The invariably generating graph
of the alternating and symmetric groups

Daniele Garzoni*

Communicated by Timothy C. Burness

Abstract. Given a finite group G, the invariably generating graph of G is defined as the undirected graph in which the vertices are the nontrivial conjugacy classes of G, and two classes are adjacent if and only if they invariably generate G. In this paper, we study this object for alternating and symmetric groups. The main result of the paper states that if we remove the isolated vertices from the graph, the resulting graph is connected and has diameter at most 6.

1 Introduction

Given a finite group G and a subset $\{x_1, \ldots, x_t\}$ of G, we say that $\{x_1, \ldots, x_t\}$ *invariably generates* G if $\langle x_1^{g_1}, \ldots, x_t^{g_t} \rangle = G$ for every $g_1, \ldots, g_t \in G$. This concept was introduced by Dixon with motivations from computational Galois theory; see [5] for details. Note that invariable generation can be thought of as a property of conjugacy classes, rather than individual elements.

1.1 The invariably generating graph

Given a finite group G, we define the *invariably generating graph* $\Lambda(G)$ of G as follows. The vertices are the conjugacy classes of G different from $\{1\}$, and two vertices x^G and y^G are adjacent if and only if $\{x, y\}$ invariably generates G. The purpose of this paper is to initiate the study of this object for finite (almost) simple groups, and more precisely, for alternating and symmetric groups. It was proved by Kantor–Lubotzky–Shalev [12], and Guralnick–Malle [9] independently, that finite simple groups are invariably generated by two elements so that, in this case, $\Lambda(G)$ is nonempty. It is also known that S_n is invariably generated by two elements if and only if $n \neq 6$ (see [15, Proposition 4.10]). Set

$$\mathcal{P} = \left\{ \frac{q^d - 1}{q - 1} : q \text{ is a prime power and } d \geqslant 2 \right\}.$$

The first two results of the paper are the following.

Theorem 1.1. *Assume $n \geqslant 5$, and let $G \in \{A_n, S_n\}$. Then $\Lambda(G)$ does not have isolated vertices if and only if $G = A_n$ and n is a prime satisfying $n \notin \mathcal{P} \cup \{11, 23\}$ and $n \equiv -1 \bmod 12$.*

Theorem 1.2. *The following statements hold.*

(1) *Let (G_i) be a sequence of alternating or symmetric groups so that $|G_i| \to \infty$. Assume that, for every i, G_i is not alternating of prime degree. Then the number of isolated vertices of $\Lambda(G_i)$ tends to infinity.*

(2) *Assume n is a prime not contained in $\mathcal{P} \cup \{11, 23\}$. Then the number of isolated vertices of $\Lambda(A_n)$ is at most 2.*

In Theorem 1.1, we assumed $n \geqslant 5$. We will keep this assumption throughout the paper; see Lemma 2.15 for the remaining cases. For the sake of clarity, we mention that $\Lambda(A_{11})$ and $\Lambda(A_{23})$ have 5 and 6 isolated vertices, respectively (Lemma 3.2). The only case not addressed in Theorem 1.2 is $G = A_n$ with $n \in \mathcal{P}$ prime. In Remark 3.3, we will obtain a partial result, dealing with the case $n = (q^d - 1)/(q - 1)$ with $d \to \infty$.

Once Theorems 1.1 and 1.2 are proved, one may ask what happens if the isolated vertices are removed from $\Lambda(G)$. With this purpose, we define a graph $\Xi(G)$ which is obtained from $\Lambda(G)$ by removing the isolated vertices. The next result states that, except in case $G = S_6$, this graph is connected with bounded diameter (we already recalled that S_6 is not invariably generated by two elements, hence $\Xi(S_6)$ is the null graph).

Theorem 1.3. *Assume $n \geqslant 5$, and let $G \in \{A_n, S_n\}$, with $G \neq S_6$. Then $\Xi(G)$ is connected with diameter at most 6.*

In many cases, we prove better estimates on the diameter.

Theorem 1.4. *Assume $n \geqslant 5$. If $G = S_n$ and n is odd, or if $G = A_n$ and n is even, then $d(\Xi(G)) \leqslant 4$. If $G = A_n$ and $n \notin \mathcal{P}$ is prime, then $d(\Xi(G)) \leqslant 3$.*

The proofs of Theorems 1.3 and 1.4 rely on some recent results, proved in [11] and [8], which classify the primitive subgroups of S_n containing elements having certain cycle types. These results depend on the Classification of Finite Simple Groups.

The upper bound in Theorem 1.3 is attained since $d(\Xi(S_8)) = 6$ (Lemma 3.7). However, we conjecture that this can happen only for finitely many groups.

Conjecture 1.5. Let $G \in \{A_n, S_n\}$. If n is sufficiently large, then $d(\Xi(G)) \leqslant 4$.

In Section 4, we obtain a partial result towards a proof of this conjecture. It is interesting to observe that, in this partial result, we use the Prime Number Theorem, but we do not use the CFSG. See also Lemma 4.5, which establishes that $d(\Xi(S_n)) \geqslant 4$ for all primes $n \geqslant 7$, so the bound in Conjecture 1.5, if true, is attained infinitely often.

Theorem 1.3 suggests a natural question for all finite simple groups.

Question 1.6. Let G be a finite simple group. Is the graph $\Xi(G)$ connected?

1.2   Some context

The invariably generating graph is the analogue, for invariable generation, of the so-called *generating graph* $\Gamma(G)$ of a finite group G. This is defined as follows. The vertices are the nonidentity elements of G, and two vertices x and y are adjacent if and only if $\langle x, y \rangle = G$.

Many properties of generation of a finite simple group by two elements can be stated in terms of the generating graph. Guralnick and Kantor [10] proved that if G is a finite simple group, then, for every $1 \neq x \in G$, there exists $y \in G$ such that $\langle x, y \rangle = G$. Later, Breuer, Guralnick and Kantor [3] showed that if $1 \neq x_1, x_2 \in G$, then there exists $y \in G$ such that $\langle x_1, y \rangle = \langle x_2, y \rangle = G$. These properties can be stated respectively as follows: $\Gamma(G)$ has no isolated vertices, and it is connected with diameter at most 2.

Theorems 1.1 and 1.2 say that, for alternating and symmetric groups, the invariably generating graph has quite different properties; it usually has isolated vertices, and the number of isolated vertices usually grows as the order of the group grows.

On the other hand, Theorem 1.3 says that if we remove the isolated vertices, we obtain a graph which in some sense shares similarities with the generating graph $\Gamma(G)$.

1.3   An alternative definition

In light of Theorem 1.2, one could ask how the proportion of isolated vertices of $\Lambda(G)$ behaves as $|G|$ tends to infinity. The elementary approach used in the proof of Theorem 1.2 is not sufficient to address this problem. Here, however, one comment is in order. We have chosen the vertices of $\Lambda(G)$ to be the nontrivial conjugacy classes of G. One could define a graph $\Lambda_e(G)$ in which the vertices are the nontrivial *elements* of G, and two vertices are adjacent if and only if they invariably generate G. Of course, the property of connectedness and the value of the diameter are the same in the two graphs. However, when one counts the edges, or the vertices having certain properties, the situation can radically change. Indeed,

in $\Lambda_e(G)$, there is a dependence on the size of the conjugacy classes which does not exist in $\Lambda(G)$.

Probabilistic invariable generation has always been considered in terms of elements (cf. [5, 6, 13, 14]). Still, we believe it is worth exploring the problem of counting conjugacy classes – although, in this paper, we do not address any question of this kind.

2   Notation and preliminary results

In this section, we fix some notation, and we gather some preliminary lemmas and observations that we will use throughout the paper.

2.1   Notation

The vertices of our graphs are conjugacy classes of alternating and symmetric groups. We will identify conjugacy classes of S_n with their cycle type, i.e., we will represent conjugacy classes of S_n as partitions of n. We now introduce some terminology about partitions.

Let $H \leqslant S_n$, and let $\mathfrak{p}$ be a partition of n. We will say that $\mathfrak{p}$ *belongs to H*, or that $\mathfrak{p}$ *is contained in H*, if H contains elements with cycle type $\mathfrak{p}$. If C is the conjugacy class of S_n corresponding to $\mathfrak{p}$, this is equivalent to the condition $H \cap C \neq \emptyset$. Of course, this condition depends only on the S_n-conjugacy class of the subgroup H. Therefore, in the above terminology, we are allowed, if we wish, to replace H by its conjugacy class, and to say that $\mathfrak{p}$ belongs to the S_n-conjugacy class of H.

