Title
Maximal cocliques in the generating graphs of the alternating and symmetric groups

Journal
Combinatorial Theory, 2(1)

ISSN
2766-1334

Authors
Kelsey, Veronica
Roney-Dougal, Colva M.

Publication Date
2022

DOI
10.5070/C62156879

Maximal cocliques in the generating graphs of the alternating and symmetric groups

Veronica Kelsey*[1] and Colva M. Roney-Dougal*[2]

[1]*Department of Mathematics, University of Manchester, U.K.*
veronica.kelsey@manchester.ac.uk
[2]*School of Mathematics and Statistics, University of St Andrews, U.K.*
Colva.Roney-Dougal@st-andrews.ac.uk

Submitted: Nov 2, 2020; Accepted: Dec 18, 2021; Published: Mar 31, 2022

Abstract. The *generating graph* $\Gamma(G)$ of a finite group G has vertex set the non-identity elements of G, with two elements adjacent exactly when they generate G. A *coclique* in a graph is an empty induced subgraph, so a coclique in $\Gamma(G)$ is a subset of G such that no pair of elements generate G. A coclique is *maximal* if it is contained in no larger coclique. It is easy to see that the non-identity elements of a maximal subgroup of G form a coclique in $\Gamma(G)$, but this coclique need not be maximal.

In this paper we determine when the intransitive maximal subgroups of S_n and A_n are maximal cocliques in the generating graph. In addition, we prove a conjecture of Cameron, Lucchini, and Roney-Dougal in the case of $G = \mathrm{A}_n$ and S_n, when n is prime and $n \neq \frac{q^d-1}{q-1}$ for all prime powers q and $d \geqslant 2$. Namely, we show that two elements of G have identical sets of neighbours in $\Gamma(G)$ if and only if they belong to exactly the same maximal subgroups.

Keywords. Generating graph, alternating groups, symmetric groups

Mathematics Subject Classifications. 20D06, 05C25, 20B35

1. Introduction

The *generating graph* $\Gamma(G)$ of a finite group G has vertex set the non-identity elements of G, with two elements connected exactly when they generate G. A subset of vertices in a graph forms a *coclique* if no two vertices in the subset are adjacent. A coclique is *maximal* if it is contained in no larger coclique.

*Both authors would like to thank the Isaac Newton Institute for Mathematical Sciences for support and hospitality during the programme *Groups, representations and applications: new perspectives*, when work on this paper was undertaken. This work was supported by: EPSRC grant number EP/R014604/1. In addition, the second author was partially supported by a grant from the Simons Foundation.

The definition of a generating graph was first introduced by Liebeck and Shalev in [**?**]. Let $m(G)$ denote the minimum index of a proper subgroup of G. Liebeck and Shalev showed that for all $c < 1$, if G is a sufficiently large simple group, then $\Gamma(G)$ contains a clique of size at least $cm(G)$. That is, G contains a subset S of size at least $cm(G)$ such that all two-element subsets of S generate G. See [**?**], [**?**] and [**?**] for more results about cliques in generating graphs.

Less is known about cocliques in generating graphs. In a slight abuse of language, we shall refer to maximal subgroups as cocliques in $\Gamma(G)$, even though strictly speaking it is their non-identity elements that form a coclique. Recently in [**?**], Saunders proved that for each odd prime p, a maximal coclique in $\Gamma(\mathrm{PSL}_2(p))$ is either a maximal subgroup, the conjugacy class of all involutions, or has size at most $\frac{129}{2}(p-1)+2$.

This paper determines when an intransitive maximal subgroup M of $G = \mathrm{S}_n$ or $G = \mathrm{A}_n$ is a maximal coclique in $\Gamma(G)$. In each case we either show that M is a maximal coclique or determine the maximal coclique containing M.

In a forthcoming paper, the authors determine when an imprimitive maximal subgroup M is a maximal coclique in the generating graph of $G = \mathrm{S}_n$ or A_n. The methods used are similar to those in this paper, but the arguments are necessarily longer. The case of M a primitive maximal subgroup for $G = \mathrm{S}_n$ or A_n will require new techniques. As demonstrated in Theorem 1.1 and in [**?**], a maximal subgroup is not necessarily a maximal coclique.

Our first main result is the following.

Theorem 1.1. *Let $n \geqslant 4$, let $G = \mathrm{S}_n$ or A_n, let $n > k > \frac{n}{2}$ and let $M = (\mathrm{S}_k \times \mathrm{S}_{n-k}) \cap G$ be an intransitive maximal subgroup of G.*

(i) *If $G = \mathrm{S}_n$, then M is a maximal coclique in $\Gamma(G)$ if and only if $\gcd(n,k) = 1$ and $(n,k) \neq (4,3)$.*

(ii) *If $G = \mathrm{A}_n$, then M is a maximal coclique in $\Gamma(G)$ if and only if $(n,k) \notin \{(5,3),(6,4)\}$.*

Our second main theorem concerns the exceptional cases of Theorem 1.1.

Theorem 1.2. (i) *Let $n \geqslant 4$, let $G = \mathrm{S}_n$, let $n > k > \frac{n}{2}$ and let $M = \mathrm{S}_k \times \mathrm{S}_{n-k}$ be an intransitive maximal subgroup of G, setwise stabilising $\{1,\dots,k\}$.*

(a) *If $\gcd(n,k) > 1$, then the unique maximal coclique of $\Gamma(G)$ containing M is*

$$\left(M \cup (1,k+1)^M\right) \setminus \{1\}.$$

(b) *If $(n,k) = (4,3)$, then the unique maximal coclique of $\Gamma(G)$ containing M is*

$$\left(M \cup (1,4)(2,3)^M\right) \setminus \{1\}.$$

(ii) *Let $(n,k) \in \{(5,3),(6,4)\}$, let $G = \mathrm{A}_n$ and let $M = (\mathrm{S}_k \times \mathrm{S}_{n-k}) \cap G$ be an intransitive maximal subgroup of G.*

(a) *If $(n,k) = (5,3)$, then the unique maximal coclique of $\Gamma(G)$ containing M is*

$$\left(M \cup (1,4)(2,3)^M\right) \setminus \{1\}.$$

(b) *If* $(n,k)=(6,4)$*, then the unique maximal coclique of* $\Gamma(G)$ *containing* M *is*

$$\left(M\cup(1,5)(2,6)^M\right)\setminus\{1\}.$$

In [**?**], Cameron, Lucchini and Roney-Dougal define an equivalence relation $\equiv_m$ and a chain of equivalence relations $\equiv_m^{(r)}$ on the elements of a finite group G. Two elements $x,y\in G$ satisfy $x\equiv_m y$ exactly when x and y can be substituted for one another in all generating sets for G. Equivalently, $x\equiv_m y$ when x and y lie in exactly the same maximal subgroups of G. Conversely, $x\equiv_m^{(r)} y$ when x and y can be substituted for one another in all generating sets for G of size r. The relations $\equiv_m^{(r)}$ become finer as r increases, with limit $\equiv_m$, and $\psi(G)$ is defined to be the smallest value of r for which $\equiv_m$ and $\equiv_m^{(r)}$ coincide.

Conjecture 1.3 ([**?**, Conjecture 4.7])**.** Let G be a finite group such that no vertex of $\Gamma(G)$ is isolated. Then $\psi(G)\leqslant 2$.

Settling a long-standing conjecture, Burness, Guralnick and Harper show in [**?**] that if G is a finite group of order greater than two such that all proper quotients of G are cyclic, then no vertex of $\Gamma(G)$ is isolated. The result for $G=\mathrm{A}_n$ and S_n goes back much further, see [**?**].

Cameron, Lucchini and Roney-Dougal observe in [**?**] that to prove this conjecture, it suffices to show that each maximal subgroup is a maximal coclique in $\Gamma(G)$. This motivates the following theorem.

Theorem 1.4. *Let* $p\geqslant 5$ *be a prime such that* $p\neq\frac{q^d-1}{q-1}$ *for all prime powers* q *and all* $d\geqslant 2$*. Let* $G=\mathrm{S}_p$ *or* A_p*.*

(i) *If* $G=\mathrm{S}_p$*, then each maximal subgroup of* G *is a maximal coclique in* $\Gamma(G)$*.*

(ii) *If* $G=\mathrm{A}_p$*, then each maximal subgroup* M *of* G *is a maximal coclique in* $\Gamma(G)$ *except when* $p=5$ *and* M *is conjugate to* $(\mathrm{S}_3\times\mathrm{S}_2)\cap G$*.*

Theorem 2.26 of [**?**] states that $\psi(\mathrm{A}_5)=2$. Hence the following is immediate.

Corollary 1.5. *Let* G *and* p *be as in Theorem 1.4. Then* $\psi(G)=2$*. That is, two elements of* G *belong to exactly the same maximal subgroups of* G *if and only if they can be substituted for each other in all generating pairs for* G*.*

This paper is structured as follows. In Section 2 we begin with some background results on number theory, cycle structures of elements of S_n and block systems of imprimitive permutation groups. In Section 3 we show that Theorems 1.1 and 1.2 hold for $n\leqslant 11$ and prove some preliminary lemmas. In Section 4 we complete the proof of Theorems 1.1 and 1.2. Finally, in Section 5 we prove Theorem 1.4.

2. Background Results

2.1. Number Theoretical Background

In this subsection we collect results about the existence of primes in certain subsets of the integers. We start with Bertrand's Postulate. Throughout this subsection, all $\log$s are natural logarithms.

Theorem 2.1 (Bertrand's Postulate. See for example [**?**, §1])**.** *Let $m \in \mathbb{N}$. If $m \geqslant 4$, then there exists at least one prime p such that $m < p < 2m - 2$. Hence for $k \in \mathbb{N}$ with $k \geqslant 7$, there exists a prime $p_k \geqslant 5$ with $\frac{k}{2} < p_k < k - 1$.*

Notation 2.2. For $k \in \mathbb{N}$ with $k \geqslant 7$, let p_k denote a prime as in Theorem 2.1.

We note that p_k does not divide k, and that p_k is not uniquely determined by k, but at least one such prime must exist.

The proof of the following lemma is straightforward.

Lemma 2.3. *Let $n > k > \frac{n}{2}$ with $k \geqslant 7$ and let p_k be as in Notation 2.2. If $p_k \mid (n-k)$ then $p_k = n - k$, and if $p_k \mid (n-k-1)$ then $p_k = n - k - 1$.*

We will need two variations of Bertrand's Postulate.

