_n)$ is connected for every n.

Binder showed in [3] that $\Gamma(\mathrm{Sym}_n)$ is connected and has diameter 2 for $n > 4$. In fact $\Gamma(\mathrm{Sym}_3)$ has diameter 2 and is therefore connected but $\Gamma(\mathrm{Sym}_4)$ is not connected as any even involution of Sym_4 is an isolated vertex of $\Gamma(\mathrm{Sym}_4)$. In particular $\Gamma(\mathrm{Sym}_n)$ is connected for every $n \neq 4$.

Also note that $\mathrm{Sym}_n^{ab} \cong C_2$ for $n \geqslant 3$, $\mathrm{Alt}_n^{ab} \cong C_3$ for $n \in \{3, 4\}$ and Alt_n^{ab} is trivial for $n \geqslant 5$. (For a positive integer m, C_m denotes the cyclic group of order m.)

We characterize the integers n such that $|N_{\mathrm{Alt}_n}(\langle g \rangle)|$ is even for every $g \in \mathrm{Alt}_n$, as well as the integers n such that $|N_{\mathrm{Sym}_n}(\langle g \rangle)|$ is divisible by 4

for every $g \in \mathrm{Sym}_n$. This gives our first examples of alternating and symmetric groups having an Eulerian generating graph.

PROPOSITION 2. *Let $G = \mathrm{Alt}_n$ or $G = \mathrm{Sym}_n$ where $n \geqslant 3$ is an integer. Let $\Gamma(G)$ be the generating graph of G and let $1 \neq g \in G$. Let $e \in \{2, 4\}$ be such that $e = 2$ if $G = \mathrm{Alt}_n$, otherwise $e = 4$. The following assertions hold.*

(i) *If $G = \mathrm{Sym}_3$ then $|N_G(\langle g \rangle)| \equiv 2 \bmod 4$.*

(ii) *Suppose $G \neq \mathrm{Sym}_3$. Then $|N_G(\langle g \rangle)| \not\equiv 0 \bmod e$ if and only if there exists a prime number p congruent to 3 modulo 4 and a positive integer k such that $|g| = p^k$ and n can be decomposed into a sum*

$$n = \sum_{i=0}^{k} a_i p^i, \qquad (1)$$

where $a_k = 1$, $a_i \in \{0, 1\}$ for $0 \leqslant i < k$ and, only when $G = \mathrm{Alt}_n$, the number of nonzero integers a_i with i odd is odd. Moreover, if $|N_G(\langle g \rangle)| \not\equiv 0 \bmod e$ then the set of cycle lengths (in a decomposition of g into disjoint cycles) is given by $\{p^i : a_i \neq 0\}$.

(iii) *If $|g| \neq p^k$ where p is a prime number congruent to 3 modulo 4 and $k \in \mathbb{N}$, or n cannot be decomposed into a sum as in (1), then $\delta(g)$ is even.*

(iv) *If n cannot be decomposed into a sum as in (1) where p is a prime number congruent to 3 modulo 4 and $k \in \mathbb{N}$, then $\Gamma(G)$ is Eulerian.*

Given G, an alternating or a symmetric group, our main result determines the vertices of $\Gamma(G)$ of odd degree as well as whether or not $\Gamma(G)$ is Eulerian.

THEOREM 3. *Let $G = \mathrm{Alt}_n$ or $G = \mathrm{Sym}_n$ where $n \geqslant 3$ is an integer. Let $1 \neq g \in G$. Then $\delta(g)$ is odd if and only if there exists a prime number p congruent to 3 modulo 4 such that $p \in \{n, n-1\}$ and $|g| = p$. In particular, $\Gamma(G)$ is Eulerian if and only if n and $n - 1$ are not equal to a prime number congruent to 3 modulo 4.*

COROLLARY 4. *Let $G = \mathrm{Alt}_n$ or $G = \mathrm{Sym}_n$ where $n \geqslant 3$ is an integer. Suppose $\Gamma(G)$ is not Eulerian, that is, there exists a prime number p congruent to 3 modulo 4 such that $p \in \{n, n-1\}$. Let $\mathcal{P}$ be the probability that a randomly chosen element in $\Gamma(G)$ has odd degree. Then*

$$\mathcal{P} = \frac{|\mathrm{Out}(G)|}{p(1 - |\mathrm{Out}(G)|/n!)}.$$

In particular, $\mathcal{P} \to 0$ as $n \to \infty$.

Note that Corollary 4 follows immediately from Theorem 3. Indeed, since $\Gamma(G)$ is not Eulerian, an element g of $\Gamma(G)$ has odd degree if and only if g is a p-cycle. The total number of p-cycles in G is $n!/p$ and the total number of vertices in $\Gamma(G)$ is $-1 + n!/|\mathrm{Out}(G)|$. Hence

$$\mathcal{P} = \frac{n!}{p} \cdot \frac{|\mathrm{Out}(G)|}{n! - |\mathrm{Out}(G)|}$$

and the result follows.

We fix some notation that will be used throughout the paper. We remind the reader that for a finite group G and an element $g \in G$, we denote by $|g|$ the order of g, set $\Gamma(G)$ to be the generating graph of G and, if $g \neq 1$, we let $\delta(g)$ be the degree of g in $\Gamma(G)$. Given a positive integer m, we let $(\mathbb{Z}/m\mathbb{Z})^*$ be the group of units of $\mathbb{Z}/m\mathbb{Z}$ and set $\phi(m) = |(\mathbb{Z}/m\mathbb{Z})^*|$. In particular, $\phi : \mathbb{N} \to \mathbb{N}$ is the Euler's totient function.

Given two positive integers a and b, we let (a, b) denote their greatest common divisor.

We also use some standard group-theoretical notation as set in [6, Ch. 5, Section 2].

The paper is organized as follows. In Section 2, given a finite group G and $1 \neq g \in G$, we give some preliminary results on $\delta(g)$, inclusively a formula determining $\delta(g)$ via the Möbius function of G. In Section 3, we prove Proposition 1. In Section 4, we prove Proposition 2. In Section 5, we prove that if $G = \mathrm{Alt}_n$ or $G = \mathrm{Sym}_n$ and $g \in G$ does not lie in a maximal primitive subgroup of G other than Alt_n then $\delta(g)$ is even. This latter result is an important ingredient required in the proof of Theorem 3. In Section 6, we prove Theorem 3 for $G = \mathrm{Sym}_n$. Finally, in Section 7, we prove Theorem 3 for $G = \mathrm{Alt}_n$.

2. Preliminaries

Let G be a finite group and let $\Gamma(G)$ be its generating graph. Given an element $g \in G$, we let $|g|$ be the order of g in G and if $g \neq 1$ we let $\delta(g)$ denote the degree of g in $\Gamma(G)$. In this section, we collect some preliminary results on $\delta(g)$. Some of the results rely on the Möbius function μ_G of G. Recall that μ_G is the function defined inductively on the lattice of subgroups H of G by

$$\sum_{K \geqslant H} \mu_G(K) = \delta_{H,G},$$

where $\delta_{G,G} = 1$ and $\delta_{H,G} = 0$ if $H \neq G$. We give below two general properties of μ_G.

PROPOSITION 2.1. *Let G be a finite group. The following assertions hold:*

(i) *The Möbius function μ_G is invariant under conjugation, that is, if H_1 and H_2 are conjugate in G then $\mu_G(H_1) = \mu_G(H_2)$.*

(ii) *Given a subgroup H of G, $\mu_G(H) = 0$ except possibly if H is an intersection of maximal subgroups of G or $H = G$.*

Proof. Part (i) is clear and part (ii) is [**12**, Theorem 2.3]. □

Given $1 \neq g \in G$, we can relate the degree $\delta(g)$ of g in $\Gamma(G)$ to μ_G in the following way:

PROPOSITION 2.2. *Let G be a finite group and $1 \neq g \in G$. Then*

$$\delta(g) = \sum_{H \ni g} \mu_G(H)|H|.$$

Proof. This follows from [**17**, (1.1)]. □

We now record a result of Hawkes, Isaacs and Özaydin from 1989. In the statement below, the square-free part of a positive integer n denotes the product of the distinct prime divisors of n.

PROPOSITION 2.3 [**13**, Theorem 4.5]. *Let G be a finite group, H be a subgroup of G and set $m(H)$ to be the square-free part of $|G : G'H|$. Then $|N_G(H) : H|$ divides $m(H)\mu_G(H)$.*

We finally record two general results on the degree of a vertex g in $\Gamma(G)$.

PROPOSITION 2.4. *Let G be a noncyclic finite group and $1 \neq g \in G$. Then $\delta(g)$ is even if and only if the number of involutions in G adjacent to g is even.*

Proof. Let X be the set of vertices of $\Gamma(G)$ adjacent to g and let N be the number of involutions of G adjacent to g. If $X = \emptyset$ then $\delta(g) = 0$ and the result is immediate. We therefore suppose that $X \neq \emptyset$. Let x be any element of X. For any $i \in (\mathbb{Z}/|x|\mathbb{Z})^*$, we have $\langle x \rangle = \langle x^i \rangle$ and so $G = \langle g, x \rangle = \langle g, x^i \rangle$. As G is not cyclic, $x^i \neq g$ and so $x^i \in X$.

We define a relation $\sim$ on X as follows: given $x_1, x_2 \in X$ we say $x_1 \sim x_2$ if and only if $x_2 = x_1^i$ for some $i \in (\mathbb{Z}/|x_1|\mathbb{Z})^*$. One easily checks that $\sim$ is an equivalence relation on X.

Given $x \in X$, we let $[x]$ be the equivalence class of X containing x and note that $|[x]| = \phi(|x|)$. Since $1 \notin X$, X is the disjoint union of the distinct equivalence classes and $\phi(m)$ is odd if and only if $m \leqslant 2$, we deduce that $|X| \equiv N \bmod 2$. In other words $\delta(g) \equiv N \bmod 2$, as required. $\qquad\square$

PROPOSITION 2.5. *Let G be a finite group and $1 \neq g \in G$. Set*

$$C := C_{\mathrm{Aut}(G)}(g) = \{\psi \in \mathrm{Aut}(G) : \psi(g) = g\}.$$

Then $|C|$ divides $\delta(g)$.

Proof. Let X be the set of vertices of $\Gamma(G)$ adjacent to g. If $X = \emptyset$ then $\delta(g) = 0$ and the result is immediate. We therefore suppose that $X \neq \emptyset$. Then $C = C_{\mathrm{Aut}(G)}(g)$ acts on X. The action is semiregular. Indeed, suppose that $\psi \in C$ is such that $\psi(x) = x$ for some $x \in X$. Since $\psi(g) = g$ and $\langle g, x \rangle = G$, we get $\psi = 1$.

As the action of C on X is semiregular, it follows from the orbit-stabilizer theorem that the size of every orbit of X under C is equal to $|C|$. Hence $|C|$ divides $|X| = \delta(g)$, as required. $\qquad\square$

3. Criterion for even degree

In this section we prove Proposition 1.

Proof of Proposition 1. Set $K = N_G(\langle g \rangle)$. Let

$$\mathcal{S} = \{H : H \leqslant G, g \in H, |H| \equiv 1 \bmod 2, \ \mu_G(H) \equiv 1 \bmod 2\}.$$

If $\mathcal{S} = \emptyset$ then Propositions 2.2 gives $\delta(g) \equiv 0 \bmod 2$.