Let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be two partitions of n. If $\mathfrak{p}_1$ and $\mathfrak{p}_2$ both belong to H, we will say that $\mathfrak{p}_1$ and $\mathfrak{p}_2$ *share H*. When $\mathfrak{p} \in S_i \times S_{n-i}$, with $1 \leqslant i < n$, we will say that i *is a partial sum in $\mathfrak{p}$*. This is indeed equivalent to the condition that the integer i can be written as the sum of some parts of $\mathfrak{p}$. In a partition, i^m will mean m parts of length i. Therefore, $(a_1^{m_1}, a_2^{m_2}, \ldots, a_t^{m_t})$ will mean m_1 parts of length a_1, m_2 parts of length a_2, $\ldots$, and m_t parts of length a_t.

Occasionally, given a partition $\mathfrak{p}$ and a positive integer i, we will write $\mathfrak{p}^i$ to denote "the i-th power of $\mathfrak{p}$", namely the partition obtained by replacing each part of length ℓ by d parts of length ℓ/d, where $d = (\ell, i)$. Note that if $x \in S_n$ has cycle type $\mathfrak{p}$, then x^i has cycle type $\mathfrak{p}^i$.

Finally, we define

$$\mathcal{P} = \left\{ \frac{q^d - 1}{q - 1} : q \text{ is a prime power and } d \geqslant 2 \right\}.$$

2.2   Maximal overgroups of certain elements

Most of the arguments will rely heavily on the knowledge of the maximal over-groups of certain elements in S_n; specifically, cycles, or elements having few orbits in the natural action on n points. The intransitive maximal subgroups are easily determined. For convenience, we now isolate some elementary observations regarding transitive imprimitive subgroups, while then moving to the more difficult case of primitive subgroups. We use some of the language introduced in the previous subsection. The following two lemmas are a consequence of [2, Theorem 2.5].

Lemma 2.1. *Let n be a natural number, m a nontrivial divisor of n and $1 \leqslant i < n$. The partition (a_1, a_2) belongs to $S_m \wr S_{n/m}$ if and only if either m divides a_1 or n/m divides a_1.*

Proof. If (a_1, a_2) belongs to $S_m \wr S_{n/m}$, the induced permutation on the blocks has at most two cycles. If it has two cycles, then m divides a_1. If it is an (n/m)-cycle, then n/m divides a_1. The converse implication is proved in the same way.   □

Lemma 2.2. *Let n be a natural number, m a nontrivial divisor of n and $1 \leqslant i < n$. The partition (a_1, a_2, a_3) belongs to $S_m \wr S_{n/m}$ if and only if one of the following conditions is satisfied:*

(a) *m divides a_i for every i;*

(b) *n/m divides a_i for every i;*

(c) *there exist $1 \leqslant t < n/m$ and $i \neq j \in \{1, 2, 3\}$ such that*

$$a_k = tb_k \quad for\ k = i, j, \quad with\ b_i + b_j = m.$$

Proof. Similar to the previous lemma. In case (a), the induced permutation on the blocks has cycle type $(a_1/m, a_2/m, a_3/m)$. In case (b), it is an (n/m)-cycle. In case (c), it has cycle type $(t, a_\ell/m)$, where $\ell \in \{1, 2, 3\} \setminus \{i, j\}$.   □

We now move to primitive subgroups. Our main tool is a theorem which classifies the primitive subgroups of S_n containing a cycle, and which relies on the CFSG. This should be seen as a generalization of a classical theorem of Jordan (see e.g. [16, Theorem 13.9]) stating that there are no proper primitive subgroups of S_n different from A_n containing a cycle of prime length fixing at least 3 points. Since we will apply this result several times, for convenience, we report here the statement.

Theorem 2.3 ([11]). *Let G be a primitive permutation group of finite degree n, not containing the alternating group A_n. Suppose that G contains a cycle fixing k*

points, where $0 \leqslant k \leqslant n - 2$. *Then one of the following holds:*

(1) $k = 0$ *and*

    (a) *either* $C_p \leqslant G \leqslant \mathrm{AGL}_1(p)$ *with* $n = p$ *prime,*

    (b) *or* $\mathrm{PGL}_d(q) \leqslant G \leqslant \mathrm{P\Gamma L}_d(q)$ *with* $n = (q^d - 1)/(q - 1)$ *and* $d \geqslant 2$ *for some prime power* q,

    (c) *or* $G = \mathrm{PSL}_2(11)$, M_{11} *or* M_{23} *with* $n = 11, 11$ *or* 23, *respectively.*

(2) $k = 1$ *and*

    (a) *either* $\mathrm{AGL}_d(q) \leqslant G \leqslant \mathrm{A\Gamma L}_d(q)$ *with* $n = q^d$ *and* $d \geqslant 1$ *for some prime power* q,

    (b) *or* $G = \mathrm{PSL}_2(p)$ *or* $\mathrm{PGL}_2(p)$ *with* $n = p + 1$ *for some prime* $p \geqslant 5$,

    (c) *or* $G = M_{11}$, M_{12} *or* M_{24} *with* $n = 12, 12$ *or* 24, *respectively.*

(3) $k = 2$ *and* $\mathrm{PGL}_2(q) \leqslant G \leqslant \mathrm{P\Gamma L}_2(q)$ *with* $n = q + 1$ *for some prime power* q.

Note that the statement implies that there are no proper primitive subgroups of S_n different from A_n containing a cycle fixing at least 3 points, generalizing indeed Jordan's theorem. We note the following immediate consequence.

Corollary 2.4. *Assume* $x \in S_n$ *is such that a suitable power of* x *is a nontrivial cycle fixing at least* 3 *points. Then* x *does not lie in proper primitive subgroups of* S_n *different from* A_n.

We also mention that we will make essential use of the main result from [8], which classifies the primitive subgroups of S_n containing an element having at most 4 cycles.

We will shortly apply the previous results to certain elements (or partitions) of particular interest to us.

2.3 Conjugacy classes of A_n

If a partition of n is made of distinct odd parts, the corresponding S_n-conjugacy class splits into two A_n-conjugacy classes (and vice versa), giving rise to two vertices of $\Lambda(A_n)$. Often, this does not represent a serious change; the following technical lemmas give conditions under which the two vertices may be essentially thought of as a unique vertex.

Lemma 2.5. *Let* $x \in A_n$, *and let* $H \leqslant S_n$ *be such that* $H^{A_n} = H^{S_n}$. *Then* H *contains elements belonging to* x^{A_n} *if and only if it contains elements belonging to* $(x')^{A_n}$ *for every* $x' \in x^{S_n}$.

Proof. Assume $x^z \in H$ with $z \in A_n$, and assume $x' = x^{zg}$ with $g \in S_n$. Then $x' = x^{zg} \in H^g = H^h$ for some $h \in A_n$ by hypothesis, hence $(x')^{h^{-1}} \in H$. This concludes the proof. □

Notation 2.6. Assume $x, y \in A_n$ are such that $(x')^{A_n}$ is adjacent to $(y')^{A_n}$ in $\Lambda(A_n)$ for any $x' \in x^{S_n}$ and for any $y' \in y^{S_n}$. Under these assumptions, we say with slight abuse of notation that x^{S_n} is adjacent to y^{S_n} in $\Lambda(A_n)$.

This notation will be convenient, as we will represent S_n-conjugacy classes as partitions, and we will be allowed to say that "a partition $\mathfrak{q}$ is adjacent to a partition $\mathfrak{p}$", rather than "any A_n-conjugacy class of elements with cycle type $\mathfrak{q}$ is adjacent to any A_n-conjugacy classes of elements with cycle type $\mathfrak{p}$". We will now see that, in many cases, the assumption of Notation 2.6 is satisfied.

Lemma 2.7. *Let $x \in A_n$, and assume $\langle x \rangle^{A_n} = \langle x \rangle^{S_n}$. Let $y \in A_n$. Then x^{A_n} is adjacent in $\Lambda(A_n)$ to y^{A_n} if and only if x^{S_n} and y^{S_n} are adjacent (in the terminology of Notation* 2.6).

Proof. Choose $x' \in x^{S_n}$. We show first that if y^{A_n} is not adjacent to x^{A_n}, then y^{A_n} is not adjacent to $(x')^{A_n}$. By assumption, we can write $x' = (x^i)^z$ for some integer i and for some $z \in A_n$. Again by assumption, $\{x^{g_1}, y^{g_2}\} \subseteq H$ for some $g_1, g_2 \in A_n$, and for some proper subgroup H of A_n. Then

$$(x')^{z^{-1}g_1} = (x^i)^{g_1} = (x^{g_1})^i \in H,$$

whence $\{(x')^{z^{-1}g_1}, y^{g_2}\} \subseteq H$ and y^{A_n} is not adjacent to $(x')^{A_n}$, as required.