Lemma 2.4. *Let $n > k > \frac{n}{2}$, with $k \geqslant 10$. Then there exists an odd prime $p^{(1)} \leqslant k - 5$ such that $p^{(1)} \nmid (n-k)$.*

Proof. Let $Q = \{q \text{ prime} : 2 \leqslant q \leqslant k - 5\}$. The product of the set of prime divisors of $n - k$ is at most $n - k$, so if

$$2(n-k) < \prod_{q \in Q} q, \tag{2.1}$$

then there exists an odd prime $p_k \in Q$, as required.

Since $k \geqslant 10$, the set Q contains $\{2, 3, 5\}$ and so $\prod_{q\in Q} q \geqslant 30$. If $k \leqslant 15$, then $n - k \leqslant k - 1 \leqslant 14$. Hence (2.1) holds for $10 \leqslant k \leqslant 15$.

Assume from now on that $k > 15$, and set $m = k - 5 > 10$. Applying Theorem 2.1 with m in place of k provides a prime p_m with $5 < \frac{m}{2} < p_m < m - 1$. Hence $2, 3, 5$ and p_m are in Q. Observe also that $15m > 2(m + 4)$ and $m + 4 = k - 1 \geqslant n - k$. Hence

$$2(n-k) \leqslant 2(m+4) < 15m < 3 \cdot 5 \cdot (2p_m) \leqslant \prod_{q \in Q} q,$$

as required. □

Lemma 2.5. *Let $n > k > \frac{n}{2}$. If $n - k > 10$, then at least one of the following holds.*

(i) *There exists a prime $p^{(2)}$ with $2 < p^{(2)} < n - k - 3$, such that $p^{(2)} \nmid k$.*

(ii) *The inequality $n - k + 1 < 2(\sqrt{n} - 1)$ holds.*

Proof. First suppose that $10 < n-k < 26$ and let $P = \{q \text{ prime} : 2 < q < n-k-3\}$. If (i) does not hold, then all primes in $q \in P$ divide k, and hence $\prod_{q \in P} q \leqslant k < n$. For $10 < n - k < 26$ a straightforward calculation shows that

$$\frac{(n-k+3)^2}{4} < \prod_{q \in P} q,$$

and so $(n-k+3)^2/4 < n$. Rearranging gives the desired inequality in (ii).

Now suppose that $n-k \geqslant 26$. Let $m = n-k-3$, so that $m \geqslant 23$, and let $\pi(m)$ be the number of primes less than or equal to m. We shall first prove that

$$2\Big(\pi(m-1)-4\Big) > \log\left(2\Big(\frac{m}{2}+3\Big)^2\right). \tag{2.2}$$

To do so let $y := y(m)$ be the following function of m

$$y = (m-1) - \log\left(\frac{m}{2}+3\right)\log(m-1) - \frac{1}{2}\Big(\log(2)+8\Big)\log(m-1).$$

Then

$$\frac{dy}{dm} = 1 - \frac{\log\left(\frac{m}{2}+3\right)}{m-1} - \frac{\log(m-1)}{m+6} - \frac{\log(2)+8}{2(m-1)}.$$

The functions $\frac{\log(\frac{m}{2}+3)}{m-1}$ and $\frac{\log(2)+8}{2(m-1)}$ are monotonically decreasing for $m \geqslant 2$, the function $\frac{\log(m-1)}{m+6}$ is monotonically decreasing for $m \geqslant 9$, and $\frac{dy}{dm}$ is positive at $m = 9$. Hence $\frac{dy}{dm}$ is positive for $m \geqslant 9$. Since $y(23) > 0$, it follows that y is positive for $m \geqslant 23$. Hence for $m \geqslant 23$

$$(m-1) - 4\log(m-1) > \log(\frac{m}{2}+3)\log(m-1) + \frac{1}{2}\log(2)\log(m-1),$$

and so

$$2\Big(\frac{m-1}{\log(m-1)} - 4\Big) > 2\log\left(\frac{m}{2}+3\right) + \log(2) = \log\left(2\Big(\frac{m}{2}+3\Big)^2\right). \tag{2.3}$$

Corollary 1 of [?] states that $\pi(x) > \frac{x}{\log(x)}$ for $x \geqslant 17$. Hence (2.3) implies (2.2).

Let $Q = \{q \text{ prime} : 2 \leqslant q < m\}$ and $Q_0 = \{q \in Q : q > 7\}$. Observe that if $q \in Q_0$, then $\log(q) > 2$. Therefore

$$\log\left(\prod_{q\in Q} q\right) = \sum_{q\in Q}\log(q) > \sum_{q\in Q_0} 2 = 2\Big(\pi(m-1)-4\Big) > \log\left(2\Big(\frac{m}{2}+3\Big)^2\right).$$

Thus

$$\prod_{q\in Q} q > 2\Big(\frac{m}{2}+3\Big)^2.$$

If (i) does not hold, then $q \mid k$ for all odd primes $q \in Q$. Then k is greater than or equal to the product of all such primes, so

$$2n > 2k \geqslant \prod_{q\in Q} q > 2\Big(\frac{m}{2}+3\Big)^2.$$

Hence $\sqrt{n} > \frac{m}{2}+3$ and so

$$2(\sqrt{n}-1) > m+4 = (n-k-3)+4 = n-k+1,$$

as in (ii). Hence the lemma holds. $\square$

2.2. Elementary Results on Cycle Structures and Primitivity

This subsection collects several technical results concerning cycle structures, primitive groups and block systems.

Definition 2.6. For $n \geqslant 12$ we refer to the following elements of S_n as *Jordan elements*:

(i) products of two transpositions;

(ii) cycles fixing at least three points;

(iii) permutations with support size less than or equal to $2(\sqrt{n}-1)$.

The following result will be used extensively in the rest of the paper.

Theorem 2.7. *Let $G \leqslant \mathrm{S}_n$ be primitive. If G contains a Jordan element, then $\mathrm{A}_n \leqslant G$.*

Proof. Types (i), (ii) and (iii) from Definition 2.6 are dealt with by page 43 of [**?**], Corollary 1.3 of [**?**] and Corollary 3 of [**?**] respectively. □

Notation 2.8. Let $y \in \mathrm{S}_n$, and let $c_1c_2\dots c_t$ be the disjoint cycle decomposition of y (including trivial cycles). For $1 \leqslant i \leqslant t$ let $\Theta_i = \mathrm{Supp}(c_i)$. We denote the cycle type of y by $\mathcal{C}(y) = |c_1| \cdot |c_2| \cdots |c_t|$. Often the "·" notation is omitted when it is clear without, and we sometimes gather together common cycle orders and use the usual exponent notation.

For example, if $y = (1,2,3)(4,5)(6,7)$ then we may let $c_1 = (1,2,3)$, $c_2 = (4,5)$ and $c_3 = (6,7)$. Then $\Theta_1 = \{1,2,3\}$, $\Theta_2 = \{4,5\}$ and $\Theta_3 = \{6,7\}$, and we write $\mathcal{C}(y) = 3 \cdot 2 \cdot 2$ or $\mathcal{C}(y) = 3 \cdot 2^2$.

Lemma 2.9. *Let $y \in \mathrm{S}_n$, and let t be the number of cycles in the the disjoint cycle decomposition of y (including trivial cycles). Then y is even if and only if t and n have the same parity.*

Proof. Let y have t_1 cycles of odd length and t_2 cycles of even length, so that $t_1 + t_2 = t$. Then $n \equiv t_1 \bmod 2$ so

$$t - n \equiv t - t_1 = t_2 \bmod 2.$$

Hence t and n have the same parity if and only if t_2 is even, that is if and only if y is even. □

The next lemma guarantees under certain circumstances the existence of suitable sets of distinct points.

Lemma 2.10. *Let $\frac{n}{2} < k < n$, and let $x \in \mathrm{S}_n$ be such that $1^x = k+1$.*

(i) *If $|\mathrm{Supp}(x)| \geqslant 8$ and x does not have cycle type $1^{(n-8)} \cdot 2 \cdot 3^2$, $1^{(n-8)} \cdot 3 \cdot 5$ or $1^{(n-9)} \cdot 3^3$, then there exist distinct points $r, r^x, s, s^x, t, t^x \in \mathrm{Supp}(x) \backslash \{1, k+1\}$.*

(ii) *If $|\mathrm{Supp}(x)| \geqslant 8$ and x does not have cycle type $1^{(n-8)} \cdot 2^4$, then there exist distinct points $s, s^x, t, t^x, u, v \in \mathrm{Supp}(x) \backslash \{1, k+1\}$ such that (u, v) is not a cycle of x.*

Proof. Let $S = \mathrm{Supp}(x)$ and $T = S \backslash 1^{\langle x \rangle}$. We split into cases based on $|1^{\langle x \rangle}|$.

(i) If $|1^{\langle x\rangle}| \geqslant 8$, then we may let $r = 1^{x^2}, s = 1^{x^4}$ and $t = 1^{x^6}$. If $6 \leqslant |1^{\langle x\rangle}| \leqslant 7$, then $|T| \geqslant 2$. Let $r = 1^{x^2}$, $s = 1^{x^4}$ and let $t \in T$. If $4 \leqslant |1^{\langle x\rangle}| \leqslant 5$, then $|T| \geqslant 4$ because x does not have cycle type $1^{(n-8)} \cdot 3 \cdot 5$. Hence either $\langle x\rangle$ has at least two orbits on T of size at least 2 or one of size at least 4. Hence we may let $r = 1^{x^2}$ and $s, t \in T$. If $|1^{\langle x\rangle}| \leqslant 3$, then $|T| \geqslant 6$ because x does not have cycle type $1^{(n-8)} \cdot 3 \cdot 5$ or $1^{(n-8)} \cdot 2 \cdot 3^2$. Hence either $\langle x\rangle$ has one orbit on T of size at least 6, or exactly two orbits, with sizes at least 3 and 4 respectively (because x does not have cycle type $1^{(n-9)} \cdot 3^3$), or at least 3 orbits. Hence we may let $r, s, t \in T$.