We therefore suppose that $\mathcal{S} \neq \emptyset$. Given a positive integer n, we let n_2 be the 2-part of n. Given $H \in \mathcal{S}$, let $m(H)$ be the square-free part of $|G : G'H|$. Note that for every $H \in \mathcal{S}$ we have $m(H)_2 = \epsilon$.

By Proposition 2.2,

$$\delta(g) \equiv \sum_{H \in \mathcal{S}} \mu_G(H)|H| \quad \bmod 2. \qquad (2)$$

One easily checks that K acts on $\mathcal{S}$ by conjugation. Let $\mathcal{S}_i$ ($1 \leqslant i \leqslant r$) be the distinct orbits of $\mathcal{S}$ under the action of K, and for $1 \leqslant i \leqslant r$, let H_i be a representative of $\mathcal{S}_i$, so that $\mathcal{S}_i = \mathrm{Orb}(H_i)$. Then

$$\mathcal{S} = \bigsqcup_{i=1}^{r} \mathrm{Orb}(H_i)$$

and

$$\sum_{H \in S} \mu_G(H)|H| = \sum_{i=1}^{r} |\text{Orb}(H_i)|\mu_G(H_i)|H_i|. \tag{3}$$

Let $1 \leqslant i \leqslant r$. We have $\text{Stab}_K(H_i) = K \cap N_G(H_i)$. By the orbit-stabilizer theorem $|\text{Orb}(H_i)| = |K : \text{Stab}_K(H_i)|$ and so $|\text{Orb}(H_i)| = |K : K \cap N_G(H_i)|$. Since $|H_i|$ and $\mu_G(H_i)$ are both odd, Proposition 2.3 yields that $|N_G(H_i)|_2$ divides $m(H_i)_2 = \epsilon$. Since $|N_G(H_i)|_2 \in \{1, \epsilon\}$ and 2^ϵ divides $|K|_2$, we deduce that $|\text{Orb}(H_i)|$ is even. Equations (2) and (3) now give $\delta(g) \equiv 0 \bmod 2$. $\qquad\square$

4. Normalizers of cyclic subgroups

In this section we prove Proposition 2. We let $G = \text{Alt}_n$ or $G = \text{Sym}_n$ where $n \geqslant 3$ is an integer. We first study the cases where $n \in \{3, 4\}$.

PROPOSITION 4.1. *Let $G = \text{Alt}_n$ or $G = \text{Sym}_n$ where $n \in \{3, 4\}$ and let $g \in G$. The following assertions hold:*

(i) *Suppose $G = \text{Alt}_3$. The vertices of $\Gamma(G)$ correspond to the two elements of G of order 3. Moreover, $\Gamma(G)$ is the complete graph K_2 on two vertices and is not Eulerian. Finally, $N_G(\langle g \rangle) = G$.*

(ii) *Suppose $G = \text{Alt}_4$. The graph $\Gamma(G)$ has eleven vertices, eight of which correspond to the elements of G of order 3, the others to the involutions of G. If $|g| = 2$ then g is only adjacent to every element of G of order 3, whereas if $|g| = 3$ then g is adjacent to the nine elements in $G \setminus \langle g \rangle$. Moreover, $\Gamma(G)$ is connected, has diameter 2 but is not Eulerian. Finally, $|N_G(\langle g \rangle)| \equiv 0 \bmod 2$ if and only if $|g| \neq 3$.*

(iii) *Suppose $G = \text{Sym}_3$. The graph $\Gamma(G)$ has five vertices, two of which correspond to the elements of G of order 3, the others to the involutions of G. If $|g| = 2$ then g is adjacent to the four elements in $G \setminus \langle g \rangle$, whereas if $|g| = 3$ then g is only adjacent to the three involutions of G. Moreover, $\Gamma(G)$ is connected, has diameter 2 but is not Eulerian. Finally, $|N_G(\langle g \rangle)| \equiv 0 \bmod 2$.*

(iv) *Suppose $G = \text{Sym}_4$. The graph $\Gamma(G)$ has three isolated vertices corresponding to the even involutions of G. In particular, $\Gamma(G)$ is not Eulerian. Finally, $|N_G(\langle g \rangle)| \equiv 0 \bmod 4$ if and only if $|g| \neq 3$.*

Proof. The various statements about the order of $N_G(g)$ can be easily checked. Also part (i) is clear.

We now consider part (ii). Every nontrivial element of G is either an involution or an element of order 3. More precisely G has three involutions and eight elements of order 3. By Propositions 2.2 or 2.5, if $|g| = 2$ then $\delta(g)$ is even. Alternatively, two involutions of G generate the Klein four-subgroup of G and so Proposition 2.4 yields that if $|g| = 2$ then $\delta(g)$ is even. In fact if $|g| = 2$ then g is adjacent to every element of G of order 3. Also, by Proposition 2.4 if $g \in G$ is such that $|g| = 3$ then $\delta(g)$ is odd. Indeed any element of G of order 3 with any of the three involutions of G generate G. In fact, if $|g| = 3$ then g is adjacent to the nine elements in $G \setminus \langle g \rangle$.

We consider part (iii). Every nontrivial element of G is either an involution or an element of order 3. Also G has three involutions and two elements of order 3. If $|g| = 2$ then Propositions 2.2 or 2.5 yields that $\delta(g)$ is even. Alternatively, by Proposition 2.4, if g is an involution then $\delta(g)$ is even, since g is adjacent to the two involutions in $G \setminus \langle g \rangle$. In fact, if $|g| = 2$ then g is adjacent to the four elements in $G \setminus \langle g \rangle$. Also by Proposition 2.4, if $g \in G$ is such that $|g| = 3$ then $\delta(g)$ is odd. Indeed any element of G of order 3 with any of the three involutions of G generate G.

Finally part (iv) consists of an easy check. □

The proof of Proposition 2 requires several lemmas.

LEMMA 4.2. *Let $S = \text{Sym}_n$ where $n \geqslant 3$ is an integer. Let g be an element of S. Set $m = |g|$ and let D_g be a decomposition of g into disjoint cycles. Let $\psi : N_S(\langle g \rangle) \to (\mathbb{Z}/m\mathbb{Z})^*$ be defined as follows: for an element s of $N_S(\langle g \rangle)$, let $\psi(s)$ be the unique element i_s in $(\mathbb{Z}/m\mathbb{Z})^*$ such that $s^{-1}gs = g^{i_s}$. The following assertions hold.*

(i) *The map ψ is an epimorphism, $\ker(\psi) = C_S(g)$ and $N_S(\langle g \rangle)/C_S(g) \cong (\mathbb{Z}/m\mathbb{Z})^*$.*

(ii) *The group $N_S(\langle g \rangle)$ is of even order.*

(iii) *If $n > 3$ or $m > 2$ then $|N_S(\langle g \rangle)| \equiv 0 \bmod 4$ except possibly if $m = p^k$ for some prime number p congruent to 3 modulo 4 and some $k \in \mathbb{N}$.*

(iv) *Suppose $n > 3$ and $m = p^k$ for some prime number p congruent to 3 modulo 4 and some $k \in \mathbb{N}$. If $|N_S(\langle g \rangle)| \not\equiv 0 \bmod 4$ then any two cycles in D_g have distinct lengths.*

Proof. We first consider part (i). One easily checks that $\psi : N_S(\langle g \rangle) \to (\mathbb{Z}/m\mathbb{Z})^*$ is a surjective homomorphism and $\ker(\psi) = C_S(g)$. The result follows from the first isomorphism theorem. In particular, $|N_S(\langle g \rangle)/C_S(g)| = \phi(m)$.

We now consider parts (ii) and (iii). Note that if $m = 1$ then $g = 1$ and $N_S(\langle g \rangle) = S$ is of even order. Moreover, S has order divisible by 4 for $n > 3$. Also if $m = 2$ then $N_S(\langle g \rangle) = C_S(g)$ contains an involution, namely g, and so $N_S(\langle g \rangle)$ is of even order. In fact, if $m = 2$ then $N_S(\langle g \rangle) = C_S(g)$ is of order divisible by 4 for $n > 3$. Suppose that $m > 2$ is even. Then $|C_S(g)| \equiv 0 \bmod 2$ and, as $\phi(m) \equiv 0 \bmod 2$, part (i) now yields $|N_S(\langle g \rangle)| \equiv 0 \bmod 4$.

Suppose finally that $m > 2$ is odd. Then $\phi(m)$ is even. Also $\phi(m) \not\equiv 0 \bmod 4$ if and only if $m = p^k$ for some prime number p congruent to 3 modulo 4 and some positive integer k. The result now follows from part (i).

We now consider part (iv). Since $\phi(m)$ is even, it follows from parts (i) and (ii) that if $|N_S(\langle g \rangle)| \not\equiv 0 \bmod 4$ then $C_S(g)$ is of odd order. The result follows. □

LEMMA 4.3. *Let $A = \mathrm{Alt}_n$ where $n > 3$ is an integer. Let $g \in A$ be an element of order m. Then $N_A(\langle g \rangle)$ is of even order except possibly if $m = p^k$ for some prime number p congruent to 3 modulo 4 and some $k \in \mathbb{N}$.*

Proof. If $m = 1$ or m is even then $N_A(\langle g \rangle)$ contains an involution and so $N_A(\langle g \rangle)$ is of even order. We can therefore assume that $m > 1$ is odd. Set $S = \mathrm{Sym}_n$. It is easy to check that

$$|N_A(\langle g \rangle)/C_A(g)| = |N_S(\langle g \rangle)/C_S(g)|/\ell$$

where $\ell \in \{1, 2\}$. It now follows from Lemma 4.2 that if $\phi(m) \equiv 0 \bmod 4$ then $N_A(\langle g \rangle)$ is of even order. Since $m > 1$ is odd, $\phi(m) \equiv 0 \bmod 4$ if and only if m is not a power of a prime number congruent to 3 modulo 4. The result follows. □

LEMMA 4.4. *Let $A = \mathrm{Alt}_n$ and $S = \mathrm{Sym}_n$ where $n = p^a$ for some prime number p congruent to 3 modulo 4 and some $a \in \mathbb{N}$. Let $g \in A$ be an n-cycle. Let h be any element of $N_S(\langle g \rangle)$, say h conjugates g to g^i for some $i \in (\mathbb{Z}/n\mathbb{Z})^*$. Let c_i be the order of i in $(\mathbb{Z}/n\mathbb{Z})^*$. The following assertions hold.*

(i) $C_S(g) = \langle g \rangle$.

(ii) *The element h is of even order if and only if $c_i \equiv 0 \bmod 2$.*

(iii) *Suppose h is of even order. Then h belongs to A if and only if a is even.*

Proof. Part (i) is clear. Indeed g is an n-cycle in $S = \mathrm{Sym}_n$, so $|C_S(g)| = n$ and $C_S(g) = \langle g \rangle$.

Since $|g| = n$, let $\psi : N_S(\langle g \rangle) \to (\mathbb{Z}/n\mathbb{Z})^*$ be the map defined as in Lemma 4.2. We have

$$\frac{N_S(\langle g \rangle)}{\langle g \rangle} \cong \operatorname{Im}(\psi) \cong C_{\phi(n)}$$

where the latter isomorphism follows from the fact that n is a power of a prime number. As $|g|$ is odd, $|h|$ is even if and only if $|\psi(h)|$ is even. This yields part (ii).