Assume now $y' \in y^{S_n}$. We show that if y^{A_n} is not adjacent to x^{A_n}, then $(y')^{A_n}$ is not adjacent to x^{A_n}. This will conclude the proof. We may assume $y^{A_n} \neq (y')^{A_n}$ and $x^{A_n} \neq x^{S_n}$; otherwise, the statement is easy. Choose $x' \in x^{S_n} \setminus x^{A_n}$. By the previous paragraph, if y^{A_n} is not adjacent to x^{A_n}, then it is not adjacent to $(x')^{A_n}$ so that $\{x^{g_1}, y^{g_2}\} \subseteq H$ for some proper subgroup H of A_n, some $g_1 \in S_n \setminus A_n$ and $g_2 \in A_n$. Then $\{x, y^{g_2 g_1^{-1}}\} \subseteq H^{g_1^{-1}}$, and since $y^{g_2 g_1^{-1}}$ is A_n-conjugate of y', the proof is concluded. □

We now apply the previous considerations to certain elements and subgroups of S_n.

Lemma 2.8. *Let H be a maximal subgroup of S_n which is either intransitive, or transitive and imprimitive. Then $H^{A_n} = H^{S_n}$.*

Proof. We may assume $n \geqslant 3$. We have $H^{A_n} = H^{S_n}$ if and only if $N_{S_n}(H) \not\leqslant A_n$. In our case, $H \not\leqslant A_n$ since every maximal intransitive or imprimitive subgroup of S_n contains transpositions. □

Lemma 2.9. *Assume $x \in A_n$ belongs to no proper primitive subgroup of S_n different from A_n. Let $y \in A_n$. Then x^{A_n} and y^{A_n} are adjacent in $\Lambda(A_n)$ if and only if x^{S_n} and y^{S_n} are adjacent (in the terminology of Notation 2.6).*

Proof. By assumption, x lies in no proper primitive subgroups different from A_n. Therefore, x^{A_n} is adjacent to y^{A_n} if and only if, for every $g_1, g_2 \in A_n$, $\langle x^{g_1}, y^{g_2} \rangle$ is primitive or, equivalently, is not contained in intransitive or imprimitive maximal subgroups. By Lemmas 2.5 and 2.8, this condition depends only on the cycle type of the elements, rather than on their A_n-conjugacy class. The lemma follows. $\square$

Lemma 2.10. *Let $2 \leqslant i \leqslant n/2$ be coprime with n. Then $(i, n - i)$ does not belong to proper primitive subgroups different from A_n, and does not belong to transitive imprimitive subgroups.*

Proof. The fact that $(i, n - i)$ does not lie in imprimitive subgroups follows from Lemma 2.1. Regarding primitive subgroups, $(i, n - i)^{n-i} = (i, 1^{n-i}) \neq (1^n)$, and $n - i \geqslant 3$ (the conditions on i imply $n \geqslant 5$); hence the statement follows from Corollary 2.4. $\square$

Theorem 2.3 can be used to generalize the previous lemma to the case $i = 1$; one just needs to take care of some specific examples of primitive subgroups. The following easy lemma will be used with this purpose.

Lemma 2.11. *Let q be a prime power and d a positive integer.*

(1) *An element of $\mathrm{AGL}_d(q)$, in the natural action on q^d points, either is a derangement, or fixes a number of points equal to q^s for some $0 \leqslant s \leqslant d$.*

(2) *Assume $g \in \mathrm{P\Gamma L}_2(q)$ fixes at least 3 points in the natural action on $q + 1$ points. Then g fixes a number of points having the same parity of $q + 1$. Moreover, if $g \in \mathrm{PGL}_2(q)$, then $g = 1$.*

Proof. (1) If $g \in \mathrm{AGL}_d(q)$ fixes some point, we may assume that it fixes 0. Hence, $g \in \mathrm{GL}_d(q)$. Now just observe that the set of fixed points of an element of $\mathrm{GL}_d(q)$ is an $\mathbf{F}_q$-subspace of $\mathbf{F}_q^d$.

(2) Consider $\mathrm{P\Gamma L}_2(q)$ acting (on the right) on the set Ω of 1-dimensional subspaces of $\mathbf{F}_q^2$. Write $q = p^r$ with p prime. For $\phi \in \mathrm{Gal}(\mathbf{F}_q/\mathbf{F}_p)$, denote by f_ϕ the permutation of Ω induced by the mapping $(\lambda_1, \lambda_2) \mapsto (\lambda_1^\phi, \lambda_2^\phi)$ of $\mathbf{F}_q^2$. Then we may express each element $g \in \mathrm{P\Gamma L}_2(q)$ as $g = x f_\phi$, where $x \in \mathrm{PGL}_2(q)$ and $\phi \in \mathrm{Gal}(\mathbf{F}_q/\mathbf{F}_p)$.

Note that $\mathrm{P\Gamma L}_2(q)$ is 3-transitive on Ω. Hence, if $g = x f_\phi \in \mathrm{P\Gamma L}_2(q)$ fixes at least 3 points, we may assume that it fixes $\langle (1, 0) \rangle$, $\langle (0, 1) \rangle$ and $\langle (1, 1) \rangle$. It follows

that $x = 1$ and $g = f_\phi$. Then g fixes $p^\ell + 1$ points, where ℓ is a divisor of r; in particular, it fixes a number of points having the same parity of $q + 1$. Moreover, if $g \in \mathrm{PGL}_2(q)$, then $f_\phi = 1$. The lemma is proved. $\quad\square$

Lemma 2.12. *Assume n is either an odd prime, or $n \equiv 3 \bmod 4$. Assume $x \in A_n$ is an n-cycle. Then $\langle x \rangle^{A_n} = \langle x \rangle^{S_n}$.*

Proof. If $n \geqslant 3$ is an odd integer, then an n-cycle is normalized by elements having cycle type $(1, 2^{(n-1)/2})$. If n is an odd prime, then an n-cycle is normalized by an $(n - 1)$-cycle. In particular, if x is as in the statement, then $\mathrm{N}_{S_n}(\langle x \rangle) \not\leqslant A_n$, from which $\langle x \rangle^{A_n} = \langle x \rangle^{S_n}$. $\quad\square$

We deduce another consequence of the previous lemmas.

Lemma 2.13. *Assume $n \geqslant 4$, and let $x \in A_n$. Then, for every $g \in S_n$, x^{A_n} and $(x^g)^{A_n}$ are not adjacent in $\Lambda(A_n)$.*

Proof. By Lemma 2.8, we may assume that x is not contained in intransitive or imprimitive subgroups. It follows that n is prime and x is an n-cycle. The statement follows then by Lemma 2.12. $\quad\square$

This lemma suggests a natural question for all finite simple groups.

Question 2.14. Let G be a finite simple group. Let $x \in G$, and let $\sigma \in \mathrm{Aut}(G)$. Is it possible that $\{x, x^\sigma\}$ invariably generates G?

It is easy to check that the statement is true for $G = A_6$, in which case, S_6 has index two in $\mathrm{Aut}(G)$. This, together with Lemma 2.13, implies that the question has a negative answer for $G = A_n$.

2.4 Small degrees

The main theorems are stated for $n \geqslant 5$. For completeness, we address here the cases of degree $n \leqslant 4$. We assume $n \geqslant 3$ in order to avoid trivialities.

Lemma 2.15. *Let $3 \leqslant n \leqslant 4$, and assume $G \in \{A_n, S_n\}$. Then $\Lambda(G)$ has isolated vertices if and only if $G = S_4$. Moreover, $\Xi(G)$ is connected with diameter at most 2.*

Proof. This is an easy check. The graphs $\Xi(A_3)$, $\Xi(S_3)$, $\Xi(S_4)$ have diameter 1, while $\Xi(A_4)$ has diameter 2; the two classes of 3-cycles are connected by a path of length 2 passing through the class (2^2). In $\Lambda(S_4)$, the vertices corresponding to $(1^2, 2)$ and (2^2) are isolated. $\quad\square$

3 Proofs

In this section, we prove the theorems stated in the introduction.

3.1 Proof of Theorems 1.1 and 1.2

We begin with a lemma which proves Theorem 1.2 (2) and the "if" part of Theorem 1.1.