(ii) If $|1^{\langle x\rangle}| \geqslant 8$, then let $u = 1^{x^2}$, $v = 1^{x^3}$, $s = 1^{x^4}$ and $t = 1^{x^6}$. If $6 \leqslant |1^{\langle x\rangle}| \leqslant 7$, then let $u = 1^{x^2}$, $v = 1^{x^3}$, $s = 1^{x^4}$ and let $t \in T$. The arguments for $|1^{\langle x\rangle}| \in \{3, 4, 5\}$ are straightforward. If $|1^{\langle x\rangle}| = 2$, then $|T| \geqslant 6$ and $\langle x\rangle$ does not have 3 orbits of size 2 on T, since the cycle type of x is not $1^{(n-8)} \cdot 2^4$. Hence we may let $u, v, s, t \in T$. □

For the rest of this section, let Ω be a finite set and let H be a transitive subgroup of $\mathrm{Sym}(\Omega)$ with a block system $\mathcal{B}$. We include the possibility of $\mathcal{B}$ being trivial, that is blocks of size 1 or $|\Omega|$.

Notation 2.11. For h_i a cycle of $h \in H$, let $h_i^{\mathcal{B}}$ be the permutation that h induces on the set of blocks in $\mathcal{B}$ which contain elements of $\mathrm{Supp}(h_i)$.

In the following lemmas we make a slight abuse of notation to take the support of a 1-cycle to be the unique point in it (even though it does not move that point).

Lemma 2.12. *Let $h \in H$ with cycle h_i. Then $h_i^{\mathcal{B}}$ is a cycle whose length divides the length of h_i.*

Proof. Since h_i is transitive on the points of $\mathrm{Supp}(h_i)$, it follows that $h_i^{\mathcal{B}}$ is a cycle. Let Δ be a block containing $m > 0$ points of $\mathrm{Supp}(h_i)$. It follows that each block of $\mathcal{B}$ contains exactly m or 0 points of $\mathrm{Supp}(h_i)$. Hence $|h_i| = m|h_i^{\mathcal{B}}|$. □

Lemma 2.13. *Let $h \in H$ with disjoint (possibly trivial) cycles h_1 and h_2.*

(i) *Suppose that Δ is a block of $\mathcal{B}$ containing $\alpha \in \mathrm{Supp}(h_1)$ and $\beta \in \mathrm{Supp}(h_2)$. Then $h_1^{\mathcal{B}} = h_2^{\mathcal{B}}$.*

(ii) *If h_1 has prime length p, then the points of $\mathrm{Supp}(h_1)$ either lie in one block or each lie in different blocks.*

(iii) *Suppose h_1 and h_2 have coprime lengths. If there exists a block Δ of $\mathcal{B}$ that contains points from both $\mathrm{Supp}(h_1)$ and $\mathrm{Supp}(h_2)$, then $\mathrm{Supp}(h_1) \cup \mathrm{Supp}(h_2) \subseteq \Delta$.*

Proof. (i) Since $\alpha, \beta \in \Delta$, it follows that for all i, the points α^{h^i} and β^{h^i} lie in the same block. From $\alpha^{h^i} = \alpha^{h_1^i}$ and $\beta^{h^i} = \beta^{h_2^i}$, it follows that $h_1^{\mathcal{B}} = h_2^{\mathcal{B}}$.

(ii) By Lemma 2.12, $h_1^{\mathcal{B}}$ is either a p-cycle or a 1-cycle.

(iii) By Part (i), $h_1^{\mathcal{B}} = h_2^{\mathcal{B}}$. Since h_1 and h_2 have coprime lengths, it follows from Lemma 2.12 that $h_1^{\mathcal{B}}$ is trivial. □

Definition 2.14. Let H be transitive, with block system $\mathcal{B}$, and let $\Delta \in \mathcal{B}$. If $|\Delta| \geqslant 2$ then we say that $\mathcal{B}$ is a *non-singleton* block system.

Lemma 2.15. *Let $\mathcal{B}$ be a non-singleton block system for H. Suppose that there exists $h \in H$ with a cycle h_i of prime length, which is coprime to the lengths of all other cycles of h. Then there exists a block Δ of $\mathcal{B}$ such that $\mathrm{Supp}(h_i) \subseteq \Delta$. In particular, $\Delta^h = \Delta$.*

Proof. Let Δ be a block containing at least one point $\alpha \in \mathrm{Supp}(h_i)$, and let $\beta \in \Delta \backslash \{\alpha\}$. If $\beta \in \mathrm{Supp}(h_i)$, then the result follows by Lemma 2.13(ii). If $\beta \notin \mathrm{Supp}(h_i)$, then $\mathrm{Supp}(h_i) \subseteq \Delta$ by Lemma 2.13(iii). □

3. Preliminary Results

We begin by showing that Theorems 1.1 and 1.2(i) hold when $n \leqslant 11$ and prove Theorem 1.2(ii). We then set up the notation for the rest of the paper, prove some preliminary lemmas and divide the task of proving Theorems 1.1 and 1.2(i) into subcases, see Hypothesis 3.4.

Notation 3.1. Throughout this and the next section let G be either S_n or A_n, acting on the set $\Omega = \{1, 2, \ldots, n\}$ with $n \geqslant 4$. Let $\Omega_1 = \{1, 2, \ldots, k\}$ and $\Omega_2 = \{k+1, \ldots, n\}$ with $k > n-k$. Let $M = \mathrm{Stab}_G(\Omega_1) = \mathrm{Stab}_G(\Omega_2)$. Then M is isomorphic to $\left(\mathrm{S}_k \times \mathrm{S}_{n-k}\right) \cap G$. We let $x \in G \backslash M$.

We first prove Theorem 1.1 for some small values of n and $n-k$. From this Theorem 1.2 Parts (i)(b), (ii)(a) and (ii)(b) will also follow.

Lemma 3.2. *Let $n \leqslant 11$. Then Theorems 1.1 and 1.2 hold.*

Proof. Using Magma (see [?]), we create a list of all possibilities for $x \in G\backslash M$, up to M-conjugacy. For each such x, we create a corresponding list L of elements of M up to conjugation by $C_M(x)$. We then discard all x for which there exists a $y \in L$ such that $\langle x, y\rangle = G$.

The only remaining G, M and x are

(i) $G = \mathrm{S}_n$, $x = (1, k+1)$ and $(n, k) = (6, 4)$, $(8, 6)$, $(9, 6)$, $(10, 6)$ or $(10, 8)$;

(ii) $(G, k, x) = (\mathrm{S}_4, 3, (1, 4)(2, 3))$, $(\mathrm{A}_5, 3, (1, 4)(2, 3))$, or $(\mathrm{A}_6, 4, (1, 5)(2, 6))$.

In each case, x is an involution and two involutions generate a dihedral group. Hence in these cases the maximal coclique in $\Gamma(G)$ containing M is $(M \cup x^M)\backslash\{1\}$. □

Proposition 3.3. *Let $n \geqslant 12$ and let G and M be as in Notation 3.1. Then M is a maximal coclique of $\Gamma(G)$ if and only if for all $x \in G\backslash M$ such that $1^x = k+1$ there exists $y \in M$ such that $\langle x, y\rangle = G$.*

Proof. The forward implication is clear, so assume that M is not a maximal coclique of $\Gamma(G)$. Then there exists $x_1 \in G\backslash M$ such that $\langle x_1, y\rangle \neq G$ for all $y \in M$. Since A_m is transitive for $m \geqslant 3$, there exists $h \in M$ such that x_1^h maps 1 to $k+1$. Hence for all $y \in M$ we deduce that $\langle x_1^h, y^h\rangle \neq G^h = G$. □

We now define two distinct hypotheses which between them cover all possibilities in the case where $x \in G \backslash M$ is not a transposition and $n \geqslant 12$.

Hypothesis 3.4. Recall the set up of Notation 3.1. Let $n \geqslant 12$ so that $k \geqslant 7$.

(A) Let $G = \mathrm{A}_n$ if n is odd and $G = \mathrm{S}_n$ if n is even.

(B) Let $G = \mathrm{A}_n$ if n is even and $G = \mathrm{S}_n$ if n is odd.

In both cases, assume that $1^x = k+1$ and that $x \neq (1, k+1)$.

Notation 3.5. For $y \in M$ define

$$\mathcal{C}_M(y) := \mathcal{C}_1(y) \mid \mathcal{C}_2(y),$$

where $\mathcal{C}_i(y) := \mathcal{C}(y|_{\Omega_i})$ for $i = 1, 2$ is as in Notation 2.8.

We now prove two useful elementary lemmas that will help to simplify the proof of Theorem 1.1. Recall Definition 2.6, of a Jordan element.

Lemma 3.6. *Let n, G, M, and x be as either case of Hypothesis 3.4. If $|\mathrm{Supp}(x) \cap \Omega_1| = 1$, the group $\langle x \rangle$ contains no Jordan element, and $n - k \leqslant 10$, then Theorem 1.1 holds.*

Proof. Since $|\mathrm{Supp}(x) \cap \Omega_1| = 1$, it follows that $|\mathrm{Supp}(x)| \leqslant n - k + 1 \leqslant 11$. Hence, since x is not a Jordan element,

$$2(\sqrt{n} - 1) < |\mathrm{Supp}(x)| \leqslant 11,$$

and so $12 \leqslant n \leqslant 42$. Notice that $|\mathrm{Supp}(x) \cap \Omega_2| \geqslant 2$. Hence by 2-set transitivity of A_m for $m \geqslant 3$, we may assume that $\{k+1, k+2\} \in \mathrm{Supp}(x)$.

If Hypothesis 3.4(A) holds, then let $\mathcal{Y}$ be the set of $y = c_1 c_2 c_3 \in M$ with $\Theta_3 = \{k+2\}$ and $\mathcal{C}_M(y) = k \mid (n-k-1)1$. If Hypothesis 3.4(B) holds, then let $\mathcal{Y}$ be the set of elements of M with cycle type $k \mid (n-k)$. By Lemma 2.9, $\mathcal{Y} \subseteq \mathrm{A}_n$ if and only if $G = \mathrm{A}_n$.