We now consider part (iii). Since $n = p^a$ where p is a prime number congruent to 3 modulo 4, $\phi(n) = 2m$ where m is an odd positive integer. Hence, as $|g|$ is odd, every Sylow 2-subgroup of $N_S(\langle g \rangle)$ has order 2. In particular, h belongs to A if and only if the involution $h^{|h|/2}$ belongs to A. Also, an involution of $N_S(\langle g \rangle)$ belongs to A if and only if every involution of $N_S(\langle g \rangle)$ belongs to A. Hence h belongs to A if and only if the involution of $N_S(\langle g \rangle)$ sending g to g^{-1} belongs to A. The latter happens if and only if a is even. The result follows. □

We can now prove Proposition 2.

Proof of Proposition 2. The case where $n \in \{3, 4\}$ follows directly from Proposition 4.1 (together with Proposition 1 when $G = \mathrm{Sym}_4$). We therefore assume that $n > 4$. Note that part (iv) is an immediate consequence of part (iii). We consider parts (ii) and (iii). Let D_g be a decomposition of g into disjoint cycles. We first suppose that $G = \mathrm{Alt}_n$.

Suppose that $N_G(\langle g \rangle)$ is of odd order. By Lemma 4.3, $|g| = p^k$ for some prime number p congruent to 3 modulo 4 and some $k \in \mathbb{N}$. Since $|g| = p^k$, it follows that, in D_g, a cycle has length p^i for some integer $0 \leqslant i \leqslant k$. For $0 \leqslant i \leqslant k$, let a_i be the number of cycles in D_g of length p^i. Since $N_G(\langle g \rangle)$ is of odd order we must have $a_i \in \{0, 1\}$ for $0 \leqslant i \leqslant k$. Moreover, as $|g| = p^k$, $a_k = 1$. Finally, suppose for a contradiction, that the number N of nonzero integers a_i with i odd is even. Using Lemma 4.4 one easily checks that there exists an involution in $N_G(\langle g \rangle)$ conjugating g to g^{-1}, contradicting $N_G(\langle g \rangle)$ being of odd order. Hence N is odd.

Suppose now that there exist a prime number p congruent to 3 modulo 4, $k \in \mathbb{N}$ and integers a_i ($0 \leqslant i \leqslant k$) such that: $|g| = p^k$, $a_i \in \{0, 1\}$, $a_k = 1$ and $n = \sum_{i=0}^k a_i p^i$ where the number N of nonzero integers a_i with i odd is odd. In particular, in D_g, there are a_i cycles of length p^i for $0 \leqslant i \leqslant k$. Since N is odd, it follows from Lemma 4.4 that $N_G(\langle g \rangle)$ is of odd order.

This establishes part (ii). Part (iii) now follows from Proposition 1.

The proof for $G = \mathrm{Sym}_n$ is similar using Lemma 4.2. □

5.   A deterministic result for alternating and symmetric groups

In this section, we provide an important ingredient needed for the proof of Theorem 3.

THEOREM 5.1. *Let $G = \text{Alt}_n$ or $G = \text{Sym}_n$ where $n > 4$ is an integer. Let $1 \neq g \in G$. If g does not belong to a maximal primitive subgroup of G not equal to Alt_n then $\delta(g)$ is even. In particular, if n is such that Sym_n and Alt_n are the only primitive groups of degree n, then every vertex in $\Gamma(G)$ has even degree and so G is Eulerian.*

Proof. Suppose for a contradiction that $\delta(g)$ is odd. By Proposition 2 we deduce that $|g| = p^k$ for some prime number p congruent to 3 modulo 4 and some positive integer k. In particular, g belongs to Alt_n. Moreover, in a decomposition D_g of g into disjoint cycles, all cycles have odd length and any two cycles have distinct lengths. Hence, without loss of generality, we can suppose that

$$g = \prod_{i=1}^{r} \sigma_i$$

where $r \in \mathbb{N}$ and, for $1 \leqslant i \leqslant r$, $|\sigma_i| = p^{a_i}$, where the sequence $(a_i)_{i=1}^{r}$ of nonnegative integers is strictly decreasing and $a_1 = k$. Moreover, we can assume that $\sigma_1 = (1, 2, 3, \ldots, p^{a_1})$. The assumption on g implies that a maximal subgroup of G containing g is either the alternating group Alt_n (if $G = \text{Sym}_n$), or an intransitive group, or an imprimitive group.

By Proposition 2.1(ii), a subgroup H of G containing g and such that $\mu_G(H) \neq 0$ is either G, Alt_n (if $G = \text{Sym}_n$), a maximal intransitive group, a maximal imprimitive group, or the intersection of at least two maximal subgroups of G of the kind just described.

Note that if $r = 1$ then $g = \sigma_1$, $n = p^{a_1}$ and no intransitive subgroup of G contains g. Also if $r > 1$ the intersection of all maximal intransitive subgroups of Sym_n containing g is the group

$$H_1 = \prod_{i=1}^{r} \text{Sym}_{p^{a_i}} .$$

Since $n > 4$ the group H_1 is of order divisible by 4.

Now suppose that g belongs to a maximal imprimitive subgroup K of Sym_n. Note that $a_1 \geqslant 2$, as otherwise $a_1 = 1$, g is a p-cycle and $n \in \{p, p+1\}$, but there is no imprimitive subgroup of Sym_n containing a p-cycle. Let $\Omega = \{1, \ldots, p^{a_1}\}$ be the support of σ_1 and let $B_1, \ldots, B_t$ be the blocks of K having

nonempty intersection with Ω. The integer t is the smallest positive integer such that $g^t(B_1) = B_1$. In particular, $t \leqslant p^{a_1}$ and t divides p^{a_1}. Hence $t = p^\beta$ for some integer $0 \leqslant \beta \leqslant a_1$. Without loss of generality, $i \in B_i$ for $1 \leqslant i \leqslant t$.

Note that

$$n - p^{a_1} = \sum_{i=2}^{r} p^{a_i}$$
$$\leqslant \sum_{i=0}^{a_2} p^i$$
$$= \frac{p^{a_2+1} - 1}{p - 1}$$
$$< p^{a_1}.$$

We claim that $t \neq 1$. Indeed, suppose $t = 1$. Then a block B of K has size at least p^{a_1}. Since $n - p^{a_1} < p^{a_1}$, it follows that K has a single block contradicting the imprimitivity of K. We claim also that $t \neq p^{a_1}$. Indeed, suppose $t = p^{a_1}$. Then $n - t < t$, a contradiction.

It follows that $1 \leqslant \beta \leqslant a_1 - 1$. Since $\beta \leqslant a_1 - 1$, we have

$$\Gamma_1 = \{i \cdot p^{a_1-1} + 1 : 0 \leqslant i \leqslant p - 1\} \subseteq B_1, \tag{4}$$
$$\Gamma_2 = \{i \cdot p^{a_1-1} + 2 : 0 \leqslant i \leqslant p - 1\} \subseteq B_2, \tag{5}$$

and $\mathrm{Sym}(\Gamma_1) \times \mathrm{Sym}(\Gamma_2) \cong \mathrm{Sym}_p \times \mathrm{Sym}_p$ is a subgroup of K of order divisible by 4.

Let H be any proper subgroup of G containing g and such that $\mu_G(H) \neq 0$.

If $r = a_1 = 1$ then $G = \mathrm{Sym}_n$, $H = \mathrm{Alt}_n$ and, as $n > 3$, H is of even order. If $r = 1$ and $a_1 \geqslant 2$ then H contains $(\mathrm{Sym}(\Gamma_1) \times \mathrm{Sym}(\Gamma_2)) \cap \mathrm{Alt}_n$ which is of even order. If $r > 1$ and $a_1 = 1$ then H contains $H_1 \cap \mathrm{Alt}_n$ which is of even order. Finally if $r > 1$ and $a_1 > 1$ then H contains $H_1 \cap \mathrm{Alt}_n \cap (\mathrm{Sym}(\Gamma_1) \times \mathrm{Sym}(\Gamma_2)) = \mathrm{Alt}_n \cap (\mathrm{Sym}(\Gamma_1) \times \mathrm{Sym}(\Gamma_2))$ which is again of even order. We deduce that H has even order and by Proposition 2.2 it follows that $\delta(g)$ is even, contradicting our supposition that $\delta(g)$ is odd. Arguing by contradiction, we have showed that $\delta(g)$ is even for every $g \in \Gamma(G)$, as required.

The final part of the theorem now follows at once. $\qquad\square$

6. More on symmetric groups

In this section, we prove Theorem 3 for symmetric groups. We will need a few lemmas.

LEMMA 6.1. *Let $S = \mathrm{Sym}_n$ where $n = p^a$ for some odd prime number p and some positive integer a. Assume $n > 5$. Suppose H is an almost simple primitive subgroup of S with $\mathrm{soc}(H) = \mathrm{PSL}_d(q)$ where $d \geqslant 2$ and $q = r^f$ for some prime number r and some positive integer f. If the action of H is on the set of points of the projective space $\mathrm{PG}_{d-1}(q)$ then d is prime, $(d, q-1) = 1$, $\mathrm{PSL}_d(q) = \mathrm{PGL}_d(q)$ and $H \leqslant \mathrm{Alt}_n$.*

Proof. Note that $H \leqslant \mathrm{P\Gamma L}_d(q)$, as if $d > 2$ the graph automorphism of H does not act on the set of points of the projective space $\mathrm{PG}_{d-1}(q)$. Also since n is odd, if $d = 2$ then $q = n - 1$ is even and so $(d, q-1) = 1$. In fact, since $n = (q^d - 1)/(q - 1)$ is a power of a prime, if $d \geqslant 3$ then, by [7, Proposition 1], d is prime and $(d, q-1) = 1$. Therefore, under the assumptions of the lemma, d is prime, $(d, q-1) = 1$ and $\mathrm{PGL}_d(q) = \mathrm{PSL}_d(q)$. It remains to show that $H \leqslant \mathrm{Alt}_n$.

Suppose first that $d = 2$. Then $n = q + 1$. As n is odd, $r = 2$. Also $f \neq 2$ as $n > 5$. By [2, Table 3C] $H \leqslant \mathrm{Alt}_n$.