Lemma 3.1. *Let $n \geq 5$ be an odd prime. Then $(1, 2^{(n-1)/2})$ and $(1, 3^{(n-1)/3})$ are isolated in $\Lambda(A_n)$ (when they make sense and are even permutations). If $n \notin \mathcal{P} \cup \{11, 23\}$, then there are no other isolated vertices in $\Lambda(A_n)$.*

Proof. The two mentioned vertices are not adjacent to (n) (this terminology makes sense by Lemma 2.7, Lemma 2.12 and Notation 2.6) because they are contained in $\mathrm{AGL}_1(n)$. Therefore, they might be adjacent only to some A_n-conjugacy class with cycle type $(a_1, \ldots, a_t)$, with $t \geq 3$. Every $1 \leq i \leq (n-1)/2$ is a partial sum in $(1, 2^{(n-1)/2})$, so this vertex is isolated (recall Lemmas 2.8 and 2.5), and the values of i that are not partial sums in $(1, 3^{(n-1)/3})$ are exactly those that satisfy $i \equiv 2 \bmod 3$. If $a_1, a_2 \equiv 2 \bmod 3$, then $a_1 + a_2 \equiv 1 \bmod 3$, so one among a_1, a_2 and $a_1 + a_2$ is a partial sum. We conclude that $(1, 3^{(n-1)/3})$ is indeed isolated.

Assume now $n \notin \mathcal{P} \cup \{11, 23\}$. Let x^{A_n} be a vertex of $\Lambda(A_n)$ different from the two above; we want to show it is not isolated. If $x \notin \mathrm{AGL}_1(n)$, we deduce from Theorem 2.3 that x^{A_n} is adjacent to (n). On the other hand, if $x \in \mathrm{AGL}_1(n)$, then either it is an n-cycle, or it has cycle type $(1, t^{(n-1)/t})$, with $t \geq 4$. As just remarked, a class of n-cycles is not isolated. If $t \geq 5$, by Corollary 2.4, x^{A_n} is adjacent to $(2^2, n-4)$. If $t = 4$, for the same reason, x^{A_n} is adjacent to $(3^2, n-6)$.
□

For the sake of clarity, we deal with the cases $n = 11, 23$.

Lemma 3.2. *The graphs $\Lambda(A_{11})$ and $\Lambda(A_{23})$ have 5 and 6 isolated vertices, respectively.*

Proof. Recall Theorem 2.3. Let $n \in \{11, 23\}$. Let $1 \neq x \in A_n$. If x does not belong to M_{11} (for $n = 11$) and M_{23} (for $n = 23$), the same argument as in the previous lemma shows that x^{A_n} is adjacent to (n) (note that $\mathrm{PSL}_2(11)$ can be embedded in M_{11}). Inspection (using for instance GAP) shows that if $n = 11$ and $1 \neq x \in M_{11}$, then x^{A_n} belongs to

$$\{(1^3, 2^4), (1^3, 4^2), (1^2, 3^3), (2, 3, 6), (1, 2, 8)\}.$$

These are not adjacent to (n) because of M_{11}. By looking at partial sums, we see

that these are all isolated. If $n = 23$ and $1 \neq x \in M_{23}$, then either x^{A_n} is adjacent to one between $(2^2, 19)$ and $(3^2, 17)$, or x^{A_n} belongs to

$$\{(1^5, 3^6), (1^3, 5^4), (1^7, 2^8), (1, 2^2, 3^2, 6^2), (1^3, 2^2, 4^4), (1, 2, 4, 8^2)\}.$$

These are all isolated for the same reason as above.   □

We are now ready to prove Theorems 1.1 and 1.2.

Proof of Theorems 1.1 *and* 1.2. In the proof, we will use Lemmas 2.5, 2.7 and 2.8 with no further mention. Recall also Notation 2.6.

We begin with Theorem 1.2. Item (2) follows from Lemma 3.1; hence we focus on item (1). Let $G = A_n$ or S_n, with n nonprime if $G = A_n$. For every n, we will define I_n, a subset of the set of isolated vertices of $\Lambda(G)$, whose cardinality, as $n \to \infty$, goes to infinity. This will prove Theorem 1.2. For every m, denote by p_m^E the set of all partitions of m different from (1^m) which correspond to even permutation.

We first assume that, whenever n is odd, $G = S_n$. Define I_n as the set of all partitions of n of the form $(1^{\lfloor n/2 \rfloor}, \mathfrak{p})$, where $\mathfrak{p}$ is whatsoever partition of $p_{\lceil n/2 \rceil}^E$.

Let $\mathfrak{q} \in I_n$. Every $1 \leqslant i \leqslant n/2$ is a partial sum, so $\mathfrak{q}$ is not adjacent to classes of elements with at least two cycles. If n is even, then $\mathfrak{q}$ is not adjacent to (n) since $n/2$ is a partial sum in $\mathfrak{q}$, hence $\mathfrak{q} \in S_{n/2} \wr S_2$. If n is odd, then $G = S_n$, and $\mathfrak{q}$ is not adjacent to (n) since $\mathfrak{q}$ corresponds to even permutations. Therefore, I_n consist of isolated vertices. Clearly, the size of I_n goes to infinity as $n \to \infty$.

Assume now that $G = A_n$ and n is odd and not prime. Fix n, and let p_n be the smallest prime divisor of n. Define I_n as the set of all partitions of n of the form $(1^{n(p_n-1)/p_n}, \mathfrak{p})$, where $\mathfrak{p}$ is any partition of p_{n/p_n}^E.

If $\mathfrak{q} \in I_n$, then $\mathfrak{q} \in S_{n/p_n} \wr S_{p_n}$; the first $p_n - 1$ blocks are fixed pointwise. Therefore, $\mathfrak{q}$ is not adjacent to (n). Moreover, every $1 \leqslant i \leqslant n/2$ is a partial sum, so $\mathfrak{q}$ is not adjacent to classes of elements having at least 2 cycles. It follows that $\mathfrak{q}$ is isolated. Note now that $n/p_n \geqslant \sqrt{n}$; hence the size of I_n goes to infinity as $n \to \infty$. This concludes the proof of Theorem 1.2.

We now move to Theorem 1.1. Note that Lemma 3.1 proves the "if" part. We now prove the "only if" part. Assume first that n is prime and $G = A_n$. If $n \not\equiv -1 \bmod 12$, by Lemma 3.1, there are isolated vertices in $\Lambda(A_n)$. The cases $n = 11, 23$ have been considered in Lemma 3.2. If $n = (q^d - 1)/(q - 1)$, let x be any involution lying in a subgroup of S_n conjugate to $\mathrm{P\Gamma L}_d(q)$. The fact that n is odd implies that every $1 \leqslant i \leqslant n/2$ is a partial sum in (the cycle type of) x; hence x^{A_n} might only be adjacent to a class of n-cycles. However, this does not happen because of the containment in $\mathrm{P\Gamma L}_d(q)$. Therefore, x^{A_n} is isolated.

The case $G = A_n$ with n prime is therefore proved. For the remaining cases, we apply what we proved for Theorem 1.2. We define $\mathfrak{q} = (1^{n-3}, 3)$. This partition

belongs to I_n, as defined in this proof; hence it is an isolated vertex of $\Lambda(G)$. This concludes the proof.   □

Remark 3.3. The unique case not discussed in Theorem 1.2 is the case $G = A_n$ and $n \in \mathcal{P}$ prime. We obtain here the partial result that if $n_i = (q^{d_i} - 1)/(q - 1)$ is prime and $d_i \to \infty$, then the number of isolated vertices of $\Lambda(A_{n_i})$ tends to infinity. Note that since n_i is prime, d_i must be prime. To establish whether infinitely many such primes (i.e., primes d such that $(q^d - 1)/(q - 1)$ is prime for some prime power q) do actually exist, however, is a hard open problem in number theory; see for instance [4].

Assume first $n = (q^d - 1)/(q - 1)$ with q (and d) odd. The action of $\mathrm{PGL}_d(q)$ on the 1-dimensional subspaces of $\mathbf{F}_q^d$ gives an embedding $\mathrm{PGL}_d(q) < S_n$. For every $1 \leqslant r < d/2$, let $x = x(r)$ be a diagonal matrix of $\mathrm{GL}_d(q)$ with 1's and -1's on the diagonal, and assume the number of -1's is r. Let $\bar{x}$ denote the image of x in $\mathrm{PGL}_d(q) < S_n$. Then $\bar{x}$ has $(q^r + q^{d-r} - 2)/(q - 1)$ fixed points. In particular, any two distinct $1 \leqslant r < d/2$ give rise to elements of S_n which have a different number of fixed points, and which therefore belong to different S_n-conjugacy classes. It is easy to check that the element $\bar{x}$ arising in this way belongs to A_n. The number of possibilities for r in order to obtain such an element is $(d - 1)/2$. As remarked in the previous proof, $(\bar{x})^{A_n}$ is isolated in $\Lambda(A_n)$; therefore, the number of isolated vertices of $\Lambda(A_n)$ is at least $(d - 1)/2$.