Since $\langle x \rangle$ contains no Jordan element, no power of x is a cycle or the product of two transpositions. From this and the fact that $|\mathrm{Supp}(x)| \leqslant 11$ there are few possible cycle structures for x. Using Magma, for each x, n and k we find a random element of $y \in \mathcal{Y}$ and construct $H(y) = \langle x, y \rangle$, by repeating this sufficiently many times we find $y \in \mathcal{Y}$ such that $H(y) = G$. □

Lemma 3.7. *Let n, G, M and x be as either case of Hypothesis 3.4. Assume that $|\mathrm{Supp}(x)| < 8$ or that $\mathcal{C}(x) \in T := \{1^{(n-8)} \cdot 2 \cdot 3^2,\ 1^{(n-8)} \cdot 3 \cdot 5,\ 1^{(n-8)} \cdot 2^4,\ 1^{(n-9)} \cdot 3^3\}$. Then at least one of the following holds.*

(i) *The group $X = \langle x \rangle$ contains a Jordan element.*

(ii) *There exists an element $y \in M$ such that $\langle x, y \rangle = G$.*

Proof. If $\mathcal{C}(x) \notin S := \{1^{(n-6)} \cdot 2^3,\ 1^{(n-6)} \cdot 3^2,\ 1^{(n-8)} \cdot 2^4,\ 1^{(n-9)} \cdot 3^3\}$, then X contains a Jordan element, so assume that $\mathcal{C}(x) \in S$. If $n > 30$ then $2(\sqrt{n} - 1) > 9$, and so x is a Jordan element, so assume that $n \leqslant 30$. Since $|\mathrm{Supp}(x)| > 2$, and A_m is 2-set transitive for $m \geqslant 3$, we may assume that either $\{k+1, k+2\} \in \mathrm{Supp}(x)$ or $\{1, 2\} \in \mathrm{Supp}(x)$.

Suppose that Hypothesis 3.4(A) holds. If $k+2 \in \mathrm{Supp}(x)$, then let $\mathcal{Y}$ be the set of elements $y = c_1c_2c_3 \in M$ such that $\mathcal{C}_M(y) = k \mid (n-k-1)1$ with $\Theta_3 = \{k+2\}$. If $2 \in \mathrm{Supp}(x)$, then let $\mathcal{Y}$ be the set of elements $y = c_1c_2c_3 \in M$ such that $\mathcal{C}_M(y) = (k-1)1 \mid (n-k)$ with $\Theta_2 = \{2\}$. If Hypothesis 3.4(B) holds let $\mathcal{Y}$ be the set of elements $y = c_1c_2 \in M$ with $\mathcal{C}_M(y) = k \mid (n-k)$. By Lemma 2.9, $\mathcal{Y} \subseteq \mathrm{A}_n$ if and only if $G = \mathrm{A}_n$.

Using Magma, for each x, n and k we find a random element of $y \in \mathcal{Y}$ and construct $H(y) = \langle x, y\rangle$, by repeating this sufficiently many times we find $y \in \mathcal{Y}$ such that $H(y) = G$. □

4. Proof of Theorems 1.1 and 1.2

In this section we complete the proofs of Theorems 1.1 and 1.2.

4.1. Hypothesis 3.4(A)

In this section we show that under Hypothesis 3.4(A) for all $x \in G\backslash M$ there exists $y \in M$ such that $\langle x, y\rangle = G$. We begin by putting restrictions on x.

Lemma 4.1. *Let n, G, M and x be as in Hypothesis 3.4(A). If $|\mathrm{Supp}(x) \cap \Omega_1| = 1$ and x is a Jordan element, then there exists $y \in M$ such that $\langle x, y\rangle = G$.*

Proof. By Hypothesis 3.4, there exists a point $t \in \mathrm{Supp}(x)\backslash\{1, k+1\}$. Our assumption that $|\mathrm{Supp}(x) \cap \Omega_1| = 1$ implies that $t \in \Omega_2$.

By Lemma 2.9, elements of S_n composed of three cycles lie in A_n if and only if $G = \mathrm{A}_n$, so there exists $y = c_1c_2c_3 \in M$ satisfying

$$\mathcal{C}_M(y) = k \mid (n-k-1)1,$$

with $\Theta_3 = \{t\}$. Let $H = \langle x, y\rangle$ and let $Y = \langle y\rangle$. Since $1 \in \Theta_1$ and $k+1 \in \Theta_2$, it follows that $\Theta_1 \cup \Theta_2 = \Omega\backslash\{t\} \subseteq 1^H$. Since $t \in \mathrm{Supp}(x)$, the group H is transitive.

We show that H is primitive. Let Δ be a non-singleton block for H containing t, and let a be an element of $\Delta\backslash\{t\}$. Since t is fixed by y, it follows that $\Delta^y = \Delta$. Hence $a^Y \cup \{t\} \subseteq \Delta$. If $a \in \Theta_1$, then $|\Delta| \geqslant k+1 > \frac{n}{2}$ and so $\Delta = \Omega$. If $a \in \Theta_2$, then $\Theta_2 \cup \{t\} \subseteq \Delta$. Since $\mathrm{Supp}(x) \cap \Theta_1 = \{1\}$ and $(k+1)^{x^{-1}} = 1 \neq t^{x^{-1}}$, it follows that $t^{x^{-1}} \in \Theta_2 \subseteq \Delta$. Hence $\Delta^{x^{-1}} = \Delta$, and so $\Delta^H = \Delta$. By the transitivity of H, it follows that $\Delta = \Omega$.

Hence $H = \langle x, y\rangle$ is primitive, and contains the Jordan element x. Thus $\mathrm{A}_n \leqslant H$, by Theorem 2.7, and so $H = G$. □

We now show that if $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$, then there exists $y \in M$ such that $\langle x, y\rangle = G$.

Lemma 4.2. *Let n, G, M and x be as in Hypothesis 3.4(A). If $|\mathrm{Supp}(x) \cap \Omega_1| = 1$, then there exists $y \in M$ such that $\langle x, y\rangle = G$.*

Proof. By Lemma 4.1, the result holds if x is a Jordan element, and by Lemma 3.6 the result holds if $n-k \leqslant 10$. Hence we may assume that $n-k > 10$ and that $|\mathrm{Supp}(x)| \geqslant 2(\sqrt{n}-1)$. Thus $2(\sqrt{n}-1) \leqslant n-k+1$, so there exists a prime $p^{(2)}$ as in Lemma 2.5. In addition, by Lemma 3.7 the result holds if $|\mathrm{Supp}(x)| < 8$ or if $\mathcal{C}(x) = 1^{(n-8)} \cdot 2^4$, so we may assume otherwise. Hence we may let $s, t, u, v \in \mathrm{Supp}(x)\backslash\{1, k+1\}$ be as in Lemma 2.10(ii).

The proof splits into two cases. First suppose that $p^{(2)} \mid (n-k)$. By Lemma 2.9, elements composed of five cycles lie in A_n if and only if $G = \mathrm{A}_n$, so there exists $y = c_1c_2c_3c_4c_5 \in M$ such that

$$\mathcal{C}_M(y) = k \mid p^{(2)}(n-k-p^{(2)}-2)1^2,$$

with $s, t, t^x \in \Theta_2$, $k+1, s^x \in \Theta_3$, $\Theta_4 = \{u\}$ and $\Theta_5 = \{v\}$. Let $H = \langle x, y\rangle$. Since $1 \in \Theta_1$ and $k+1 \in \Theta_3$, it follows that $\Theta_1, \Theta_3 \subseteq 1^H$. Then because $s \in \Theta_2$ and $s^x \in \Theta_3$, it follows that $\Theta_2 \subseteq 1^H$. Since (u, v) is not a cycle of x and $\Omega\backslash\{u, v\} \subseteq 1^H$, the group H is transitive.

Let $\mathcal{B}$ be a non-singleton block system for H. Since $p^{(2)} > 2$ and $p^{(2)} \mid (n-k)$, it follows that $p^{(2)} \nmid (n-k-p^{(2)}-2)$. Hence by Lemma 2.15, there exists a block $\Delta \in \mathcal{B}$ such that $\Theta_2 \subseteq \Delta$. Therefore $\Delta^y = \Delta$. Furthermore, from $t, t^x \in \Theta_2$ we deduce that $\Delta^H = \Delta$, and hence $\Delta = \Omega$. Thus H is primitive and contains the Jordan element $y^{k(n-k-p_k-2)}$, and so $H = G$.

Next suppose that $p^{(2)} \nmid (n-k)$. By Lemma 2.9, elements composed of three cycles lie in A_n if and only if $G = \mathrm{A}_n$, so there exists $y = c_1c_2c_3 \in M$ such that

$$\mathcal{C}_M(y) = k \mid p^{(2)}(n-k-p^{(2)}),$$

with $s, t, t^x \in \Theta_2$ and $k+1, s^x \in \Theta_3$. Let $H = \langle x, y\rangle$. The argument that H is transitive, primitive and contains a $p^{(2)}$-cycle follows as in the previous case, and so $H = G$. □

We now complete the proof that under Hypothesis 3.4(A) there exists $y \in M$ such that $\langle x, y\rangle = G$.

Lemma 4.3. *Let n, G, M and x be as in Hypothesis 3.4(A). Then there exists $y \in M$ such that $\langle x, y\rangle = G$.*

Proof. If $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$, then the result holds by Lemma 4.2. Therefore we may assume that $|\mathrm{Supp}(x) \cap \Omega_1| \geqslant 2$, and so there exists $t \in \big(\mathrm{Supp}(x) \cap \Omega_1\big)\backslash\{1\}$. Since $k \geqslant 7$, there exists a prime p_k with $5 \leqslant p_k \leqslant k-2$, by Theorem 2.1.

First assume that $k = p_k + 2$ and $n - k = p_k$. Hence $n = 2p_k + 2$. Thus n is even and so $G = \mathrm{S}_n$ by the assumption that Hypothesis 3.4(A) holds. By Lemma 2.9, elements of S_n composed of three cycles are in $\mathrm{S}_n\backslash\mathrm{A}_n$. Let $y = c_1c_2c_3 \in M$ satisfy

$$\mathcal{C}_M(y) = 3(p_k-1) \mid p_k,$$

with $1 \in \Theta_1$, $t \in \Theta_2$ and $t^x \notin \Theta_2$. Let $H = \langle x, y\rangle$. Since $1^x = k+1$, it follows that $\Theta_1, \Theta_3 \subseteq 1^H$. Then $t \in \Theta_2$ and $t^x \in \Theta_1 \cup \Theta_3$, so H is transitive.

Let $\mathcal{B}$ be a non-singleton block system for H. By Lemma 2.15, there exists a block $\Delta \in \mathcal{B}$ with $\Theta_3 \subseteq \Delta$. Hence $\Delta^y = \Delta$ and so Δ is a union of the orbits of y and contains Θ_3. Since $|\Delta| \mid n$, it follows that $\Delta = \Omega$. Hence H is primitive and contains the Jordan element $y^{3(p_k-1)}$, so $H = G$.