Suppose now that $d > 2$. If f is odd then by [2, Table 3C] $H \leqslant \mathrm{Alt}_n$. Finally, we claim that f is not even. Suppose otherwise and write $f = 2\ell$ for some $\ell \geqslant 1$. Since $d \geqslant 3$ is prime and $(q^d - 1)/(q - 1)$ is a power of a prime, one easily checks that $(r, f, d) \notin \{(2, 2, 3), (2, 2, 6), (2, 4, 3)\}$. By Zsigmondy's theorem there is a prime divisor u_1 of $r^{fd} - 1$ not dividing $r^s - 1$ for every $1 \leqslant s < fd$. Clearly $u_1 = p$. Again, applying Zsigmondy's theorem, there is a prime divisor u_2 of $r^{\ell d} - 1$ not dividing $r^s - 1$ for every $1 \leqslant s < \ell d$. Clearly $u_2 \neq p$. Now

$$p^a(r^{2\ell} - 1) = r^{2\ell d} - 1 = (r^{\ell d} - 1)(r^{\ell d} + 1)$$

and so u_2 divides $r^{2\ell} - 1$, a contradiction, as $2\ell < \ell d$ (since $d \geqslant 3$). $\qquad\square$

LEMMA 6.2. *Let $S = \mathrm{Sym}_{p+1}$ where p is an odd prime number and let g be a nontrivial p-element of S. Then there is a unique transitive subgroup of S isomorphic to $\mathrm{PGL}_2(p)$ containing g.*

Proof. The group $\mathrm{PSL}_2(p)$ acts 2-transitively and faithfully on the set of points of the projective space $\mathrm{PG}_1(p)$ of cardinality $p + 1$. In particular $\mathrm{PSL}_2(p)$ is a transitive subgroup of Sym_{p+1}. Moreover, $\mathrm{PGL}_2(p)$ is a subgroup of the normalizer of $\mathrm{PSL}_2(p)$ in Sym_{p+1}. By [2, Proposition 3.9.2], there is a unique conjugacy class of transitive subgroups of S isomorphic to $\mathrm{PSL}_2(p)$. In particular there is a single conjugacy class of transitive subgroups of S isomorphic to $\mathrm{PGL}_2(p)$. Since $\mathrm{PGL}_2(p)$ contains a nontrivial p-element and all nontrivial p-elements are conjugate in Sym_{p+1}, we deduce that there is a subgroup H of Sym_{p+1} isomorphic to $\mathrm{PGL}_2(p)$ containing g. From the cycle shape of g, we have $C_{\mathrm{Sym}_{p+1}}(g) = C_p$ and following Lemma 4.2, $N_{\mathrm{Sym}_{p+1}}(\langle g \rangle)$ has order $p(p-1)$.

It follows that $N_{\mathrm{Sym}_{p+1}}(\langle g \rangle)$ is the unique parabolic subgroup P of H containing g. We claim that P is not a subgroup of any other subgroup H_0 of Sym_{p+1} conjugate to H. Suppose otherwise. Then there exists $k \in \mathrm{Sym}_{p+1}$ such that $H^k = H_0$, $H_0 \neq H$, $P \leqslant H$ and $P \leqslant H_0$. Let $P_0 = P^k$ and note that P_0 is a parabolic subgroup of H_0. Since all parabolic subgroups of H_0 are conjugate, there exists $a \in H_0$ such that $P_0 = P^a$. We obtain that $ka^{-1} \in N_{\mathrm{Sym}_{p+1}}(P)$. Since $P = N_{\mathrm{Sym}_{p+1}}(\langle g \rangle)$ and $\langle g \rangle$ is a p-Sylow subgroup of Sym_{p+1}, we in fact have $N_{\mathrm{Sym}_{p+1}}(P) = P$. In particular, $ka^{-1} \in P$. Since $a \in H_0$, we obtain $k \in H_0$, and $H = H_0$, a contradiction. It follows that H is the unique transitive subgroup of Sym_{p+1} isomorphic to $\mathrm{PGL}_2(p)$ and containing g. □

LEMMA 6.3. *Let $S = \mathrm{Sym}_n$ where $n \geqslant 3$ is an integer. Let $p \leqslant n$ be a prime number and g be a p-element of S having no two cycles of same length. Then $|g| > n/2$.*

Proof. Say g has order $|g| = p^a$ for some $a \in \mathbb{N}$. Clearly

$$
\begin{aligned}
n &\leqslant \sum_{i=0}^{a} p^i \\
&= p^a + \sum_{i=0}^{a-1} p^i \\
&= p^a + \frac{p^a - 1}{p - 1} \\
&< 2p^a \\
&= 2|g|.
\end{aligned}
$$

□

LEMMA 6.4. *Let $S = \mathrm{Sym}_n$ where $n \geqslant 3$ is an integer. Let $p \leqslant n$ be a prime number and g be a p-element of S having no two cycles of same length. Suppose that g belongs to a primitive subgroup H of S. Then either H is almost simple or H is of affine type.*

Proof. By Lemma 6.3, $|g| > n/2$.

By [19, Theorem 1], the finite quasiprimitive permutation groups split into eight families: AS, HA, SD, HS, HC, CD, TW and PA. The latter subdivision is described in [20, Section 5] where the eight types of quasiprimitive groups are defined (depending on the structure and on the action of the socle), namely HA (Holomorphic Abelian), AS (Almost Simple), SD (Simple Diagonal), CD (Compound Diagonal), HS (Holomorphic Simple), HC (Holomorphic

Compound), TW (Twisted Wreath) and PA (Product Action), and it follows from the O'Nan–Scott theorem (see [**16**] or [**8**, Ch. 4]) that every primitive group is of exactly one of these types.

To establish that H is almost simple or of affine type amounts to showing that H is of AS or HA type. By [**10**, Theorem 5.9] if a primitive group of degree n of type SD contains an element h of order $|h| \geqslant n/4$ then $n = 60$ and $|h| = 15$. As $|g| > n/2$, it follows that the group H is not of type SD. Also as a primitive group of type HS is contained in a primitive group of type SD, H cannot be of type HS. If H is of type HC, CD, TW then by [**10**, Section 5.3] H does not contain any element of order greater than $n/4$, contradicting $|g| > n/2$.

We claim finally that if H is of type PA then H is in fact almost simple. Suppose indeed that H is of type PA. Then $\mathrm{soc}(H) = T^\ell$ for some nonabelian finite simple group T and for some $\ell \in \mathbb{N}$. Moreover, $H \leqslant X \mathrm{wr} \, \mathrm{Sym}_\ell$ where $\mathrm{soc}(X) = T$ and $X \leqslant \mathrm{Sym}_a$ for some $a \in \mathbb{N}$ such that $n = a^\ell$. We show that $\ell = 1$, establishing that H is indeed almost simple. Since $g \in H \leqslant X \mathrm{wr} \, \mathrm{Sym}_\ell$, there exist $x_1, \dots, x_\ell$ in X and σ in Sym_ℓ such that $g = (x_1, \dots, x_\ell)\sigma$. As g is a p-element, σ is a p-element of Sym_ℓ of order at most ℓ. In particular, there exists $k \in \mathbb{N}$ with $k \leqslant \ell$ such that $g^k \in X^\ell$. Now g^k is a p-element of $(\mathrm{Sym}_a)^\ell$ and has order at most a. In particular, there exists $j \in \mathbb{N}$ with $j \leqslant a$ such that $g^{kj} = 1$. It follows that $|g| \leqslant kj \leqslant a\ell$. Since $|g| > n/2 = a^\ell/2$, we deduce that $a\ell > a^\ell/2$. That is $2\ell \geqslant a^{\ell-1}$. Since X is almost simple, $a \geqslant 5$ and so $\ell = 1$. In particular H is almost simple. The result follows. □

LEMMA 6.5. *Let $S = \mathrm{Sym}_n$ where $n \geqslant 3$ is an integer. Let $p \leqslant n$ be a prime number and g be a p-element of S having no two cycles of same length. Suppose that g belongs to an almost simple primitive subgroup H of S with $\mathrm{soc}(H) = \mathrm{Alt}_m$ for some $m \in \mathbb{N}$. If $1 < k < m-1$ then the action of H is not on the set of k-subsets from $\{1, \dots, m\}$.*

Proof. Note that $m \geqslant 5$. Suppose that H acts on the set of k-subsets from $\{1, \dots, m\}$. Then $n = \binom{m}{k}$. The assumption on k gives that $\binom{m}{k} \geqslant 2m$, that is $n \geqslant 2m$. Now $g \in \mathrm{Alt}_m$ being a p-element has order at most m and so $|g| \leqslant n/2$ contradicting Lemma 6.3. □

LEMMA 6.6. *Let $S = \mathrm{Sym}_n$ where $n \geqslant 3$ is an integer. Let $p \leqslant n$ be a prime number congruent to 3 modulo 4 and let g be a p-element of S having no two cycles of same length. Suppose that g belongs to an almost simple primitive subgroup H of S with $\mathrm{soc}(H) = \mathrm{PSL}_d(q)$ for some $2 \leqslant d \in \mathbb{N}$ and some prime power $q = r^f$. If the action of H is on the set of points of the projective space $\mathrm{PG}_{d-1}(q)$ then one of the following holds:*

(i) $d = 2$, $q = r = p$, $n = p + 1$ *and* $|g| = p$;

(ii) $|g| = n = (q^d - 1)/(q - 1)$ *and* $r \neq p$.

Proof. Note that from the existence of the subgroup H of G, we must have $n \geqslant 5$. Say $|g| = p^a$ for some $a \in \mathbb{N}$. By assumption,

$$n = (q^d - 1)/(q - 1) = (r^{fd} - 1)/(r^f - 1).$$

Also by Lemma 6.3, $|g| > n/2$. Since g has odd order and a graph automorphism of $\mathrm{PSL}_d(q)$ is an involution, $g \in \mathrm{PGL}_d(q) \rtimes \langle \psi \rangle$ where ψ is a generator of the group of field automorphisms and has order f. In particular there exist $g_1 \in \mathrm{PGL}_d(q)$ and $\psi_1 \in \langle \psi \rangle$ such that $g = g_1 \psi_1$. Set $h = |\psi_1|$. Note that h divides f. Since $|g| = p^a$, $h = p^b$ for some nonnegative integer $b \leqslant a$.

We show that $g \in \mathrm{PGL}_d(q)$. Suppose not. Then $h > 1$ and so $b \geqslant 1$. By the proof of [10, Theorem 2.16], $g_2 = g^h$ belongs to $\mathrm{PGL}_d(q^{1/h})$. In particular, g has order dividing $h|g_2|$. Moreover, by [10, Corollary 2.7],

$$|g_2| \leqslant \frac{r^{(f/h)d} - 1}{r^{f/h} - 1}.$$

Since $h \geqslant 3$, one can check that

$$2h \frac{r^{(f/h)d} - 1}{r^{f/h} - 1} \leqslant \frac{r^{fd} - 1}{r^f - 1}$$

unless $d = 2$, $r = 2$, and $h = f = 3$ or $h = f = 4$. The latter does not hold as p is odd. It follows that $|g| \leqslant n/2$ except possibly if $d = 2$, $r = 2$ and $h = f = 3$. Suppose $d = 2$, $r = 2$ and $h = f = 3$. Then $\mathrm{soc}(H) = \mathrm{PSL}_2(2^3)$, $n = 9$ and $|g|$ has order dividing 9. However $\mathrm{PGL}_2(2^3) \rtimes \langle \psi \rangle$ has no element of order 9 and so $|g| = 3$. In particular $|g| \leqslant n/2$ in all cases, a contradiction. Hence $g \in \mathrm{PGL}_d(q)$ as claimed.

Suppose first that $r = p$. Then g is a unipotent element of $\mathrm{PGL}_n(q)$. Note that $d \neq 3$. Indeed, otherwise, $|g| = p$ and $n = q^2 + q + 1$, and so $|g| \leqslant n/2$, a contradiction.

We show that $d = 2$. Suppose not. Then $d \geqslant 4$. By [10, Proposition 2.6], $|g| \leqslant p^{\lceil \ln(d)/\ln(p) \rceil}$. Since $p \geqslant 3$, $|g| < p^{\ln(d)+1}$. But $p^{\ln(d)+1} \leqslant (q^d - 1)/2(q - 1)$ for $p \geqslant 3$ and $d \geqslant 4$, and so $|g| \leqslant n/2$, a contradiction.