Assume now q is even. For every $1 \leqslant \ell \leqslant d/2$, consider a unipotent element $x = x(\ell)$ of $\mathrm{SL}_d(q)$ with ℓ Jordan blocks of size 2, and with the other Jordan blocks of size 1. This is an involution of $\mathrm{SL}_d(q)$. Denote again by $\bar{x}$ the image of x in $\mathrm{PSL}_d(q) < S_n$. Then $\bar{x}$ has $(q^{d-\ell} - 1)/(q - 1)$ fixed points; hence any two distinct $1 \leqslant \ell \leqslant d/2$ give rise to elements belonging to different S_n-conjugacy classes. Moreover, $\bar{x} \in A_n$ (unless $(q, d) = (2, 2)$, but recall we are assuming $n \geqslant 5$), and $(\bar{x})^{A_n}$ is isolated in $\Lambda(A_n)$. Hence the number of isolated vertices of $\Lambda(A_n)$ is at least $(d - 1)/2$.

3.2 Proof of Theorems 1.3 and 1.4

In this subsection, we prove Theorems 1.3 and 1.4.

One brief comment about the terminology we will adopt. The proofs will begin with a sentence of the type "Let $\mathfrak{p}$ be a vertex of $\Xi(G)$", without any preliminary consideration showing that $\Xi(G)$ is not the null graph. However, along the proof suitable edges will be exhibited in $\Lambda(G)$ so that the initial choice of $\mathfrak{p}$ will be licit. (In other words, we are saying that, although we will not state it explicitly, in the proofs, it will be shown that the groups are invariably generated by two elements.)

We begin by proving Theorem 1.4 (in two separate results).

Theorem 3.4. *Assume $n \geqslant 5$ is a prime and $n \notin \mathcal{P}$. Then $\Xi(A_n)$ is connected and $d(\Xi(A_n)) \leqslant 3$.*

Proof. Let $x \in A_n$, and assume x^{A_n} is a vertex of $\Xi(A_n)$. If $n \neq 11, 23$, in the proof of Lemma 3.1, we showed that x^{A_n} is adjacent to one among (n), $(2^2, n - 4)$ and $(3^2, n - 6)$ (see Lemma 2.12). These vertices are pairwise adjacent by Corollary 2.4; hence we have indeed $d(\Xi(A_n)) \leqslant 3$. If $n = 11$ or 23, we observed in the proof of Lemma 3.2 that a class inside M_{11} or M_{23} is either isolated, or adjacent to one between $(2^2, n - 4)$ and $(3^2, n - 6)$. Therefore, by Corollary 2.4, also in this case, $d(\Xi(A_n)) \leqslant 3$. □

For a later use, we point out that the same estimate holds for the groups A_{13} and A_{17}.

Assume $n = 13 = (3^3 - 1)/(3 - 1)$. Inspection shows that every class lying in $\mathrm{PGL}_3(3)$ is either isolated or adjacent to $(3^3, 7)$; hence $d(\Xi(A_{13})) \leqslant 3$ by the same argument as in the proof of the previous theorem. Assume finally that $n = 17 = 16 + 1$. Here every class lying in $\mathrm{P\Gamma L}_2(16)$ is either isolated or adjacent to one between $(3^2, 11)$ and $(4^2, 9)$. It is easy to deduce that $d(\Xi(A_{17})) \leqslant 3$.

Theorem 3.5. *Let $n \geqslant 5$ be an integer.*

(1) *If n is odd, then $\Xi(S_n)$ is connected and $d(\Xi(S_n)) \leqslant 4$.*

(2) *If n is even, then $\Xi(A_n)$ is connected and $d(\Xi(A_n)) \leqslant 4$.*

Proof. (1) Let $\mathfrak{p}$ be a vertex of $\Xi(S_n)$. Assume $\mathfrak{p}$ is not adjacent to $(i, n - i)$ for any $2 \leqslant i \leqslant n/2$ coprime with n. Then, by Lemma 2.10, every such i is a partial sum in $\mathfrak{p}$. Since $\mathfrak{p}$ is a vertex of $\Xi(S_n)$, $\mathfrak{p}$ will be adjacent to some vertex $\mathfrak{q}$. Necessarily, no $2 \leqslant i \leqslant n/2$ coprime with n is a partial sum in $\mathfrak{q}$. Hence, again by Lemma 2.10, $\mathfrak{q}$ is adjacent to $(i, n - i)$ for every such i.

Now note that the $(i, n - i)$'s, with i as above, are pairwise adjacent. From this, it follows that, for any fixed $2 \leqslant i \leqslant n/2$ coprime with n, any vertex $\mathfrak{p}$ of $\Xi(S_n)$ has distance at most 2 from $(i, n - i)$. This concludes the proof.

(2) The statement for $n = 6$ can be checked explicitly; hence we assume $n \geqslant 8$. Then the proof is identical to (1). Recall Lemmas 2.5 to 2.10, and Notation 2.6. □

Now we move to the proof of the general case, i.e., Theorem 1.3. We are left with symmetric groups of even degree and alternating groups of odd degree.

In Theorem 3.5, the strategy was to look for edges with conjugacy classes of elements having two cycles. This approach is not available anymore. Indeed, in alternating groups of odd degree, elements with two cycles do not exist, and in symmetric groups of even degree, such elements belong to A_n; hence one must

take care of the parity of elements when dealing with generation. For these elementary reasons, our strategy will be to look for edges with elements having three cycles. This is where we will make use of [8] which, as already mentioned in the introduction, classifies the primitive permutation groups having elements with at most four cycles.

Theorem 3.6. *Let $n \geq 8$ be an even integer. Then $\Xi(S_n)$ is connected, and we have $d(\Xi(S_n)) \leq 6$.*

Proof. We first assume $n \geq 12$ and consider the remaining cases at the end of the proof. Let $\mathfrak{p}$ and $\mathfrak{q}$ be two vertices of $\Xi(S_n)$ joined by an edge. One of the two, say $\mathfrak{p}$, must correspond to odd permutations. Assume $\mathfrak{p}$ is not adjacent to $(i, n - i)$ for any $1 \leq i \leq n/2$ coprime with n. By Lemma 2.10, every such i, with $i \neq 1$, is a partial sum in $\mathfrak{p}$. We now show that also $i = 1$ is a partial sum in $\mathfrak{p}$. Assume this is not the case. Since $\mathfrak{p}$ is not adjacent to $(1, n - 1)$, we deduce from Lemma 2.1 and Theorem 2.3 that $\mathfrak{p}$ is contained in one between $\mathrm{AGL}_d(2)$, $\mathrm{PGL}_2(p)$, M_{11}, M_{12}, M_{24}. The last three are excluded because they are subgroups of A_n. Assume $\mathfrak{p} \in \mathrm{AGL}_d(2)$ or $\mathrm{PGL}_2(p)$. Since every $3 \leq i \leq n/2$ coprime with n is a partial sum, $\mathfrak{p}$ must have odd parts; let a be the smallest such part. Since $i = 1$ is not a partial sum, we have $a \geq 3$. On the other hand, by assumption, $\mathfrak{p}$ corresponds to odd permutations; hence it has even parts. It follows that $(1^n) \neq \mathfrak{p}^a$ fixes a number of points which is greater or equal to 3, and which is a multiple of a. This contradicts Lemma 2.11. Therefore, $i = 1$ is indeed a partial sum in $\mathfrak{p}$.

Now we divide the cases $n \equiv 2 \bmod 4$ and $n \equiv 0 \bmod 4$.

Assume $n \equiv 2 \bmod 4$. Then $n/2 - 2$ is coprime with n; hence it is a partial sum in $\mathfrak{p}$. Write $\mathfrak{p} = (a_1, \ldots, a_t)$, and assume $n/2 - 2 = \sum_{i=1}^{h} a_i$. If $a_k = 1$ for some $k \in \{1, \ldots, h\}$, then $n/2 - 3$ is a partial sum in $\mathfrak{p}$. Otherwise, $n/2 - 1$ is a partial sum in $\mathfrak{p}$. We show that $\mathfrak{q}$ is adjacent in the first case to $\mathfrak{a}_1 = (1, n/2 - 3, n/2 + 2)$, and in the second case to $\mathfrak{a}_2 = (1, n/2 - 2, n/2 + 1)$.