If $k \neq p_k + 2$, then $k > p_k + 2$, so for the remainder of the proof we may assume that

$$k - p_k > 2 \quad \text{or} \quad n - k \neq p_k. \tag{4.1}$$

Let $\mathcal{Y}$ be the set of elements $y = c_1c_2c_3 \in M$ satisfying

$$\mathcal{C}_M(y) = (k - p_k)p_k \mid (n - k)$$

with $1 \in \Theta_1$, $t \in \Theta_2$ and $t^x \notin \Theta_2$. By Lemma 2.9, $\mathcal{Y} \neq \varnothing$, and consists of elements of A_n if and only if $G = \mathrm{A}_n$. For all $y \in \mathcal{Y}$, let $H = H(y) = \langle x, y\rangle$ and let $Y = \langle y \rangle$. The proof of transitivity is identical to the previous case. We assume, by way of contradiction, that $H(y)$ is imprimitive for all $y \in \mathcal{Y}$, and let $\mathcal{B}$ be a non-trivial block system for H.

First suppose, by way of contradiction, that there exists $\Delta_1 \in \mathcal{B}$ with $\Theta_2 \subseteq \Delta_1$. We begin by showing that if $\Theta_2 \subseteq \Delta_1$, then $\Delta_1 = \Theta_2$. Suppose otherwise, and let $a \in \Delta_1 \backslash \Theta_2$. From $\Theta_2 \subseteq \Delta_1$ we see that $\Delta_1^y = \Delta_1$. If $a \in \Theta_1$, then $\Theta_1 \cup \Theta_2 \subseteq \Delta_1$ and so $|\Delta_1| \geqslant k > \frac{n}{2}$, a contradiction. Hence $a \in \Theta_3$, so $\Theta_2 \cup \Theta_3 \subseteq \Delta_1$, yielding the contradiction

$$|\Delta_1| \geqslant p_k + n - k > n - \frac{k}{2} > \frac{n}{2}.$$

Hence $\Delta_1 = \Theta_2$ and $p_k \mid n$. Since $\frac{n}{2} < k < 2p_k$, it follows that $n < 4p_k$, and consequently either $n = 2p_k$ or $n = 3p_k$.

If $n = 2p_k$, then $\mathcal{B}$ consists of two blocks $\Delta_1 = \Theta_2$ and $\Delta_2 = \Omega \backslash \Delta_1 = \Theta_1 \cup \Theta_3$. Since 1 and $k + 1 = 1^x \in \Delta_2$ both x and y leave Δ_2 invariant, contradicting the transitivity of H.

If $n = 3p_k$, then there exist blocks Δ_2 and Δ_3 such that $\mathcal{B} = \{\Delta_1, \Delta_2, \Delta_3\}$. Hence $\Delta_2 \cup \Delta_3 = \Theta_1 \cup \Theta_3$. Since $p_k > \frac{k}{2}$, it follows that $|\Delta_2| = p_k$ does not divide $|\Theta_1|$. Hence Δ_2 intersects both Θ_1 and Θ_3 non-trivially, and so $y^{\mathcal{B}} = (\Delta_2, \Delta_3)$. If there exists $\alpha \in \Delta_1$ such that $\alpha^x \in \Delta_1$, then $\Delta_1^x = \Delta_1 = \Delta_1^y$, a contradiction. Therefore $\Delta_1^x \subseteq \Theta_1 \cup \Theta_3$ and $|\Delta_1| \geqslant 5$. Thus there exist distinct points $a_1, a_2 \in \Delta_1$ with a_1^x, a_2^x both in Θ_1 or both in Θ_3. Let

$$\mathcal{Y}_1 = \{y \in \mathcal{Y} \mid (a_1^x)^y = a_2\},$$

and notice that $\mathcal{Y}_1 \neq \varnothing$. Hence for all $y \in \mathcal{Y}_1$, the block Δ_2 contains exactly one of $\{a_1^x, a_2^x\}$. Thus $\varnothing \neq (\Delta_1^x \cap \Delta_2) \neq \Delta_2$, a contradiction.

Therefore if n is even and $y \in \mathcal{Y}$, or if n is odd and $y \in \mathcal{Y}_1$, there is no block Δ_1 with $\Theta_2 \subseteq \Delta_1$. Hence it follows from Lemma 2.13(ii) that $c_2^{\mathcal{B}}$ is a p_k-cycle. Let $\Delta \in \mathrm{Supp}(c_2^{\mathcal{B}})$. Since $p_k > k - p_k$ and Δ is non-trivial, it follows that $c_3^{\mathcal{B}}$ is also a p_k-cycle. Since $n - k < k < 2p_k$, it follows that $p_k = n - k$ and so $|\Delta| = 2$. Therefore n is even and $c_1^{\mathcal{B}}$ is a $\left(\frac{k-p_k}{2}\right)$-cycle.

From $p_k = n - k$ and (4.1), it follows that $k - p_k > 2$. Therefore, since $c_1^{\mathcal{B}}$ is a $\left(\frac{k-p_k}{2}\right)$-cycle we deduce that there exists $a \in \Theta_1 \backslash \{1, t^{x^{-1}}\}$, and the set

$$\mathcal{Y}_a = \left\{ y = c_1c_2c_3 \in \mathcal{Y} : 1^{y^{\frac{k-p_k}{2}}} = a \right\}$$

is non-empty. For all $y \in \mathcal{Y}_a$, it follows that $\Delta_a = \{1, a\}$ is a block for $H = H(y)$. Consider $\Delta_a^x = \{k + 1, a^x\}$. If $a^x \in \Omega_2$, then $\Delta_a^x \subseteq \Omega_2 = \Theta_3$, contradicting the fact that c_3 acts regularly on the blocks in $\mathrm{Supp}(c_3^{\mathcal{B}})$. Hence $a^x \in \Omega_1$. Since $a \neq t^{x^{-1}}$, it follows that $a^x \neq t$ and so there exists $y \in \mathcal{Y}_a$ such that $a^x \in \Theta_1$. Thus $k + 1 \in \Delta_a^x \cap \Theta_3$ and $a^x \in \Delta_a^x \cap \Theta_1$, contradicting the fact that c_1 and c_3 act on disjoint sets of blocks.

Hence there exists $y \in \mathcal{Y}_1$ or $y \in \mathcal{Y}_a$ such that $H = \langle x, y\rangle$ is primitive. If $n - k \neq p_k$, then H contains the p_k-cycle $y^{(k-p_k)(n-k)}$. If $n - k = p_k$, then H contains the $(k - p_k)$-cycle y^{p_k}. Thus in both cases $H = G$ by Theorem 2.7. □

4.2. Hypothesis 3.4(B)

In this section we show that for n, G, M and x as in Hypothesis 3.4(B) there exists $y \in M$ such that $\langle x, y\rangle = G$. We begin with the case $|\Omega_1 \cap \mathrm{Supp}(x)| = 2 = |\Omega_2 \cap \mathrm{Supp}(x)|$.

Lemma 4.4. *Let G, M, n and x be as in Hypothesis 3.4(B). If $|\mathrm{Supp}(x) \cap \Omega_i| = 2$ for $i = 1$ and $i = 2$, then there exists $y \in M$ such that $\langle x, y\rangle = G$.*

Proof. Let $\mathrm{Supp}(x) \cap \Omega_1 = \{1, t\}$ and $\mathrm{Supp}(x) \cap \Omega_2 = \{k + 1, r\}$. Then there are three possibilities for x, namely $(1, k + 1, t, r)$, $(1, k + 1, r, t)$ or $(1, k + 1)(t, r)$.

By Lemma 2.9, elements of S_n composed of two cycles lie in A_n if and only if $G = \mathrm{A}_n$, so there exists $y = c_1c_2 \in M$ such that

$$\mathcal{C}_M(y) = k \mid (n - k),$$

with $1^{y^2} = t$ and $(k + 1)^y = r$. Since $1^x = k + 1$, it follows that $H = \langle x, y\rangle$ is transitive.

We prove that H is primitive. Let Δ be a non-singleton block for H containing 1. We shall show that there exists $b \in \Delta \cap \Theta_1$. Let $a \in \Delta\backslash\{1\}$. If $a \in \Theta_1$, then let $b := a$. If $a \in \Theta_2$, then let $b := 1^{y^{(n-k)}}$. Since $k > n - k$, it follows that $b \neq 1$. From $a^{y^{(n-k)}} = a$ we deduce that $\Delta^{y^{(n-k)}} = \Delta$, hence $b \in \Delta \cap \Theta_1$.

We claim that $\Delta^x = \Delta$ and so $k + 1 \in \Delta$. If $b \in \mathrm{Fix}(x)$, then this is immediate. If $b \notin \mathrm{Fix}(x)$, then looking at $\mathrm{Supp}(x)$ we deduce that $b = t = 1^{y^2}$. Hence $\Delta^{y^2} = \Delta$ and so $1^{y^4} \in \Delta$. Since $k \geqslant 7$, it follows that $1^{y^4} \neq 1, t$. Hence $1^{y^4} \in \mathrm{Fix}(x)$ and so $\Delta^x = \Delta$.

The block Δ^y contains $r \in \mathrm{Supp}(x)$ and $f := 1^y \in \mathrm{Fix}(x)$. Therefore $(\Delta^y)^x = \Delta^y$ and $r^x \in \Delta^y$. Either $r^x = t = f^y$ or $r^x = 1 = f^{y^{-1}}$. Hence either $\{f, f^y\}$ or $\{f, f^{y^{-1}}\} \subseteq \Delta^y$ hence $(\Delta^y)^y = \Delta^y$, and so $\Delta = \Omega$.

Therefore $H = \langle x, y\rangle$ is primitive. Furthermore, H contains x, which is a Jordan element since $n \geqslant 12$. Therefore $\mathrm{A}_n \leqslant H$ by Theorem 2.7 and so $H = G$. □

We now generalise to the case where both $|\Omega_1 \cap \mathrm{Supp}(x)|$ and $|\Omega_2 \cap \mathrm{Supp}(x)|$ are at least 2.

Lemma 4.5. *Let n, G, M and x be as in Hypothesis 3.4(B). If $|\mathrm{Supp}(x) \cap \Omega_1| \geqslant 2$ and $|\mathrm{Supp}(x) \cap \Omega_2| \geqslant 2$, then there exists $y \in M$ such that $\langle x, y\rangle = G$.*

Proof. By Lemma 4.4, the result holds when $|\mathrm{Supp}(x)| = 4$, and so we may assume that $|\mathrm{Supp}(x)| > 4$. Hence there exist points $t \in \Omega_1\backslash\{1\}$ and $r \in \Omega_2\backslash\{k + 1\}$ such that $t^x \neq r$.