Hence $d = 2$. Therefore $|g| = p$ and $n = q + 1$. Moreover, if $f > 1$ then $|g| \leqslant n/2$, a contradiction. So $f = 1$ and $q = p$.

Suppose now that $r \neq p$ so that g is a semisimple element of $\mathrm{PGL}_n(q)$. Since g has no two cycles of same length, the proof of [**10**, Corollary 2.7] yields that $|g|$ divides $n = (q^d - 1)/(q - 1)$ or $|g|$ divides $q^{d-1} - 1$.

We first show that $|g|$ does not divide $q^{d-1} - 1$. Suppose otherwise. Note that if $|g|$ is not equal to $q^{d-1} - 1$ then $|g| \leqslant n/2$, a contradiction. Hence $|g| = q^{d-1} - 1$. Since $|g|$ is odd, we must have $r = 2$. Moreover, as $|g|$ is a power of an odd prime, Zsigmondy's theorem yields that $d = 2$. So $n = q + 1$ and $|g| = q - 1$. Hence g must have two fixed points, a contradiction. Therefore $|g|$ does not divide $q^{d-1} - 1$, as claimed.

Suppose that $|g|$ divides n. Note that if $|g| \neq n$ then $|g| \leqslant n/2$, a contradiction. Hence $|g| = n$. The result follows. □

LEMMA 6.7. *Let $S = \mathrm{Sym}_n$ where $n \geqslant 3$ is a positive integer. Let $p \leqslant n$ be an odd prime number and g be a p-element of S having no two cycles of same length. Suppose that g belongs to an almost simple primitive subgroup H of S. Assume that if $\mathrm{soc}(H) = \mathrm{PSL}_d(q)$ then the action of H is not on the set of points of the projective space $\mathrm{PG}_{d-1}(q)$. Moreover assume that $\mathrm{soc}(H) \neq \mathrm{Alt}_n$. Then one of the following holds:*

(i) $\mathrm{soc}(H) = M_{11}$, $|g| = 11$ *and* $n \in \{11, 12\}$;

(ii) $\mathrm{soc}(H) = M_{12}$, $|g| = 11$ *and* $n = 12$;

(iii) $\mathrm{soc}(H) = M_{23}$, $|g| = 23$ *and* $n = 23$;

(iv) $\mathrm{soc}(H) = M_{24}$, $|g| = 23$ *and* $n = 24$;

(v) $\mathrm{soc}(H) = \mathrm{PSL}_2(7)$, $|g| = 7$ *and* $n = 7$;

(vi) $\mathrm{soc}(H) = \mathrm{PSL}_2(11)$, $|g| = 11$ *and* $n = 11$.

Moreover $H \leqslant \mathrm{Alt}_n$.

Proof. Suppose first that $\mathrm{soc}(H) = \mathrm{Alt}_m$ for some $m \in \mathbb{N}$. Since $m \neq n$ we can assume from Lemma 6.5 and [**10**, Theorem 1.3] that $\mathrm{soc}(H) = \mathrm{Alt}_m$ where $m \in \{5, 6, 7, 8, 9\}$. From the possible cycle shapes of g and using [**10**, Table 6] which gives the possible degrees of the corresponding action of H, we deduce that $m = n$, a contradiction.

Suppose now that $\mathrm{soc}(H)$ is of classical type. Recall that if $\mathrm{soc}(H) = \mathrm{PSL}_d(q)$ then the action of H is not on the set of points of the projective space $\mathrm{PG}_{d-1}(q)$. From the possible cycle shapes of g and using [**10**, Table 6] which gives the possible degrees of the corresponding action of H we deduce that $\mathrm{soc}(H) = \mathrm{PSL}_2(q)$ where $q \in \{7, 11\}$. Moreover $n = |g| = q$.

If soc(H) is not an alternating group nor a classical group then by [**10**, Theorem 1.3], soc(H) $= M_r$ where $r \in \{11, 12, 22, 23, 24\}$. Considering the possible cycle shapes of g and [**10**, Table 6] which gives the possible degrees of the corresponding action of H we deduce that one of the cases (i)–(iv) in the statement of the lemma holds.

We finally check that $H \leqslant \mathrm{Alt}_n$. Clearly soc($H$) $\leqslant \mathrm{Alt}_n$. We show that if H is as in (i)–(vi) then $H = \mathrm{soc}(H)$ and so $H \leqslant \mathrm{Alt}_n$.

As Out(H) is trivial for $H \in \{M_{11}, M_{23}, M_{24}\}$, if H is as in (i), (iii) or (iv) then $H = \mathrm{soc}(H)$.

Suppose that soc(H) $= \mathrm{PSL}_2(q)$ where $q \in \{7, 11\}$, so that $n = q$. As

$$\mathrm{Aut}(\mathrm{PSL}_2(q)) = \mathrm{PGL}_2(q) = \mathrm{PSL}_2(q).2$$

and $\mathrm{PGL}_2(q)$ is not a subgroup of Sym_n, we deduce that $H = \mathrm{PSL}_2(q)$ and so $H = \mathrm{soc}(H)$.

To conclude, since Out(M_{12}) is of order 2 and Sym_{12} has no subgroup of order $2|M_{12}|$, we deduce that if soc(H) $= M_{12}$ then $H = \mathrm{soc}(H)$. □

LEMMA 6.8. *Let $S = \mathrm{Sym}_n$ where $n \geqslant 3$ is an integer. Let $p \leqslant n$ be a prime number congruent to 3 modulo 4 and let g be a p-element of S having no two cycles of same length. Suppose that g belongs to a primitive subgroup H of S of affine type. Say $H \leqslant \mathrm{AGL}_d(q)$ for some $1 \leqslant d \in \mathbb{N}$ and some prime number q. Then $|g| = p$. Moreover one of the following assertions holds.*

  (i) $q = p, d = 1, n = p$;

  (ii) $q = 2, n = p + 1 = 2^d$.

Proof. Note that $n = q^d$. Suppose that $q = p$. Then $|g| \leqslant pt$ where t is the order of some unipotent element of $\mathrm{GL}_d(q)$. By [**9**, Lemma 2.2] we have

$$\begin{aligned} t &\leqslant p^{\lceil \ln(d)/\ln(p) \rceil} \\ &\leqslant p^{\ln(d)/(\ln(p))+1} \\ &\leqslant dp. \end{aligned}$$

It follows that $|g| \leqslant dp^2$. Now by Lemma 6.3, $|g| > n/2$ and so $|g| > p^d/2$. It follows that $dp^2 > p^d/2$ and so $2d > p^{d-2}$. Since $p \equiv 3 \bmod 4$, the latter inequality does not hold if $d \geqslant 4$, or $d \geqslant 3$ and $p \neq 3$. Thus $d \leqslant 2$ or $d = p = 3$.

Suppose that $d = 3$ and $p = 3$. Then $t \leqslant p$ and so $|g| \leqslant 3^2$. But $|g| > 3^3/2$, and so $|g| > 3^2$, a contradiction. Thus $d \leqslant 2$. We claim that $d \neq 2$. Suppose otherwise.

Then $n = p^2$, g is a p^2-cycle and $|g| = p^2$. But $\mathrm{AGL}_2(p)$ has exponent p, and so $|g| \neq p^2$ and $d \neq 2$. Hence $d = 1$, $n = p$ and so g is a p-cycle.

Suppose now that $q \neq p$. Since g is a p-element and $q \neq p$, we must have $g \in \mathrm{GL}_d(q)$. In particular $|g|$ divides $q^a - 1$ for some positive integer a satisfying $1 \leqslant a \leqslant d$. Since, by Lemma 6.3, $|g| > n/2$, we must have $|g| = q^d - 1 = n - 1$. Hence there exists a positive integer u such that $p^u = q^d - 1$. As p is odd, $q = 2$ and $p^u + 1 = 2^d$. We show that $u = 1$. Suppose otherwise. Then $u > 1$ and by Zsigmondy's theorem, there is a prime number dividing $p^{2u} - 1$ but not $p^u - 1$. So $p^u + 1$ is divisible by an odd prime, a contradiction. Therefore $u = 1$, $|g| = p$ and $n = p + 1 = 2^d$. □

We can now prove Theorem 3 for symmetric groups.

Proof of Theorem 3 for symmetric groups. If $n \in \{3, 4\}$ then Theorem 3 follows from Proposition 4.1 (together with Proposition 1 when $G = \mathrm{Sym}_4$). We therefore assume that $n > 4$. By Propositions 1 and 2 if $|g|$ is not a power of a prime number congruent to 3 modulo 4 or if there are two cycles of same length in a decomposition D_g of g into disjoint cycles, then $\delta(g)$ is even. We therefore assume that n is such that there exists an element $h \in \mathrm{Sym}_n$ such that
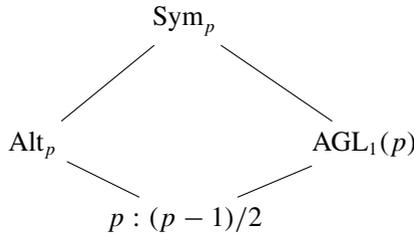
- $|h| = p^a$ for some prime number p congruent to 3 modulo 4 and some $a \in \mathbb{N}$

- in D_h no two cycles have the same length.

Without loss of generality we assume that g is an element of Sym_n having the two defining properties of h above, as otherwise $\delta(g)$ is even. In particular, $|g| = p^a$, and by Lemma 6.3, $|g| > n/2$.

Suppose first that n and $n - 1$ are not equal to a prime congruent to 3 modulo 4. By [10, Theorem 1.3] and Lemmas 6.4–6.7, a proper primitive subgroup H of Sym_n, with $H \neq \mathrm{Alt}_n$ and $g \in H$, satisfies $\mathrm{soc}(H) = \mathrm{PSL}_d(q)$ for some positive integer $d \geqslant 2$ and some prime power q. Moreover $|g| = n = (q^d - 1)/(q - 1)$. Since n is a power of a prime, by Lemma 6.1, we in fact have $H \leqslant \mathrm{Alt}_n$. In particular the only maximal primitive subgroup of Sym_n containing g is Alt_n and Theorem 5.1 yields that $\delta(g)$ is even. It follows that $\Gamma(\mathrm{Sym}_n)$ is Eulerian.