By the considerations above, $\mathfrak{q}$ and $\mathfrak{a}_i$ do not share intransitive subgroups. Moreover, $\mathfrak{a}_1$ and $\mathfrak{a}_2$ correspond to odd permutations, and belong to no transitive imprimitive subgroups by Lemma 2.2. Finally, $\mathfrak{a}_1$ and $\mathfrak{a}_2$ belong to no core-free primitive subgroups by [8, Theorem 1.1]. We have therefore our desired edge between $\mathfrak{q}$ and $\mathfrak{a}_1$ or $\mathfrak{a}_2$.

Assume $n \equiv 0 \bmod 4$. We employ the same argument as above, with $n/2 - 2$ replaced by $n/2 - 1$. The same reasoning lead us to look for an edge between $\mathfrak{q}$ and $\mathfrak{b}_1 = (1, n/2 - 2, n/2 + 1)$ or $\mathfrak{b}_2 = (1, n/2, n/2 - 1)$. Again, $\mathfrak{q}$ and $\mathfrak{b}_i$ do not share intransitive subgroups. It follows from [8, Theorem 1.1] that $\mathfrak{b}_1$ and $\mathfrak{b}_2$ are not contained in core-free primitive subgroups (for $\mathfrak{b}_2$, we may also use Corollary 2.4). Regarding maximal transitive imprimitive subgroups, we only have

that $\mathfrak{b}_2$ is contained in $S_{n/2} \wr S_2$. However, by construction, we consider $\mathfrak{b}_2$ only when $n/2$ is a partial sum in $\mathfrak{p}$ so that $\mathfrak{p}$ belongs to $S_{n/2} \wr S_2$. Since $\mathfrak{p}$ and $\mathfrak{q}$ are adjacent, we deduce that $\mathfrak{q}$ is not contained in $S_{n/2} \wr S_2$. Therefore, we have an edge between $\mathfrak{q}$ and $\mathfrak{b}_1$ or $\mathfrak{b}_2$.

Now we deduce the connectedness of $\Xi(S_n)$ and the bound to the diameter. The considerations above imply that an edge with $\mathfrak{a}_i$ and $\mathfrak{b}_i$ concerns only intransitive subgroups (i.e., partial sums), except for $\mathfrak{b}_2$, where one has to deal also with $S_{n/2} \wr S_2$.

Assume first $n \equiv 2 \bmod 4$. The argument given above shows that every vertex of $\Xi(S_n)$ has distance at most 2 from one among $\mathfrak{a}_1, \mathfrak{a}_2$ and $(i, n - i)$ for some $1 \leqslant i \leqslant n/2$ coprime with n. Hence, in order to conclude, it is sufficient to show that these vertices have pairwise distance at most 2. For $n = 14$, this can be checked directly. Assume then $n > 14$. We show that all these vertices are adjacent to $(2^2, n - 4)$, which clearly concludes the proof. For all the vertices except $(1, n - 1)$, this follows from Lemma 2.10 and from the considerations of the previous paragraph. For $(1, n - 1)$, by Theorem 2.3, we need to exclude the sharing of $\mathrm{AGL}_d(p)$, $\mathrm{PGL}_2(p)$, M_{24}. The last is contained in A_n, while $(2^2, n - 4)$ is not. Moreover, $n \equiv 2 \bmod 4$; hence n is not a power of 2 and we do not have affine subgroups. Finally, $(1^4, n - 4) = (2^2, n - 4)^2$ fixes at least 4 points; hence it does not belong to $\mathrm{PGL}_2(p)$ by Lemma 2.11(2). This concludes the proof in case $n \equiv 2 \bmod 4$.

Assume now $n \equiv 0 \bmod 4$. We assume first $n > 12$. As in case $n \equiv 2 \bmod 4$, in order to conclude, it is sufficient to prove that the vertices $\mathfrak{b}_1, \mathfrak{b}_2$ and $(i, n - i)$ with $1 \leqslant i \leqslant n/2$ coprime with n have pairwise distance at most 2. The vertices $\mathfrak{b}_1, \mathfrak{b}_2$ and $(i, n - i)$ with $1 \leqslant i \leqslant n/2$ coprime with n and $i \neq 3, 5$ are adjacent to $(2, 3, n - 5)$. The vertices $(i, n - i)$ with $1 \leqslant i \leqslant n/2$ coprime with n and $i \neq 1, n/2 - 1$ are adjacent to both $\mathfrak{b}_1$ and $\mathfrak{b}_2$. The vertices $(i, n - i)$ with $2 \leqslant i \leqslant n/2$ coprime with n are adjacent to $(2^2, n - 4)$. By [8, Theorem 1.1] (which in the affine case relies on [7, Theorem 1.5]), we deduce that $(2^2, n - 4)$ is not contained in affine subgroups; hence also $(1, n - 1)$ is adjacent to $(2^2, n - 4)$. These considerations imply that the vertices have pairwise distance at most 2.

Consider now the case $n = 12$. The argument of the previous paragraph does not work, and we need more detailed inspection. Let $\mathfrak{p}$ and $\mathfrak{q}$ be as at the beginning of the proof, with $\mathfrak{p}$ corresponding to odd permutations, and such that 1 and 5 are partial sums in $\mathfrak{p}$. If 2 is not a partial sum and 4 is a partial sum, then it is easy to deduce $\mathfrak{p} = (1, 4, 7)$. If 2 and 4 are not partial sums, then $\mathfrak{p} = (1, 5, 6)$. Assume now 2 is a partial sum. If 3 is not a partial sum, then it is easy to check that $\mathfrak{p}$ must have four cycles, false. If 3 is a partial sum and 4 is not a partial sum, then 5 cannot be a partial sum, false. If 4 is a partial sum, then $\mathfrak{p}$ is isolated unless 6 is not a partial sum and $\mathfrak{p}$ is adjacent to (12). With this more detailed information, it
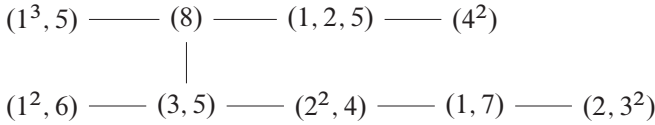
$$(1^3, 5) \text{———} (8) \text{———} (1, 2, 5) \text{———} (4^2)$$

$$(1^2, 6) \text{——} (3, 5) \text{——} (2^2, 4) \text{——} (1, 7) \text{——} (2, 3^2)$$

Figure 1. The graph $\Xi(S_8)$.

is not difficult to deduce $d(\Xi(S_{12})) \leqslant 6$. The proof of the theorem for $n \geqslant 12$ is now concluded. In the next lemma, we consider the case $n = 8$. The case $n = 10$ can be dealt with similarly, and we omit the details. □

We compute the exact diameter of $\Xi(S_8)$; this shows that the upper bound in Theorem 1.3 can be attained.

Lemma 3.7. *The graph* $\Xi(S_8)$ *is connected with diameter* 6.

Proof. In Figure 1, we have drawn the graph $\Xi(S_8)$. The group S_8 has 21 non-trivial conjugacy classes; one can compute explicitly the neighborhood of each of them in $\Lambda(S_8)$. We can save some computations in view of the following observations. Whenever 4 is a partial sum in a partition $\mathfrak{p}$, $\mathfrak{p}$ is not adjacent to partitions having only parts of even length because of the sharing of $S_4 \wr S_2$. It follows that if, in a partition $\mathfrak{p}$, the integers 1, 3 and 4 are partial sums, then $\mathfrak{p}$ is isolated. This implies that the set of vertices of $\Xi(S_8)$ is a subset of

$$A := \{(1^3, 5), (1^2, 6), (1, 2, 5), (1, 7), (3, 5),$$
$$(2, 3^2), (4^2), (2, 6), (2^4), (2^2, 4), (8)\}.$$

Note also that partitions which, for every odd integer ℓ, have an even number (possibly zero) of parts of length ℓ are not adjacent to partitions having only parts of even length because of $S_2 \wr S_4$. We observe finally that the only core-free maximal primitive subgroups of S_8 are $\mathrm{AGL}_3(2)$ and $\mathrm{PGL}_2(7)$ (up to conjugation). Among the partitions in A, $\mathrm{AGL}_3(2)$ contains $(1, 7)$, (4^2), $(2, 6)$, (2^4), and $\mathrm{PGL}_2(7)$ contains $(1^2, 6)$, $(1, 7)$, (4^2), (2^4), (8). It is now easy to draw the graph. □

The last case to consider is alternating groups of odd degree.