Let $\mathcal{Y}$ be the set of elements of M composed of four cycles, c_1 and c_2 with support in Ω_1, and c_3 and c_4 with support in Ω_2, such that $1 \in \Theta_1, t \in \Theta_2, t^x \notin \Theta_2, k + 1 \in \Theta_3$ and $\Theta_4 = \{r\}$. By Lemma 2.9, elements of S_n composed of four cycles lie in A_n if and only if $G = \mathrm{A}_n$, so $\mathcal{Y} \neq \varnothing$. For all $y \in \mathcal{Y}$, let $H = H(y) = \langle x, y\rangle$ and let $Y = \langle y\rangle$.

From $1^x = k + 1$ we deduce that $\Theta_1, \Theta_3 \subseteq 1^H$. Then $t \in \Theta_2$ and $t^x \in \Theta_1 \cup \Theta_3$ together imply that $\Omega\backslash\{r\} \subseteq 1^H$. Since $r \in \mathrm{Supp}(x)$, it follows that H is transitive. Assume, by way of contradiction, that H is imprimitive, and let $\mathcal{B}$ be a non-trivial block system for H.

Let p_k be as in Theorem 2.1. We split into two cases. First assume that $p_k = n - k - 1$ and $p_k = k - p_k + 1$. Then $n = 3p_k$ and so it follows from Hypothesis 3.4(B) that $G = \mathrm{S}_n$. Let

$$\mathcal{Y}_1 = \Big\{y = c_1c_2c_3c_4 \in \mathcal{Y} \ : \ \mathcal{C}_M(y) = (p_k + 1)(p_k - 2) \mid p_k \cdot 1\Big\}.$$

Then $\mathcal{Y}_1 \neq \varnothing$, and by Lemma 2.15, there exists a block $\Delta \in \mathcal{B}$ with $\Theta_3 \subseteq \Delta$, so $|\Delta| \geqslant p_k$. Since $n = 3p_k$, it follows that $|\Delta| = p_k$ and $\Delta = \Theta_3$. Let Γ be the block containing r, so $\Gamma^y = \Gamma$. Then Γ is a union of some of the Θ_i, a contradiction. Therefore for all $y \in \mathcal{Y}_1$, the group $H = H(y) = \langle x, y\rangle$ is primitive. Furthermore, H contains the Jordan element $y^{(p_k+1)(p_k-2)}$ and so $H = G$.

We may now assume that either

$$p_k \neq k - p_k + 1 \quad \text{or} \quad p_k \neq n - k - 1. \tag{4.2}$$

Let

$$\mathcal{Y}_2 = \Big\{ y = c_1c_2c_3c_4 \in \mathcal{Y} \ : \ \mathcal{C}_M(y) = (k - p_k)p_k \mid (n - k - 1)1 \Big\}.$$

Then $\mathcal{Y}_2 \neq \varnothing$.

We first show that there exists $\Delta \in \mathcal{B}$ with $\Theta_2 \subseteq \Delta$. If $p_k \neq n-k-1$, then $p_k \nmid (n-k-1)$ by Lemma 2.3, and so this follows from Lemma 2.15. Suppose instead that $p_k = n-k-1$. If there exist blocks $\Delta_1, \ldots, \Delta_{p_k} \in \mathcal{B}$ such that $c_2^{\mathcal{B}} = (\Delta_1, \ldots, \Delta_{p_k})$, then $\Delta_i \cap \Theta_1 = \varnothing$ and $\Delta_i \cap \Theta_4 = \varnothing$ for $1 \leqslant i \leqslant p_k$ by Lemma 2.13(iii). Since $\mathcal{B}$ is non-trivial, it follows that $c_3^{\mathcal{B}} = (\Delta_1, \ldots, \Delta_{p_k})$ also, and so block size is two. Thus $|\Delta_1| = 2$. Consider the block Γ containing r. The point r is fixed by y, so $\Gamma^y = \Gamma$, but $\Gamma \cap \Theta_1 \neq \varnothing$ so $|\Gamma| \geqslant k - p_k + 1 > 2$, a contradiction. Hence $\Theta_2 \subseteq \Delta$ by Lemma 2.13(ii).

We show next that $c_1^{\mathcal{B}} = c_3^{\mathcal{B}}$. From $|\Delta| \geqslant p_k > \frac{k}{2} > \frac{n}{4}$, it follows that $|\mathcal{B}| = 2$ or 3. First suppose that $|\mathcal{B}| = 2$, and let $\Gamma = \Omega \backslash \Delta$. Since $\Delta^y = \Delta$, it follows that $\Gamma^y = \Gamma$. If $\Theta_1 \subseteq \Delta$ or $\Theta_3 \subseteq \Delta$, then $|\Delta| > \frac{n}{2}$, and so $\Theta_1 \cup \Theta_3 \subseteq \Gamma$. Thus $1, k+1 \in \Gamma$ and $\Gamma^H = \Gamma$, a contradiction. We conclude that $|\mathcal{B}| = 3$. If Δ contains a point of Θ_1, then $\Theta_1 \cup \Theta_2 \subseteq \Delta$, a contradiction, so there exists a block $\Gamma \in \mathcal{B} \backslash \{\Delta\}$ containing a point of Θ_1. Since $|\Theta_1| < |\Theta_2| \leqslant |\Delta|$, it follows that there exists a point $b \in \Gamma \backslash \Theta_1$. If $b \in \Theta_3$, then $c_1^{\mathcal{B}} = c_3^{\mathcal{B}}$ by Lemma 2.13(i). Hence assume for a contradiction that $b \notin \Theta_3$. It follows from $\Gamma \neq \Delta$ that $b \notin \Theta_2$. Hence $b = r$, so $\Gamma^y = \Gamma$. Therefore $\Gamma = \Theta_1 \cup \{r\}$, and the third block of $\mathcal{B}$ is $\Sigma = \Theta_3$. Since $|\Sigma| = |\Delta|$, it follows that $p_k = n - k - 1$. However, $|\Gamma| = k - p_k + 1$, contradicting (4.2).

If there exists $a \in \Delta$ such that $a^x \in \Delta$, then $\Delta^H = \Delta$, a contradiction. Therefore $\Theta_2^x \subseteq \Theta_1 \cup \Theta_3 \cup \{r\}$. By Theorem 2.1, $|\Theta_2| = p_k > 5$. Hence there exist $s_1, s_2 \in \Theta_2$ such that either s_1^x, s_2^x are both in Θ_1 or both in Θ_3. There exists $y \in \mathcal{Y}_2$ such that $s_1^{xy} = s_2^x$. Hence $(\Delta^x)^y = \Delta^x$. Since $c_1^{\mathcal{B}} = c_3^{\mathcal{B}}$, it follows that $\Theta_1 \cup \Theta_3 \subseteq \Delta^x$. In particular, Δ^x contains 1 and $k+1$, and so $\Delta^{x^2} = \Delta^x = \Delta$. Hence $\Delta^H = \Delta$, a contradiction.

Hence for this y the group $H = \langle x, y\rangle$ is primitive. If $p_k \neq n - k - 1$, then $y^{(k-p_k)(n-k-1)}$ is a p_k-cycle and if $p_k = n - k - 1$, then y^{p_k} is a $(k - p_k)$-cycle. Hence in both cases $H = G$. □

We have reduced to the case of either $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$ or $|\Omega_2 \cap \mathrm{Supp}(x)| = 1$. We first consider the case where $|\Omega_1 \cap \mathrm{Supp}(x)| = 1$.

Lemma 4.6. *Let n, G, M and x be as in Hypothesis 3.4(B). If $|\mathrm{Supp}(x) \cap \Omega_1| = 1$, then there exists $y \in M$ such that $\langle x, y\rangle = G$.*

Proof. First assume that x is a Jordan element. It is immediate from Hypothesis 3.4 that there exists $t \in \mathrm{Supp}(x) \backslash \{1, k+1\}$, hence $t \in \Omega_2$. Let $s := t^{x^{-1}}$. (Observe that we only define

$k+1, (k+1)^y, (k+1)^{y^2}$ to be distinct when $|\mathrm{Supp}(x)\cap\Omega_2| \geqslant 3$.) By Lemma 2.9, elements of S_n composed of two cycles lie in A_n if and only if $G = \mathrm{A}_n$, so there exists $y = c_1c_2 \in M$ such that

$$\mathcal{C}_M(y) = k \mid (n-k),$$

with $(k+1)^y = t$, and if $s \neq k+1$, then $t^y = (k+1)^{y^2} = s$. Let $H = \langle x, y\rangle$. Since $1 \in \Theta_1$ and $k+1 \in \Theta_2$, it follows that H is transitive.

Let $\mathcal{B}$ be a non-singleton block system for H, and let $\Delta \in \mathcal{B}$ with $1 \in \Delta$. It follows, just as in the proof of Lemma 4.4, that there exists $b \in (\Delta\cap\Theta_1)\backslash\{1\}$. Since $\Theta_1 \cap \mathrm{Supp}(x) = \{1\}$ and $|\Delta\cap\Theta_1| \geqslant 2$, it follows that Δ contains a point fixed by x, and so $\Delta^x = \Delta$. Therefore $k+1 = 1^x \in \Delta$ and $\{1^y, (k+1)^y\} = \{1^y, t\} \subseteq \Delta^y$. Since 1^y is fixed by x, it follows that $(\Delta^y)^{x^{-1}} = \Delta^y$, hence $s = t^{x^{-1}} \in \Delta^y$. From $t^y = s$ or $s^y = (k+1)^y = t$ we deduce that $\Delta^{y^2} = \Delta^y = \Delta$, and so $\Delta = \Delta^H = \Omega$. Therefore H is primitive. Furthermore, H contains the Jordan element x, so $H = G$.

Hence we may assume that x is not a Jordan element, and so $|\mathrm{Supp}(x)| > 2(\sqrt{n}-1)$. By Lemma 3.6, the result holds when $n-k \leqslant 10$, and so we may assume that $n-k > 10$. Putting these two observations together, there exists a prime $p^{(2)}$ as in Lemma 2.5. Furthermore, since the result holds when x is a Jordan element, by Lemma 3.7 we may assume that $|\mathrm{Supp}(x)| \geqslant 8$ and $\mathcal{C}(x) \neq 1^{(n-8)}\cdot 2\cdot 3^2, 1^{(n-8)}\cdot 3\cdot 5$ or $1^{(n-9)}\cdot 3^3$. Hence let r, s, t be as in Lemma 2.10(i).