Suppose now that n is equal to a prime number congruent to 3 modulo 4. Then $n \geqslant 7$. Note that if g belongs to a primitive group H with $\mathrm{soc}(H) = \mathrm{PSL}_d(q)$, then, by [10, Theorem 1.3] and Lemma 6.1, $H \leqslant \mathrm{Alt}_n$. By [10, Theorem 1.3] and Lemmas 6.4–6.8, a proper primitive subgroup H of Sym_n containing g satisfies $H \leqslant \mathrm{Alt}_n$ or $n = |g| = p$ and H is a subgroup of the unique subgroup of Sym_n containing g and isomorphic to $\mathrm{AGL}_1(p) = p : (p - 1)$. If $g \notin \mathrm{AGL}_1(p)$ then the

only maximal primitive subgroup of Sym_n containing g is Alt_n and Theorem 5.1 yields that $\delta(g)$ is even. We therefore suppose that $n = |g| = p$. In particular g is a p-cycle and the only maximal subgroups of Sym_p containing g are $H_1 = \mathrm{Alt}_p$ and $H_2 = \mathrm{AGL}_1(p)$. These two subgroups intersect in a subgroup H_3 of odd order $p(p-1)/2$ and of index 2 in H_2. In particular the lattice of subgroups H of Sym_p containing g and with nonzero Möbius function $\mu_{\mathrm{Sym}_p}(H)$ is as follows:

$$
\begin{array}{ccc}
& \mathrm{Sym}_p & \\
& \diagup \quad \diagdown & \\
\mathrm{Alt}_p & & \mathrm{AGL}_1(p) \\
& \diagdown \quad \diagup & \\
& p : (p-1)/2 &
\end{array}
$$

Since $\mu_{\mathrm{Sym}_p}(H_1) = \mu_{\mathrm{Sym}_p}(H_2) = -1$ and $\mu_{\mathrm{Sym}_p}(H_3) = 1$, it follows from Proposition 2.2 that

$$
\begin{aligned}
\delta(g) &= \mu_{\mathrm{Sym}_p}(\mathrm{Sym}_p) \cdot |\mathrm{Sym}_p| + \mu_{\mathrm{Sym}_p}(H_1) \cdot |H_1| \\
&\quad + \mu_{\mathrm{Sym}_p}(H_2) \cdot |H_2| + \mu_{\mathrm{Sym}_p}(H_3) \cdot |H_3| \\
&= |\mathrm{Sym}_p| - |H_1| - |H_2| + |H_3| \\
&= p! - p!/2 - p(p-1) + p(p-1)/2 \\
&= p!/2 - p(p-1)/2 \\
&= \frac{p(p-1)}{2} \cdot ((p-2)! - 1).
\end{aligned}
$$

Since $p \geqslant 7$ and $p \equiv 3 \bmod 4$, $\delta(g)$ is odd.

Suppose now that $n - 1$ is equal to a prime congruent to 3 modulo 4. Note that $n \geqslant 8$. Also if g belongs to a primitive subgroup H of affine type contained in $\mathrm{AGL}_d(2)$, then, as $\mathrm{GL}_d(2) = \mathrm{SL}_d(2)$ is perfect, $\mathrm{AGL}_d(2)$ is perfect and so $H \leqslant \mathrm{AGL}_d(2) \leqslant \mathrm{Alt}_n$. By [10, Theorem 1.3], Lemmas 6.2 and 6.4–6.8, a proper primitive subgroup H of Sym_n containing g satisfies $H \leqslant \mathrm{Alt}_n$ or $n - 1 = |g| = p$ and H is a subgroup of a transitive subgroup of Sym_n containing g and isomorphic to $\mathrm{PGL}_2(p)$. By Lemma 6.2, the latter subgroup of Sym_n is the unique transitive subgroup of Sym_n containing g and isomorphic to $\mathrm{PGL}_2(p)$. Note that $\mathrm{PGL}_2(p) \cap \mathrm{Alt}_{p+1} \cong \mathrm{PSL}_2(p)$. If $g \notin \mathrm{PGL}_2(p)$ then the only maximal primitive subgroup of Sym_n containing g is Alt_n and Theorem 5.1 yields that $\delta(g)$ is even. We therefore suppose that $n - 1 = |g| = p$. In particular g is a p-cycle

and the only maximal subgroups of Sym_{p+1} containing g are Alt_{p+1}, $\mathrm{PGL}_2(p)$ and the intransitive subgroup of Sym_{p+1} isomorphic to Sym_p and containing g. The lattice of subgroups H of Sym_{p+1} containing g and with nonzero Möbius function $\mu_{\mathrm{Sym}_{p+1}}(H)$ is as follows:
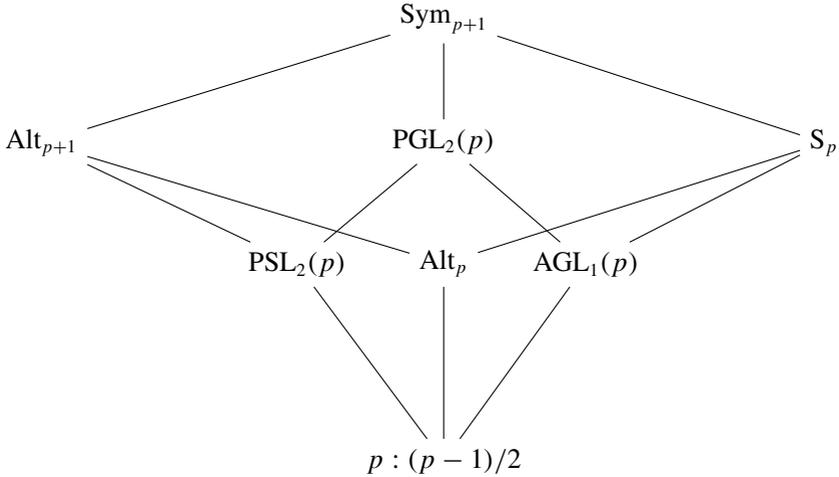
Using Proposition 2.2 and the fact that $p \equiv 3 \bmod 4$ and $p \geqslant 7$, we obtain that

$$\delta(g) = \frac{p!}{2} \cdot p - \frac{p^2(p-1)}{2}$$

is odd.   □

7. More on alternating groups

PROPOSITION 7.1. *Let $G = \mathrm{Alt}_n$ where $n \in \{7, 11, 12, 23, 24\}$. Let $1 \neq g \in G$. Then $\delta(g)$ is even if and only if $n \equiv 3 \bmod 4$ and $|g| \neq n$, or $n \equiv 0 \bmod 4$ and $|g| \neq n-1$. In particular, $\Gamma(G)$ is not Eulerian.*

Proof. Suppose first that $G = \mathrm{Alt}_7$. Let $1 \neq g \in G$. By Proposition 2, $\delta(g)$ is even except possibly if $|g| = 7$. Without loss of generality, we assume that $|g| = 7$. The lattice of subgroups H of G containing g and with nonzero Möbius function $\mu_G(H)$ is as follows:
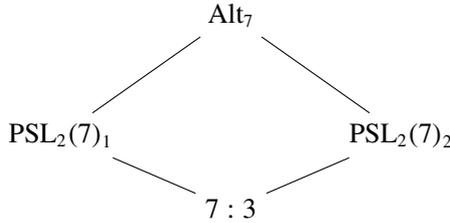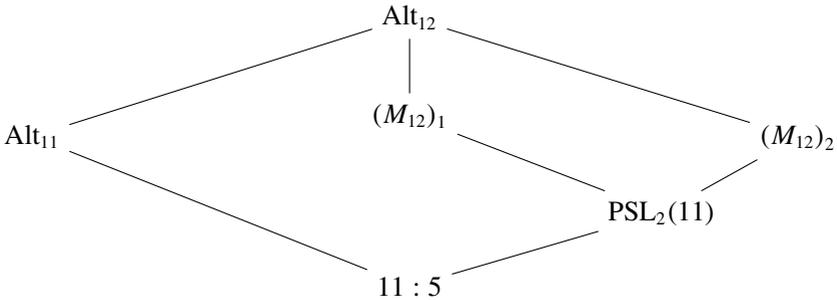
Since $\mu_G(G) = 1$, $\mu_G(\mathrm{PSL}_2(7)_i) = -1$ for $i \in \{1, 2\}$ and $\mu_G(7 : 3) = 1$, Proposition 2.2 yields $\delta(g) \equiv 1 \bmod 2$. In particular $\Gamma(G)$ is not Eulerian.

Suppose that $G = \mathrm{Alt}_{11}$. Let $1 \neq g \in G$. By Proposition 2, $\delta(g)$ is even except possibly if $|g| = 11$. Without loss of generality, we assume that $|g| = 11$. The lattice of subgroups H of G containing g and with nonzero Möbius function $\mu_G(H)$ is as follows:
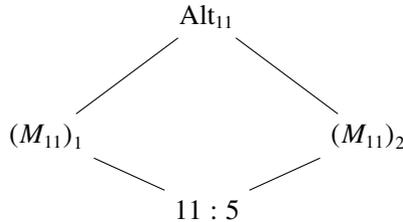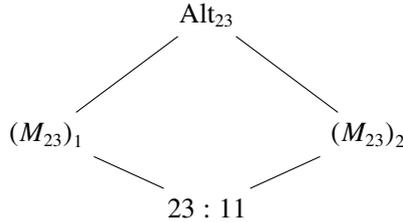

Since $\mu_G(G) = 1$, $\mu_G((M_{11})_i) = -1$ for $i \in \{1, 2\}$ and $\mu_G(11 : 5) = 1$, Proposition 2.2 yields $\delta(g) \equiv 1 \bmod 2$. In particular $\Gamma(G)$ is not Eulerian.

Suppose that $G = \mathrm{Alt}_{12}$. Let $1 \neq g \in G$. By Proposition 2, $\delta(g)$ is even except possibly if $|g| = 11$. Without loss of generality, we assume that $|g| = 11$. The lattice of subgroups H of G containing g and with nonzero Möbius function $\mu_G(H)$ is as follows:


Since $\mu_G(G) = 1$, $\mu_G(\mathrm{Alt}_{11}) = -1$, $\mu_G((M_{12})_i) = -1$ for $i \in \{1, 2\}$, $\mu_G(\mathrm{PSL}_2(11)) = 1$ and $\mu_G(11 : 5) = 1$, Proposition 2.2 yields $\delta(g) \equiv 1 \bmod 2$. In particular $\Gamma(G)$ is not Eulerian.

Suppose that $G = \text{Alt}_{23}$. Let $1 \neq g \in G$. By Proposition 2, $\delta(g)$ is even except possibly if $|g| = 23$. Without loss of generality, we assume that $|g| = 23$. The lattice of subgroups H of G containing g and with nonzero Möbius function $\mu_G(H)$ is as follows:

$$\text{Alt}_{23}$$

$$(M_{23})_1 \qquad\qquad (M_{23})_2$$

$$23 : 11$$

Since $\mu_G(G) = 1$, $\mu_G((M_{23})_i) = -1$ for $i \in \{1, 2\}$ and $\mu_G(23 : 11) = 1$, Proposition 2.2 yields $\delta(g) \equiv 1 \bmod 2$. In particular $\Gamma(G)$ is not Eulerian.