Theorem 3.8. *Let* $n \geqslant 5$ *be an odd integer. Then* $\Xi(A_n)$ *is connected, and we have* $d(\Xi(A_n)) \leqslant 6$.

Proof. The cases $n = 5, 7, 9$ can be checked explicitly; we omit the details and assume $n \geqslant 11$. The cases $n = 11, 13, 17, 19$ have been considered in Theorem 3.4 and in the comments following it. Therefore, we need to consider the cases $n = 15$

and $n \geqslant 21$. We first assume $n \geqslant 21$, and deal with the case $n = 15$ at the end of the proof. Throughout the proof, recall Lemmas 2.8 and 2.5.

Let $x, y \in A_n$, and assume x^{A_n} is adjacent to y^{A_n} in $\Xi(A_n)$. We will show that x^{A_n} or y^{A_n} is adjacent to at least one among $(1^2, n - 2)$, $(2^2, n - 4)$, every class with cycle type $(1, 3, n - 4)$, $(1, 4, n - 5)$ and $(2, 8, n - 10)$. This will show that every vertex of $\Xi(A_n)$ has distance at most 2 from one of these vertices. The argument given in the next two paragraphs shows that all these vertices are adjacent to $(6^2, n - 12)$. It will follow that every vertex of $\Xi(A_n)$ has distance at most 3 from $(6^2, n - 12)$, which clearly will conclude the proof.

Let us analyze the classes $(1^2, n - 2)$, $(2^2, n - 4)$, $(1, 3, n - 4)$, $(1, 4, n - 5)$ and $(2, 8, n - 10)$. By Lemma 2.2, only $(1, 4, n - 5)$ and $(2, 8, n - 10)$ belong to some maximal transitive imprimitive subgroup; they are contained in $S_5 \wr S_{n/5}$. Regarding maximal core-free primitive subgroups, by Theorem 2.3, $(1^2, n - 2)$ belongs only to $P\Gamma L_2(q)$ with $n = q + 1$. Moreover, $(2^2, n - 4)$, $(2, 8, n - 10)$ and $(1, 3, n - 4)$ belong to no core-free primitive subgroups, the first two by Corollary 2.4, the last by [8, Theorem 1.1]. Again by [8, Theorem 1.1], $(1, 4, n - 5)$ belongs possibly only to $AGL_d(5)$.

Now consider the class $(6^2, n - 12)$. The maximal transitive imprimitive subgroups it is contained in are $S_3 \wr S_{n/3}$ and $S_{n/3} \wr S_3$. Moreover, by Lemma 2.11, it belongs neither to $AGL_m(p)$ nor to $P\Gamma L_2(q)$. Therefore, as claimed $(1^2, n - 2)$, $(2^2, n - 4)$, every class with cycle type $(1, 3, n - 4)$, $(1, 4, n - 5)$ and $(2, 8, n - 10)$ are adjacent to $(6^2, n - 12)$.

Hence, in order to conclude the proof, it is sufficient to prove the initial claim, that is, to prove that x^{A_n} or y^{A_n} is adjacent to at least one among $(1^2, n - 2)$, $(2^2, n - 4)$, every class with cycle type $(1, 3, n - 4)$, $(1, 4, n - 5)$ and $(2, 8, n - 10)$. In a previous paragraph, we determined the maximal overgroups of these classes. In the following, we will freely use this information with no further mention.

Denote by $c(x)$ and $c(y)$ the cycle types of x and y, respectively. Assume there exists $z \in \{x, y\}$ such that 1 and 2 are not partial sums in $c(z)$; without loss of generality, $z = x$. Then, by Theorem 2.3, either x^{A_n} is adjacent to $(1^2, n - 2)$, or $x \in P\Gamma L_2(q)$. If moreover 4 is not a partial sum in $c(x)$, then x^{A_n} is adjacent to $(2^2, n - 4)$. Assume then that 4 is a partial sum in $c(x)$. The unique possibility is $c(x) = (4, \ldots)$, from which $1 \neq x^4$ fixes an even number of points greater than 3, from which $x \notin P\Gamma L_2(q)$ by Lemma 2.11 (2).

Therefore, we assume (without loss of generality) that 1 is a partial sum in $c(x)$ and 2 is a partial sum in $c(y)$, that is, $c(x) = (1, \ldots)$ and $c(y) = (2, \ldots)$. Then either x^{A_n} is adjacent to $(2^2, n - 4)$, or 4 is a partial sum in $c(x)$. In the latter case, we have $c(x) = (1, 3, \ldots)$ or $c(x) = (1, 4, \ldots)$. If $c(x) = (1, 3, \ldots)$, then y^{A_n} is adjacent to $(1, 3, n - 4)$. If $c(x) = (1, 4, \ldots)$, then y^{A_n} is adjacent to $(1, 4, n - 5)$ unless y is contained in $AGL_d(5)$ or $S_5 \wr S_{n/5}$. The option $y \in AGL_d(5)$ is ex-

cluded by Lemma 2.11 (1) because y^2 fixes 2 points. If $y \in S_5 \wr S_{n/5}$, since 5 is a partial sum in $c(x)$, the unique possibility for the 2-cycle is to act as a 2-cycle on the blocks, from which $c(y) = (2, 8, \ldots)$. Now, since certainly $x \notin S_5 \wr S_{n/5}$, x^{A_n} is adjacent to $(2, 8, n - 10)$. This concludes the proof in case $n \geqslant 21$.

There remains the case $n = 15$. Let $x, y \in A_n$, and assume x^{A_n} is adjacent to y^{A_n} in $\Xi(A_n)$. We prove that x^{A_n} or y^{A_n} is adjacent to at least one between $(1^2, 13)$, $(1, 7^2)$ and (15) (this makes sense by Lemmas 2.7 and 2.12). By Theorem 2.3 and Lemma 2.2, $(1^2, 13)$ and (15) are adjacent. Moreover, $(1, 7^2)$ and (15) are both adjacent to $(2^2, 11)$, and $(1, 7^2)$ and $(1^2, 13)$ are both adjacent to $(3^2, 9)$. It follows that $(1^2, 13)$, $(1, 7^2)$ and (15) have pairwise distance at most 2, from which indeed $d(\Xi(A_{15})) \leqslant 6$.

By Theorem 2.3, if x^{A_n} and y^{A_n} are not adjacent to $(1^2, 13)$, then (without loss of generality) $c(x) = (1, \ldots)$ and $c(y) = (2, \ldots)$. Assume now x^{A_n} and y^{A_n} are not adjacent to (15). We consider the various possibilities. Notice that $x \notin S_3 \wr S_5$ because otherwise 2 would be a partial sum in $c(x)$. Direct inspection (using for instance GAP) shows that if $x \in \mathrm{PGL}_4(2)$, then it must be $c(x) = (1, 7^2)$; hence we may assume this is not the case. Therefore, by Theorem 2.3, it must be $x \in S_5 \wr S_3$, and $y \in S_3 \wr S_5$ or $y \in \mathrm{PGL}_4(2)$. Since $x \in S_5 \wr S_3$, we have $c(x) = (1, 4, \ldots)$; hence 4 is not a partial sum in $c(y)$. Inspection immediately implies $y \notin \mathrm{PGL}_4(2)$, from which $y \in S_3 \wr S_5$. In $c(y)$, the 2-cycle either acts trivially on the blocks, or acts as a 2-cycle on the blocks. In the first case, 1 is a partial sum in $c(y)$, and in the second case, 4 is a partial sum in $c(y)$. In both cases, we get a contradiction, and the proof is finished.   □

Now the proof of Theorem 1.3 and Theorem 1.4 follows immediately from Theorems 3.4, 3.5, 3.6 and 3.8.

4   Some comments on Conjecture 1.5

Conjecture 1.5 states that if $G \in \{A_n, S_n\}$, then, up to finitely many exceptions, one has $d(\Xi(G)) \leqslant 4$. Here we reduce this conjecture to the following one (and in fact to something much weaker, see Remark 4.4).

Conjecture 4.1. Let $G \in \{A_n, S_n\}$. There exists an absolute constant $c > 0$ such that if x^G is a vertex of $\Xi(G)$, then x^G is adjacent to a class which has at most c cycles.

A way to think about this is that, since x^G is a vertex of $\Xi(G)$, by definition, x^G is adjacent to some other class y^G. It seems conceivable that, summing the parts of the cycle type of y in a suitable way, one obtains that x^G is indeed adjacent to

some z^G, where z has a bounded number of cycles. In fact, we believe that the value of c should be rather small, say at most 4; by [8], only a "few" core-free primitive subgroups contain elements having at most 4 cycles.