If $p^{(2)} \nmid (n-k-1)$, then let $i = 1$, otherwise let $i = 2$. Since $p^{(2)} \leqslant n-k-4$, it follows that $n-k-p^{(2)}-i \geqslant 2$. In addition, since $n-k \geqslant 11$, it follows that $n-k-i \geqslant 9$. Hence either $p^{(2)} \geqslant 5$ or $n-k-p^{(2)}-i \geqslant 5$. By Lemma 2.9, elements of S_n composed of four cycles lie in A_n if and only if $G = \mathrm{A}_n$, so there exists $y = c_1c_2c_3c_4 \in M$ such that

$$\mathcal{C}_M(y) = k \mid p^{(2)}(n-k-p^{(2)}-i)i,$$

with $r, t, t^x \in \Theta_2$, $k+1, r^x \in \Theta_3$, $s^x \in \Theta_4$, $s \in \Theta_2$ if $p^{(2)} \geqslant 5$, and $s \in \Theta_3$ otherwise. Let $H = \langle x, y\rangle$. It is easy to see that H is transitive.

Let $\mathcal{B}$ be a non-singleton block system for H. By Lemma 2.15, there exists $\Delta \in \mathcal{B}$ such that $\Theta_2 \subseteq \Delta$. Hence $\Delta^y = \Delta$. In addition, Δ contains $\{t, t^x\}$, so $\Delta^H = \Delta = \Omega$. Hence H is a primitive group containing the Jordan element $y^{k(n-k-p^{(2)}-i)i}$, and so $H = G$. □

It remains to consider $|\mathrm{Supp}(x)\cap\Omega_2| = 1$. We first suppose that x is a Jordan element.

Lemma 4.7. *Let G, M, n and x be as in Hypothesis 3.4(B). If $|\mathrm{Supp}(x)\cap\Omega_2| = 1$ and x is a Jordan element, then there exists $y \in M$ such that $\langle x, y\rangle = G$.*

Proof. It is immediate from Hypothesis 3.4 that there exists $t \in \mathrm{Supp}(x)\backslash\{1, k+1\}$. Our assumptions that $|\mathrm{Supp}(x)\cap\Omega_2| = 1$ and $1^x = k+1$ imply that $t, t^x \in \Omega_1$.

By Lemma 2.9, elements of S_n composed of two cycles lie in A_n if and only if $G = \mathrm{A}_n$, so there exists $y = c_1c_2 \in M$ such that

$$\mathcal{C}_M(y) = k \mid (n-k),$$

with $1^y = t$, and $t^y = t^x$ if $t^x \neq 1$. It is clear that $H = \langle x, y\rangle$ is transitive.

We assume, by way of contradiction, that H is imprimitive, and let $\mathcal{B}$ be a non-singleton block system for H. Let $\Delta \in \mathcal{B}$ be the block containing $k+1$. If $n-k=1$, then $\Delta^y = \Delta$, and so for $a \in \Delta \backslash \{k+1\}$ we find that $a^Y \cup \{k+1\} = \Omega = \Delta$, and so H is primitive. Hence we assume now that $n-k \geqslant 2$.

We claim that $1 \in \Delta$. To see this, let $\Gamma \in \mathcal{B}$ be the block containing 1. If $\Gamma \cap \mathrm{Fix}(x) \neq \varnothing$, then $k+1 = 1^x \in \Gamma$, hence $\Gamma = \Delta$. Similarly, if $\Delta \cap \mathrm{Fix}(x) \neq \varnothing$, then $\Delta = \Gamma$. Hence we may assume that $\Delta, \Gamma \subseteq \mathrm{Supp}(x)$. Since $|\Omega_2 \cap \mathrm{Supp}(x)| = 1$, it follows that Δ and Γ both contain points of Θ_1. Since Δ contains a point of Θ_2, we deduce from Lemma 2.13(i) that $c_1^{\mathcal{B}} = c_2^{\mathcal{B}}$. However $|\Omega_2 \cap \mathrm{Supp}(x)| = 1$, so $\Delta = \Gamma$ and $1 \in \Delta$.

Notice that the block Δ^y contains $1^y = t$ and $(k+1)^y \in \mathrm{Fix}(x)$. Hence $(\Delta^y)^x = \Delta^y$ and in particular Δ^y contains both t and t^x. If $t^x = 1$, then $\Delta^y = \Delta$. If $t^x \neq 1$, then $\{t, t^x\} = \{t, t^y\} \subseteq \Delta^y = \Delta^{y^2} = \Delta$. Therefore in both cases $\Delta = \Delta^H = \Omega$. Hence H is primitive and contains the Jordan element x, and so $H = G$. □

Finally, we generalise to the case $|\mathrm{Supp}(x) \cap \Omega_2| = 1$.

Lemma 4.8. *Let n, G, M and x be as in Hypothesis 3.4(B). If $|\mathrm{Supp}(x) \cap \Omega_2| = 1$, then there exists $y \in M$ such that $\langle x, y \rangle = G$.*

Proof. First assume that $k \geqslant 10$, so there exists a prime $p^{(1)}$ as in Lemma 2.4. If x is a Jordan element, then the result holds by Lemma 4.7. Hence by Lemma 3.7 the result holds if $|\mathrm{Supp}(x)| < 8$ or $\mathcal{C}(x) = 1^{(n-8)} \cdot 2 \cdot 3^2, 1^{(n-8)} \cdot 3 \cdot 5$ or $1^{(n-9)} \cdot 3^3$, so assume otherwise. Thus there exist $r, s, t \in \mathrm{Supp}(x)$ as in Lemma 2.10(i).

Let $i = 1$ if $p^{(1)} \nmid (k-1)$ and $i = 2$ otherwise. Then $k - i - p^{(1)} \geqslant 3$. By Lemma 2.9, elements of S_n composed of four cycles lie in A_n if and only if $G = \mathrm{A}_n$, so there exists $y = c_1 c_2 c_3 c_4 \in M$ such that

$$\mathcal{C}_M(y) = (k - i - p^{(1)}) p^{(1)} i \mid (n-k),$$

with $1, r, s \in \Theta_1$, $r^x, t, t^x \in \Theta_2$ and $s^x \in \Theta_3$. Let $H = \langle x, y \rangle$. Then it is easy to check that H is transitive.

Let $\mathcal{B}$ be a non-singleton block system for H. By Lemma 2.15, there exists $\Delta \in \mathcal{B}$ such that $\Theta_2 \subseteq \Delta$, hence $\Delta^y = \Delta$. In addition, $t, t^x \in \Delta$, and so $\Delta^x = \Delta = \Omega$, and hence H is primitive. Furthermore, H contains the $p^{(1)}$-cycle $y^{(k-i-p^{(1)})i(n-k)}$ and so $H = G$.

Now suppose that $k \leqslant 9$. It is immediate from Hypothesis 3.4 that $7 \leqslant k \leqslant 9$ and so $12 \leqslant n \leqslant 17$. From $|\mathrm{Supp}(x) \cap \Omega_2| = 1$, it follows that $|\mathrm{Supp}(x)| \leqslant k+1 \leqslant 10$. In Magma, for each x we find a random element of $y \in M$ and construct $H(y) = \langle x, y \rangle$. By repeating this sufficiently many times we find $y \in M$ such that $H(y) = G$. □

Lemma 4.9. *Let n, G, M and x be as in Hypothesis 3.4(B). Then there exists $y \in M$ such that $\langle x, y \rangle = G$.*

Proof. If $|\mathrm{Supp}(x) \cap \Omega_1| = 1$ or $|\mathrm{Supp}(x) \cap \Omega_2| = 1$, then the result holds by Lemma 4.6 and 4.8, respectively. Otherwise, $|\mathrm{Supp}(x) \cap \Omega_i| \geqslant 2$ for $i \in \{1, 2\}$, so the result holds by Lemma 4.5. □

4.3. Completing the proof of Theorems 1.1 and 1.2

In Lemmas 4.3 and 4.9 we prove that if $n \geqslant 12$ and $x \in G \backslash M$ is not a transposition, then there exists $y \in M$ such that $\langle x, y\rangle = G$. Here we show that if $x \in G\backslash M$ is a transposition, then there exists $y \in M$ such that $\langle x, y\rangle = G$ if and only if $\gcd(n, k) = 1$, completing the proof of Theorem 1.1. We also complete the proof of Theorem 1.2.

Theorem 4.10. *Let $n, k, G = \mathrm{S}_n$ and M be as in Notation 3.1, and let $x \in G\backslash M$ be a transposition. Then there exists $y \in M$ such that $\langle x, y\rangle = G$ if and only if* $\gcd(n, k) = 1$.

Proof. By Proposition 3.3, it suffices to consider $x = (1, k + 1)$.

First assume that $\gcd(n, k) = 1$. Let $y \in M$ with $\mathcal{C}_M(y) = k \mid (n-k)$, and let $H = \langle x, y\rangle$. It is clear that H is transitive. Let $\mathcal{B}$ be a non-singleton block system for H, let $\Delta \in \mathcal{B}$ with $1 \in \Delta$, and let $a \in \Delta\backslash\{1\}$. If $a \in \Omega_1$, then $a^x = a$ and so $\Delta^x = \Delta$. Hence $k + 1 = 1^x \in \Delta$. Therefore, without loss of generality, $a \in \Omega_2$. Thus $a^{y^{(n-k)}} = a$, and so $\Delta^{y^{(n-k)}} = \Delta$. Therefore $1^{\langle y^{(n-k)}\rangle} \subseteq \Delta$. It follows from $\gcd(n, k) = 1$ that $1^{\langle y^{(n-k)}\rangle} = \Omega_1$. Hence $|\Delta| \geqslant k + 1 > \frac{n}{2}$, so $\Delta = \Omega$. Hence H is primitive, and contains the Jordan element x. Since $x \in \mathrm{S}_n\backslash\mathrm{A}_n$, it follows that $H = \mathrm{S}_n$.

Next assume that $\gcd(n, k) = t > 1$. Let $y \in M$ be such that $\langle x, y\rangle$ is transitive. Then $\mathcal{C}_M(y) = k \mid (n-k)$. We claim that the set of translates of $\Delta = 1^{\langle y^t\rangle} \cup (k+1)^{\langle y^t\rangle}$ form a proper non-trivial block system for $\langle x, y\rangle$, so that $\langle x, y\rangle \neq \mathrm{S}_n$. To see this, notice that $|\Delta| = n/t > 1$. Also, note that $\dot{\bigcup}_{i=0}^{t-1}\Delta^{y^i} = \Omega$ and x fixes setwise Δ^{y^i} for $0 \leqslant i \leqslant t-1$. □

Proof of Theorem 1.1. The subgroup M is a maximal coclique in $\Gamma(G)$ if and only if for all $x \in G\backslash M$ there exists $y \in M$ such that $\langle x, y\rangle = G$, so let $x \in G\backslash M$. Then by Proposition 3.3 we may assume without loss of generality that $1^x = k + 1$.