Suppose finally that $G = \text{Alt}_{24}$. Let $1 \neq g \in G$. By Proposition 2, $\delta(g)$ is even except possibly if $|g| = 23$. Without loss of generality, we assume that $|g| = 23$. The lattice of subgroups H of G containing g and with nonzero Möbius function $\mu_G(H)$ is as follows:

$$\text{Alt}_{24}$$

$$\text{Alt}_{23} \qquad (M_{24})_1 \qquad\qquad (M_{24})_2$$
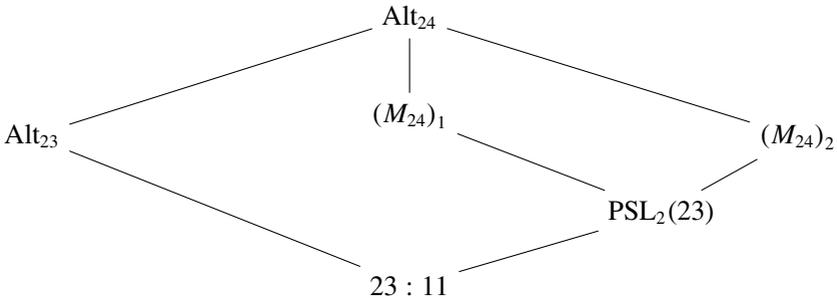
$$\text{PSL}_2(23)$$

$$23 : 11$$

Since $\mu_G(G) = 1$, $\mu_G(\text{Alt}_{23}) = -1$, $\mu_G((M_{24})_i) = -1$ for $i \in \{1, 2\}$, $\mu_G(\text{PSL}_2(23)) = 1$ and $\mu_G(23 : 11) = 1$, Proposition 2.2 yields $\delta(g) \equiv 1 \bmod 2$. In particular $\Gamma(G)$ is not Eulerian. $\qquad\square$

PROPOSITION 7.2. *Let $G = \text{Alt}_n$ where $n = p^a$ for some prime number p congruent to 3 modulo 4 and some positive integer a. Let $1 \neq g \in G$. Then $\delta(g)$ is odd if and only if $a = 1$ and $|g| = n$. In particular, $\Gamma(G)$ is Eulerian if and only if $a > 1$.*

Proof. If $n = 3$ then the result is obvious (see Proposition 4.1). We therefore assume that $n > 3$. If g does not belong to a proper primitive subgroup of G then Theorem 5.1 yields that $\delta(g)$ is even. Also if g is not an n-cycle or a is even then Proposition 2 yields that $\delta(g)$ is even. We therefore assume that g belongs

to a proper primitive subgroup of G, g is an n-cycle and a is odd. The cases $n \in \{7, 11, 23\}$ have been covered in Proposition 7.1, so we assume that $n = 19$ or $n > 23$. A maximal subgroup H of G containing g is clearly transitive, and is either imprimitive or primitive. If H is primitive then by [10, Theorem 1.3] and Lemmas 6.4–6.8 either there exist $d \in \mathbb{N}$ and a prime power $q = r^f$ (with r prime and $f \in \mathbb{N}$) such that $n = |g| = (q^d - 1)/(q - 1)$, $\mathrm{soc}(H) = \mathrm{PSL}_d(q)$ and $H = \mathrm{P\Gamma L}_d(q)$, or $n = p$ and H is the subgroup A_1 of G isomorphic to $p : (p - 1)/2$ and containing g.

Moreover, in the former case, by Lemma 6.1, d must be prime, $(d, q - 1) = 1$ and $\mathrm{PSL}_d(q) = \mathrm{PGL}_d(q)$. Note also that $n \neq 19$ (as there is no positive integer d and prime power q such that $19 = (q^d - 1)/(q - 1)$). We claim that $d > 2$. Suppose otherwise so that $d = 2$. Then $n = 1 + q$ and so, as n is odd, $r = 2$. Moreover since $n \equiv 3 \bmod 4$, f must be odd. Now $2^f + 1 \equiv 0 \bmod 3$. Following Zsigmondy's theorem, $2^f + 1$ is not a power of 3, unless $f \in \{1, 3\}$. However if $f \in \{1, 3\}$ then $n \in \{3, 9\}$, a contradiction, and so $d > 2$ as claimed.

Without loss of generality we can therefore assume that $n = 19$ or $n > 23$, moreover a is odd, g is an n-cycle and g belongs to a maximal primitive subgroup H of G. Furthermore if $\mathrm{soc}(H) = \mathrm{PSL}_d(q)$, we can assume that $n > 23$ and $d > 2$.

Suppose first that n cannot be written as $(q^d - 1)/(q - 1)$ for some prime number $d > 2$ and some prime power q. Then by assumption $n = p$ and so G has no imprimitive subgroup containing g. In particular the only maximal subgroup of G containing g is the subgroup $A_1 \cong p : (p - 1)/2$ of G containing g. Therefore, $\delta(g) = |G| - p(p - 1)/2$ and so, as $p \equiv 3 \bmod 4$, $\delta(g)$ is odd.

Suppose now that there exist a prime power q and a prime number $d > 2$ such that $n = (q^d - 1)/(q - 1)$. Note that $n > 23$. Let $K = N_G(\langle g \rangle)$. Then

$$|K| = n\phi(n)/2 = p^a \phi(p^a)/2 = p^a p^{a-1}(p - 1)/2 = p^a c$$

where $c = p^{a-1}(p - 1)/2$. In particular, as $p \equiv 3 \bmod 4$, $|K|$ is odd, and note that $K/\langle g \rangle$ is cyclic of order c. Also if $a = 1$ then K is the subgroup $A_1 \cong p : (p - 1)/2$ of G containing g.

For a positive integer b dividing c, let K_b be the unique subgroup of K containing g such that $K_b/\langle g \rangle$ is cyclic of order b. Note that for every subgroup L of K containing g, there exists a positive integer b dividing c such that $L = K_b$.

Clearly K is a transitive subgroup of G and $\mathrm{Stab}_K(1)$ is a cyclic group of order c, say $\mathrm{Stab}_K(1) = \langle h \rangle$.

Assume $a \neq 1$. Then $\mathrm{Stab}_K(1)$ is not a maximal subgroup of K. Indeed we have the following chain of pairwise distinct subgroups of K.

$$\mathrm{Stab}_K(1) \subset \langle g^{p^{a-1}}, h \rangle \subset K.$$

In particular if $a \neq 1$ then K is an imprimitive group.

Similarly, if $a \neq 1$ then K_b is imprimitive for every positive integer b dividing c. Let

$$\Omega = \{(q, d) : q \text{ is a power of a prime, } d \text{ is an odd prime, } n = (q^d - 1)/(q - 1)\}$$

and for $\omega \in \Omega$ let $\triangle_\omega$ be the family of maximal subgroups of G containing g and isomorphic to $\mathrm{P\Gamma L}_d(q)$. Let $\omega = (d, q) \in \Omega$. It is easy to check that K acts on $\triangle_\omega$ by conjugation. As $d > 2$, $\triangle_\omega$ is the union of two orbits under the action of K. As $|K|$ is odd each of these two orbits has odd length and so $\triangle_\omega$ is of even size for every $\omega \in \Omega$.

Also given $\omega \in \Omega$ and $M \in \triangle_\omega$, $K \cap M$, being the normalizer in M of a Singer cycle, is a maximal subgroup of M, see [**14**]. Moreover, as we are in the situation where $\mathrm{PSL}_d(q) = \mathrm{PGL}_d(q)$, every proper subgroup of M containing g is a subgroup of $K \cap M$.

Let M_1 and M_2 be the representatives of the two orbits of $\triangle_\omega$ under the action of K. Then, for $i \in \{1, 2\}$, $\mathrm{Stab}_K(M_i) = K \cap M_i = N_{M_i}(\langle g \rangle)$, and so $\mathrm{Stab}_K(M_i)$ is isomorphic to the normalizer in $\mathrm{P\Gamma L}_d(q)$ of a Singer cycle. In particular $|\mathrm{Stab}_K(M_1)| = |\mathrm{Stab}_K(M_2)|$ and so $|K \cap M_1| = |K \cap M_2|$. Therefore if $M \in \triangle_\omega$ then $M \cap K = K_{b_\omega}$ where b_ω is a positive integer dividing c and depends only on ω. It follows that given $\omega \in \Omega$ and a positive integer b dividing $p^{a-1}(p-1)/2$, the number of subgroups in $\triangle_\omega$ containing K_b is even.

Suppose $a = 1$. Then, since $n = p$ is prime, G has no imprimitive subgroups. Let b be a positive integer dividing c. We prove by induction on c/b that $\mu_G(K) = -1$ and $\mu_G(K_b)$ is even if $c/b > 1$. Since $a = 1$ and $n > 23$, by [**15**], K is a maximal subgroup of G and so $\mu_G(K) = -1$. Suppose $c/b > 1$. The subgroups of G properly containing K_b are:

(i) The group G. By definition $\mu_G(G) = 1$.

(ii) The subgroup K. Note that $\mu_G(K) = -1$.

(iii) The subgroups in $\triangle_\omega$ containing K_b for some $\omega \in \Omega$. Note that given $\omega \in \Omega$, the number of subgroups in $\triangle_\omega$ containing K_b is even and $\mu_G(M) = -1$ for every $M \in \triangle_\omega$. In particular

$$\sum_{\omega \in \Omega} \sum_{\substack{M \in \triangle_\omega \\ M \supset K_b}} \mu_G(M) \equiv 0 \mod 2.$$

(iv) The subgroups in $S_b = \{K_e : b \text{ properly divides } e\}$. By induction if $H \in S_b$ then $\mu_G(H) \equiv 0 \mod 2$. In particular, $\sum_{H \in S_b} \mu_G(H) \equiv 0 \mod 2$.

It follows that if $c/b > 1$ then $\mu_G(K_b) \equiv 0 \mod 2$ as claimed.

Therefore if $H \neq K$ is a subgroup of G containing g then either $|H| \equiv 0 \bmod 2$ or $\mu_G(H) \equiv 0 \bmod 2$. It follows from Proposition 2.2 that $\delta(g) \equiv -|K| \bmod 2$, and so $\delta(g)$ is odd.

Suppose finally that $a > 1$. We prove by induction on c/b that $\mu_G(K_b)$ is even. Since $a > 1$, K_b is an imprimitive subgroup of G and so K_b belongs to a maximal imprimitive subgroup of G. Let $I_1, \ldots, I_k$ be the maximal imprimitive subgroups of G containing K_b. Then, by the proof of Theorem 5.1, $\bigcap_{j=1}^{k} I_j$ has even order. In particular there is no positive integer e dividing c such that $\bigcap_{j=1}^{k} I_j \leqslant K_e$ and there is no $\omega \in \Omega$ such that $\bigcap_{j=1}^{k} I_j$ is a subgroup of an element of $\triangle_\omega$. The subgroups of G properly containing K_b are:

(i) The subgroups in $\triangle_\omega$ containing K_b for some $\omega \in \Omega$. Note that given $\omega \in \Omega$, the number of subgroups in $\triangle_\omega$ containing K_b is even and $\mu_G(M) = -1$ for every $M \in \triangle_\omega$. In particular

$$\sum_{\omega \in \Omega} \sum_{\substack{M \in \triangle_\omega \\ M \supset K_b}} \mu_G(M) \equiv 0 \quad \bmod 2.$$

(ii) The subgroups in $S_b = \{K_e : b \text{ properly divides } e\}$. By induction if $H \in S_b$ then $\mu_G(H) \equiv 0 \bmod 2$. In particular, $\sum_{H \in S_b} \mu_G(H) \equiv 0 \bmod 2$.

(iii) The subgroups in $S = \{H \leqslant G : \bigcap_{j=1}^{k} I_j \leqslant H\}$. We have $\sum_{H \in S} \mu_G(H) = 0$.

It follows that for every positive integer b dividing c, $\mu_G(K_b) \equiv 0 \bmod 2$ as claimed.