We now record a consequence of the Prime Number Theorem.

Theorem 4.2. *Fix $\xi > 0$. Denote by $\pi(n)$ the number of primes less or equal to n. Then $\pi((1 + \xi)n) - \pi(n)$ is asymptotic to $\xi n/\ln n$.*

Proof. The Prime Number Theorem states that $\pi(n)$ is asymptotic to $n/\ln n$; hence the statement follows from an easy computation.   □

Theorem 4.3. *Conjecture 4.1 implies Conjecture 1.5.*

Proof. It is sufficient to show that, for n large, vertices which have at most c cycles have pairwise distance at most 2 in $\Xi(G)$. Let x^G and y^G be two such vertices, and denote by $c(x)$ and $c(y)$ the cycle type of x and y, respectively.

We first claim that if n is sufficiently large, then there exist distinct prime numbers p and r such that

(a) $n/3 < p, r \leqslant n/2$,

(b) p, r and $p + r$ are not partial sums in $c(x)$ and in $c(y)$,

(c) p, r and $p + r$ do not divide n.

Let us prove the claim. By Theorem 4.2, the number of primes contained in the interval $(n/3, n/2]$ is asymptotic $n/6 \ln n$. The number of divisors $d(n)$ of n is much smaller; it is known that $d(n) = o(n^\epsilon)$ for every fixed $\epsilon > 0$ (cf. [1, Theorem 13.12, or Exercise 13, p. 303]).

Notice now that there are at most $2^{c+1} = O(1)$ integers i such that i is a partial sum in at least one between $c(x)$ and $c(y)$.

The claim now follows because the number of primes in the interval $(n/3, n/2]$ is much larger than all the other quantities considered above; hence, among all possibilities for p and r, we certainly find one satisfying (b) and (c).

At this point, we conclude the proof. If $G = A_n$ and n is even, or $G = S_n$ and n is odd, then both x^G and y^G are adjacent to $(p, n - p)$. Indeed, by (c) $(p, n - p)$ is not contained in transitive imprimitive subgroups, and a power of $(p, n - p)$ is a p-cycle, hence does not lie in core-free primitive subgroups by a classical theorem of Jordan [16, Theorem 13.9]. Assume now $G = A_n$ with n odd, or $G = S_n$ with n even. Then we claim that both x^G and y^G are adjacent to every class with cycle type $(p, r, n - p - r)$. It is easy to deduce from Lemma 2.2 and from (c) above that $(p, r, n - p - r)$ does not belong to transitive imprimitive subgroups

of S_n. Moreover, since $\min\{p, r\} > n/3$, we have $n - p - r < \min\{p, r\}$. It follows that a power of $(p, r, n - p - r)$ is a p-cycle, hence does not belong to corefree primitive subgroups by Jordan's theorem.

We have shown that x^G and y^G have distance at most 2 in $\Xi(G)$, and the proof is concluded. □

Remark 4.4. In the proof of the previous theorem, we have used a much weaker hypothesis than the validity of Conjecture 4.1. Indeed, the same argument works provided each vertex x^G of $\Xi(G)$ is adjacent to a vertex y^G such that the number of integers i which are partial sums in (the cycle type of) y is at most $\delta n / \log n$ for some explicit fixed constant δ. This statement seems more suitable for a combinatorial proof. Any proof of this sort would very likely avoid the use of the CFSG.

We conclude with a lemma providing a lower bound to $d(\Xi(G))$ in some cases.

Lemma 4.5. *Assume $n \geq 7$ is prime. Then $d(\Xi(S_n)) \geq 4$.*

Proof. The strategy is to define two partitions $\mathfrak{p}$ and $\mathfrak{q}$ such that $\mathfrak{p}$ is adjacent in $\Xi(S_n)$ only to (n), and $\mathfrak{q}$ is adjacent in $\Xi(S_n)$ only to $(1, n - 1)$. Since (n) and $(1, n - 1)$ are not adjacent because of the sharing of $\mathrm{AGL}_1(n)$, this will prove indeed that $d(\Xi(S_n)) \geq 4$.

Define

$$\mathfrak{p} = \begin{cases} (1^{(n-1)/2}, (n+1)/2) & \text{if } n \equiv 3 \mod 4, \\ (1^{(n+1)/2}, (n-1)/2) & \text{if } n \equiv 1 \mod 4. \end{cases}$$

Note that $\mathfrak{p}$ corresponds to odd permutations. Moreover, every $1 \leq i \leq n/2$ is a partial sum in $\mathfrak{p}$; hence $\mathfrak{p}$ is not adjacent to partitions having at least 2 parts. Finally, $\mathfrak{p}$ is adjacent to (n) by Theorem 2.3.

Now define

$$\mathfrak{q} = \begin{cases} (2^{(n-3)/2}, 3) & \text{if } n \equiv 3 \mod 4, \\ (2^{(n-9)/2}, 3^3) & \text{if } n \equiv 1 \mod 4. \end{cases}$$

Note that $\mathfrak{q}$ corresponds to even permutations, so it is not adjacent to (n). It is easy to check that every $2 \leq i \leq n/2$ is a partial sum in $\mathfrak{q}$; hence $\mathfrak{q}$ is adjacent to nothing different from $(1, n - 1)$. Finally, since $\mathfrak{q} \notin \mathrm{AGL}_1(n)$, we deduce by Theorem 2.3 that $\mathfrak{q}$ is indeed adjacent to $(1, n - 1)$. This concludes the proof of the lemma. □

Similar methods should suffice to give sensible lower bounds to $d(\Xi(G))$ in all the various cases. However, the details would become slightly technical, as one would need to specialize the argument depending on the arithmetic of n.

Bibliography

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Undergrad. Texts Math., Springer, New York, 1976.

[2] J. Araújo, J. P. Araújo, P. J. Cameron, T. Dobson, A. Hulpke and P. Lopes, Imprimitive permutations in primitive groups, *J. Algebra* **486** (2017), 396–416.

[3] T. Breuer, R. M. Guralnick and W. M. Kantor, Probabilistic generation of finite simple groups. II, *J. Algebra* **320** (2008), no. 2, 443–494.

[4] T. C. Burness, M. W. Liebeck and A. Shalev, Generation of second maximal subgroups and the existence of special primes, *Forum Math. Sigma* **5** (2017), Article ID e25.

[5] J. D. Dixon, Random sets which invariably generate the symmetric group, *Discrete Math.* **105** (1992), no. 1–3, 25–39.

[6] S. Eberhard, K. Ford and B. Green, Invariable generation of the symmetric group, *Duke Math. J.* **166** (2017), no. 8, 1573–1590.

[7] S. Guest, J. Morris, C. E. Praeger and P. Spiga, Affine transformations of finite vector spaces with large orders or few cycles, *J. Pure Appl. Algebra* **219** (2015), no. 2, 308–330.

[8] S. Guest, J. Morris, C. E. Praeger and P. Spiga, Finite primitive permutation groups containing a permutation having at most four cycles, *J. Algebra* **454** (2016), 233–251.

[9] R. Guralnick and G. Malle, Simple groups admit Beauville structures, *J. Lond. Math. Soc. (2)* **85** (2012), no. 3, 694–721.

[10] R. M. Guralnick and W. M. Kantor, Probabilistic generation of finite simple groups, *J. Algebra* **234** (2000), no. 2, 743–792.

[11] G. A. Jones, Primitive permutation groups containing a cycle, *Bull. Aust. Math. Soc.* **89** (2014), no. 1, 159–165.

[12] W. M. Kantor, A. Lubotzky and A. Shalev, Invariable generation and the Chebotarev invariant of a finite group, *J. Algebra* **348** (2011), 302–314.

[13] T. Łuczak and L. Pyber, On random generation of the symmetric group, *Combin. Probab. Comput.* **2** (1993), no. 4, 505–512.

[14] R. Pemantle, Y. Peres and I. Rivin, Four random permutations conjugated by an adversary generate $\mathcal{S}_n$ with high probability, *Random Structures Algorithms* **49** (2016), no. 3, 409–428.

[15] G. Tracey, Invariable generation of permutation and linear groups, *J. Algebra* **524** (2019), 250–289.

[16] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.

Author information

Corresponding author:
Daniele Garzoni, Dipartimento di Matematica "Tullio Levi-Civita",
Università degli Studi di Padova, Padova, Italy.
E-mail: `daniele.garzoni@phd.unipd.it`