Now a subgroup of G containing g is either of even order or is equal to some K_b for some positive integer b dividing c. Therefore Proposition 2.2 yields that $\delta(g) \equiv 0 \bmod 2$. □

PROPOSITION 7.3. *Let $G = \mathrm{Alt}_n$ where $n = p + 1$ for some prime number p congruent to 3 modulo 4. Let $1 \neq g \in G$. Then $\delta(g)$ is odd if and only if $|g| = p$. In particular, $\Gamma(G)$ is not Eulerian.*

Proof. Following Proposition 4.1 we can assume without loss of generality that $n \geqslant 8$. Since the cases $n \in \{12, 24\}$ are treated in Proposition 7.1, we suppose that $n \in \{8, 20\}$ or $n \geqslant 32$.

Let D_g be a decomposition of g into disjoint cycles. We can assume that g is an r-element for some prime number $r < n$ with $r \equiv 3 \bmod 4$ and that in D_g there are no two cycles of same length as otherwise, by Proposition 2, $|N_G(\langle g \rangle)| \equiv 0 \bmod 2$ and $\delta(g)$ is even. Note that Lemma 6.3 yields that $|g| > n/2$.

If g does not belong to a proper primitive subgroup of G then Theorem 5.1 yields that $\delta(g)$ is even. We therefore suppose that g belongs to a proper primitive

subgroup H of G. By Lemma 6.4, H is either almost simple or H is affine. Suppose H is almost simple. By [**10**, Theorem 1.3] and Lemma 6.6, $\mathrm{soc}(H) = \mathrm{PSL}_2(p)$ and $|g| = p$. If H is of affine type then it follows from [**10**, Theorem 1.3] and Lemma 6.8 that there exists a positive integer d such that $n = 2^d$, $H \leqslant \mathrm{ASL}_d(2)$ and $|g| = p$. In particular $|g| = p$.

Suppose that there exists no positive integer d such that $n = 2^d$. The lattice of subgroups H of G containing g and with nonzero Möbius function $\mu_G(H)$ is as follows:
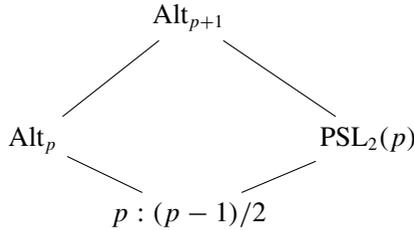
Since $\mu_G(G) = 1$, $\mu_G(\mathrm{Alt}_p) = -1$, $\mu_G(\mathrm{PSL}_2(p)) = -1$ and $\mu_G(p : (p-1)/2) = 1$, Proposition 2.2 yields $\delta(g) \equiv 1 \bmod 2$.

Finally, suppose that there exists a positive integer d such that $n = 2^d$. Note that p is a Mersenne prime and so, since $n > 4$, d is an odd prime and $2^{d-1} \equiv 1 \bmod d$.

Assume first that $n = 8$ so that $G = \mathrm{Alt}_8$. The lattice of subgroups H of G containing g and with nonzero Möbius function $\mu_G(H)$ is as follows:
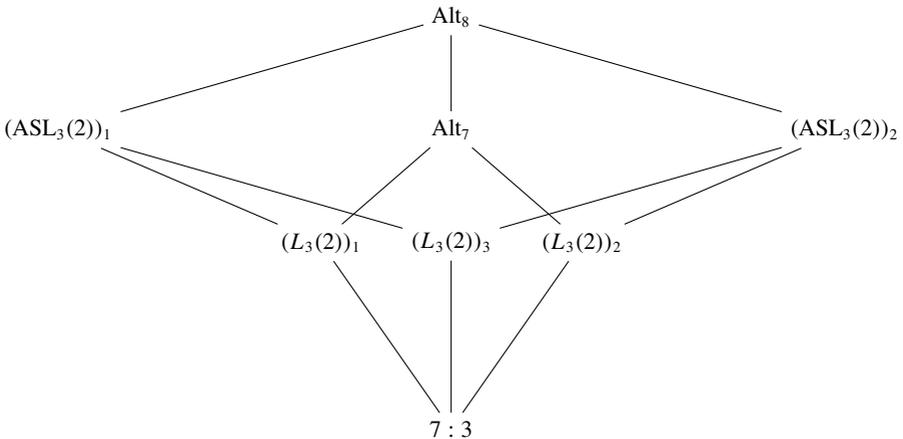
Using Proposition 2.2, we obtain $\delta(g) \equiv 1 \bmod 2$.

Assume now that $n \neq 8$. In particular $n \geqslant 32$. Now G has a unique maximal subgroup A_1 isomorphic to Alt_p and containing g and a unique maximal subgroup P_1 isomorphic to $\mathrm{PSL}_2(p)$ and containing g. Let $K = N_G(\langle g \rangle)$. Then $K = p : (p-1)/2$ and K is a subgroup of A_1 and P_1. Now G has also a maximal subgroup $H_1 \cong \mathrm{ASL}_d(2)$ containing g. Let $K_1 = K \cap H_1$ and $S_1 = A_1 \cap H_1$. Then S_1 is the unique subgroup of H_1 isomorphic to $\mathrm{SL}_d(2)$ and containing g, and $K_1 = p : d = P_1 \cap H_1$ is a maximal irreducible subgroup of S_1, namely the normalizer in S_1 of a Singer cycle of S_1. In fact G has

$$r = \frac{(p-1)}{2d}$$

maximal subgroups H_i, where $1 \leqslant i \leqslant r$, such that $H_i \cong \mathrm{ASL}_d(2)$ and H_i contains g. For $1 \leqslant i \leqslant r$, let $S_i = A_1 \cap H_i$. Then S_i is the unique subgroup of H_i isomorphic to $\mathrm{SL}_d(2)$ and containing g. Note that K_1 is a maximal irreducible subgroup of S_i. Now, for $1 \leqslant i, j \leqslant r, i \neq j$, we have $H_i \cap H_j = K_1$, $P_1 \cap H_i = K_1$ and $A_1 \cap H_i = S_i$. It follows that there are only two subgroups H of G of odd order containing g such that $\mu_G(H)$ is possibly nonzero, namely either $H = p : (p-1)/2$ or $H = p : d$. Moreover, $\mu_G(G) = \mu_G(p : (p-1)/2) = \mu_G(S_i) = 1$ for $1 \leqslant i \leqslant r$ and $\mu_G(A_1) = \mu_G(P_1) = \mu_G(H_i) = -1$ for $1 \leqslant i \leqslant r$. Hence $\mu_G(p : (p-1)/2) = 1$ and in fact $\mu_G(p : d) = 0$. Therefore, by Proposition 2.2, $\delta(g)$ is odd. $\quad\square$

We can now prove Theorem 3 for alternating groups.

Proof of Theorem 3 for alternating groups. The cases where n is a power of a prime congruent to 3 modulo 4 or $n - 1$ is a prime congruent to 3 modulo 4 have been covered (see Propositions 7.1–7.3).

Suppose now that n is not a power of a prime congruent to 3 modulo 4 or $n-1$ is not a prime congruent to 3 modulo 4. We need to show that $\delta(g)$ is even. We argue by contradiction and suppose that $\delta(g)$ is odd. By Theorem 5.1 g must belong to a maximal primitive subgroup H of Alt_n. By Proposition 2 there is a prime number p congruent to 3 modulo 4 and a positive integer k such that $|g| = p^k$. Moreover g has no two cycles of same length. Lemma 6.3 yields that $|g| > n/2$. By Lemma 6.4 H is almost simple or H is of affine type. Since n and $n - 1$ are not equal to a prime number congruent to 3 modulo 4, Lemma 6.8 yields that H is almost simple and Lemma 6.7 yields that there exist a prime power q and a positive integer $d \geqslant 2$ such that $\mathrm{soc}(H) = \mathrm{PSL}_d(q)$ and the action of H is on the set of points of the projective space $\mathrm{PG}_{d-1}(q)$. Since $n - 1$ is not a prime congruent to 3 modulo 4, Lemma 6.6 yields that $|g| = n$. Therefore $n = p^k$, contradicting the fact that n is not a power of a prime number congruent to 3 modulo 4. Hence $\delta(g)$ is even as required. $\quad\square$

Acknowledgements

References

[1] M. Aschbacher and R. Guralnick, 'Some applications of the first cohomology group', *J. Algebra* **90** (1984), 446–460.

[2] A. Basile, 'Second maximal subgroups of the finite alternating and symmetric groups', PhD Thesis, The Australian National University, 2001.

[3] G. Binder, 'The bases of the symmetric group', *Izv. Vyssh. Uchebn. Zaved. Mat.* **78** (1968), 19–25.

[4] T. Breuer, R. Guralnick and W. Kantor, 'Probabilistic generation of finite simple groups II', *J. Algebra* **320** (2008), 443–494.

[5] T. Breuer, R. Guralnick, A. Lucchini, A. Maróti and G. Nagy, 'Hamiltonian cycles in the generating graphs of finite groups', *Bull. Lond. Math. Soc.* **42** (2010), 621–633.

[6] J. Conway, R. Curtis, S. Norton, R. Parker and R. Wilson, *Atlas of Finite Groups* (Oxford University Press, Eynsham, 1985).

[7] E. Detomi and A. Lucchini, 'Profinite groups with multiplicative probabilistic zeta function', *J. Lond. Math. Soc.* **70** (2004), 165–181.

[8] J. Dixon and B. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics, 163 (Springer, New York, 1996).

[9] S. Guest, J. Morris, C. Praeger and P. Spiga, 'Affine transformations of finite vector spaces with large orders or few cycles', *J. Pure Appl. Algebra* **219** (2015), 308–330.

[10] S. Guest, J. Morris, C. Praeger and P. Spiga, 'On the maximum orders of elements of finite almost simple groups and primitive permutation groups', *Trans. Amer. Math. Soc.* **367** (2015), 7665–7694.

[11] R. Guralnick and W. Kantor, 'Probabilistic generation of finite simple groups', *J. Algebra* **234** (2000), 743–792.

[12] P. Hall, 'The Eulerian functions of a group', *J. Math. Oxford Ser.* **7** (1936), 134–151.

[13] T. Hawkes, I. Isaacs and M. Özaydin, 'On the Möbius function of a finite group', *Rocky Mountain J. Math.* **19** (1989), 1003–1034.

[14] W. Kantor, 'Linear groups containing a Singer cycle', *J. Algebra* **62** (1980), 232–234.

[15] M. Liebeck, C. Praeger and J. Saxl, 'A classification of the maximal subgroups of the finite alternating and symmetric groups', *J. Algebra* **111** (1987), 365–383.

[16] M. Liebeck, C. Praeger and J. Saxl, 'On the O'Nan–Scott theorem for finite primitive permutation groups', *J. Aust. Math. Soc.* **44** (1988), 389–396.

[17] A. Lucchini, 'The X-Dirichlet polynomial of a finite group', *J. Group Theory* **8** (2005), 171–188.

[18] G. Miller, 'On the groups generated by two operators', *Bull. Amer. Math. Soc.* **7** (1901), 424–426.

[19] C. Praeger, 'An O'Nan–Scott theorem for finite quasiprimitive permutation groups and an application to 2-arc transitive graphs', *J. Lond. Math. Soc.* **47** (1993), 227–239.

[20] C. Praeger, 'Finite quasiprimitive graphs', in *Survey in Combinatorics, 1997 (London)*, London Mathematical Society Lecture Note Series, 241 (Cambridge University Press, Cambridge, 1997), 65–85.

[21] R. Steinberg, 'Generators for simple groups', *Canad. J. Math.* **14** (1962), 277–283.