If $n \leqslant 11$, then the result holds by Lemma 3.2, so assume that $n \geqslant 12$. If Hypothesis 3.4(A) holds, then the result follows from Lemma 4.3, and if Hypothesis 3.4(B) holds, then the result follows from Lemma 4.9. If neither part of Hypothesis 3.4 holds, then $x = (1, k + 1)$, so the result follows from Theorem 4.10. □

Proof of Theorem 1.2. Parts (i)(b), (ii)(a) and (ii)(b) follow immediately from Lemma 3.2. It remains to prove (i)(a). Hence let $G = \mathrm{S}_n$ and $M = \mathrm{S}_k \times \mathrm{S}_{n-k}$ with $\gcd(n, k) > 1$. We show that the unique maximal coclique of $\Gamma(G)$ containing M is $\left(M \cup (1, k + 1)^M\right) \setminus \{1\}$.

Let C be a maximal coclique in $\Gamma(G)$ containing M. Theorem 1.1 proves that $C \neq M\backslash\{1\}$. Lemmas 4.3 and 4.9 show that if $x \in G\backslash M$ is not a transposition, then $x \notin C$. Hence

$$M\backslash\{1\} \subsetneq C \subseteq \left(M \cup (1, k + 1)^M\right) \backslash\{1\}.$$

By Theorem 4.10, for all $y, m \in M$, the group $\langle y, (1, k + 1)^m\rangle$ is not equal to G. For $n > 3$ no two transpositions generate G so $\left(M \cup (1, k + 1)^M\right) \backslash\{1\} \subseteq C$. Therefore the coclique C is equal to $\left(M \cup (1, k + 1)^M\right) \backslash\{1\}$, as required. □

5. Proof of Theorem 1.4

The methods here are different to those in Section 3, because there are relatively few maximal subgroups of S_p and A_p and these have been classified. We first consider an exceptional case. See [**?**] for the code used in the proof of the following.

Lemma 5.1. *The group M_{23} is a maximal coclique in* A_{23}.

Proof. Let $G = \mathrm{A}_{23}$. A quick calculation in MAGMA shows that the only transitive maximal subgroups of G are two conjugacy classes of groups isomorphic to M_{23}, which we denote $\mathcal{A}$ and $\mathcal{B}$. Since $\mathcal{A}$ and $\mathcal{B}$ are conjugate in S_{23} it suffices to consider $M \in \mathcal{A}$. Recall that the Sylow 23-subgroups of A_{23} are cyclic and transitive.

First suppose that the order of x is at least 4. We claim that there exists $Z \in \mathrm{Syl}_{23}(M)$ such that $\langle x, Z\rangle = G$. By calculating the permutation character of A_{23} on the cosets of M_{23} in MAGMA, we see that x lies in at most 4608 groups $B \in \mathcal{B}$, and each element of order 23 lies in exactly one $A \in \mathcal{A}$ and exactly one $B \in \mathcal{B}$. Let $Z \in \mathrm{Syl}_{23}(M)$, since $M \in \mathcal{A}$ it follows from [**?**], that $N_M(Z) = N_G(Z)$ and $N_M(Z) \leqslant_{\max} M$. Hence $|\mathrm{Syl}_{23}(M)| = [M : N_M(Z)] = 40320$, and so there are $40320 - 4608 = 35712$ possibilities for $Z \in \mathrm{Syl}_{23}(M)$ such that $H := \langle x, Z\rangle$ is contained in no $B \in \mathcal{B}$. Since $x \notin M$, and M is the unique subgroup of $\mathcal{A}$ containing Z, it follows that $H = G$.

Now suppose that x has order 2 or 3 and let $Z \in \mathrm{Syl}_{23}(M)$. By the previous case, M is the unique group of $\mathcal{A}$ containing Z and there exists a unique $B \in \mathcal{B}$ with $Z \leqslant B$. Therefore if $x \notin B$ then $\langle x, Z\rangle = G$. Hence suppose that $x \in B$ and proceed using MAGMA. Let M be the representative of one conjugacy class of M_{23} in G, and let B_0 be the representative of the other. Then B can by found by conjugating B_0 by the element of S_{23} which conjugates a subgroup of $\mathrm{Syl}_{23}(B_0)$ to Z. It is then possible to check that for each element $x \in B\backslash M$ of order 2 or 3, there exists $y \in M$ such that $\langle x, y\rangle = G$. □

The following theorem enables us to classify the maximal subgroups of S_p and A_p.

Theorem 5.2 ([**?**, p.99])**.** *A transitive group of prime degree p is one of the following:*

(i) *the symmetric group S_p or the alternating group A_p;*

(ii) *a subgroup of $\mathrm{AGL}_1(p)$;*

(iii) *a permutation representation of $\mathrm{PSL}_2(11)$ of degree 11;*

(iv) *one of the Mathieu groups M_{11} or M_{23} of degree 11 or 23, respectively;*

(v) *a group G with $\mathrm{PSL}_d(q) \leqslant G \leqslant \mathrm{P\Gamma L}_d(q)$ of degree $p = \frac{q^d-1}{q-1}$.*

In the following lemma we collect some standard facts about $\mathrm{AGL}_1(p)$.

Lemma 5.3. *Let $G = \mathrm{S}_p$ and $M = \mathrm{AGL}_1(p) \leqslant G$.*

(i) *The group M is sharply 2-transitive.*

(ii) *M has a unique Sylow p-subgroup, $P = \langle z \rangle$, and $M = N_G(P) \cong C_p : C_{p-1}$.*

(iii) *The elements of M are p-cycles or powers of $(p-1)$-cycles.*

(iv) *If $y_1, y_2 \in M$ are $(p-1)$-cycles such that $\langle y_1 \rangle \neq \langle y_2 \rangle$, then $M = \langle y_1, y_2 \rangle$.*

We now have the tools required to prove Theorem 1.4.

Proof of Theorem 1.4. Since p is prime, for all k with $p > k > \frac{p}{2}$, it follows that $\gcd(k, p-k) = 1$. If $G = \mathrm{S}_p$, then by Theorem 1.1 each intransitive maximal subgroup is a maximal coclique. If $G = \mathrm{A}_p$, then for $p \neq 5$ each intransitive maximal subgroup is a maximal coclique, and if $p = 5$, then $(\mathrm{S}_4 \times \mathrm{S}_1) \cap \mathrm{A}_5$ is a maximal coclique but $(\mathrm{S}_2 \times \mathrm{S}_3) \cap \mathrm{A}_5$ is not.

If $p = 11$ or 23 and $G = \mathrm{A}_p$, then the transitive maximal subgroups are the respective Mathieu groups. If $p = 11$, then the result follows from a straightforward MAGMA calculation (see [**?**]), similar to the one described in the proof of Lemma 3.2. The result for $p = 23$ follows from Lemma 5.1. Hence assume from now on that if $G = \mathrm{A}_p$, then $p \neq 11, 23$.

Let $G = \mathrm{S}_p$, let $M = \mathrm{A}_p$ and let $x \in G \backslash M$. Let $y \in M$ be a p-cycle such that y is not normalized by x. Then $\langle x, y \rangle$ is a transitive subgroup and lies in no conjugate of $\mathrm{AGL}_1(p) \cap G$ by Lemma 5.3(ii). Hence $\mathrm{A}_p \leqslant \langle x, y \rangle = G$, and so M is a maximal coclique.

By Theorem 5.2 the only remaining case is $M = \mathrm{AGL}_1(p) \cap G$. First consider together the cases $G = \mathrm{A}_p$, or $G = \mathrm{S}_p$ and $x \notin M$ is an odd permutation. Let $y \in M$ be a p-cycle, so $H = \langle x, y \rangle$ is transitive. By Lemma 5.3(ii), y is contained in no other conjugate of $M = N_G(\langle y \rangle)$. Since $x \notin M$, it follows that $H \neq M$, and so $H = G$.

Assume instead that $G = \mathrm{S}_p$ and $x \notin M$ is an even permutation. First let x be of order p. Let $y_1, y_2 \in M$ be $(p-1)$-cycles with $\langle y_1 \rangle \neq \langle y_2 \rangle$. Then $H_1 = \langle x, y_1 \rangle$ and $H_2 = \langle x, y_2 \rangle$ are transitive subgroups of G. Note that $y_1, y_2 \in G \backslash \mathrm{A}_p$, and so H_1 and H_2 either conjugate to M, or equal to G. In the latter case the result holds, so assume that both H_1 and H_2 are conjugate to M. Since $x \in H_1 \cap H_2$ and $N_G(\langle x \rangle)$ is the unique conjugate of M containing x, it immediately follows that $H_1 = N_G(\langle x \rangle) = H_2$, a contradiction since $M \leqslant \langle y_1, y_2 \rangle$.

Assume next that x lies in no conjugate of M. Let $t \in \mathrm{Supp}(x)$ and let y be a $(p-1)$-cycle of M fixing t. Then $\langle x, y \rangle$ is transitive and contained in no conjugate of M, and so $\langle x, y \rangle = G$.

Finally assume that x is an even permutation, not a p-cycle and lies in some conjugate of M. By Lemma 5.3(iii), x is a proper power of a $(p-1)$-cycle. We claim there exists a $(p-1)$-cycle y in M, and $z \in \langle y \rangle$, such that $H = \langle x, y \rangle$ is transitive and $1 < \mathrm{Fix}(z^{-1}x) < p$. Since, by Lemma 5.3(i), each non-identity element of M has at most one fixed point it will follow that H lies in no conjugate of M, and so $H = G$.

It remains to prove the claim. Since x is a proper power of a $(p-1)$-cycle, x has one fixed point which we shall call f. Let M_f denote the point stabilizer of f in M, and P denote the cyclic p-subgroup of M.

Since $p \geqslant 5$, there exist $a, b \in \mathrm{Supp}(x)$ with $a \neq b$. By sharp 2-transitivity there exists an element y_1 in M such that $a^{y_1} = a^x$ and $b^{y_1} = b^x$. If $y_1 \notin M_f \cup P$, then y_1 lies in a cyclic subgroup $\langle y \rangle$ of order $(p-1)$ and $H = \langle x, y \rangle$ is transitive. In addition $a, b \in \mathrm{Fix}(y_1^{-1}x)$, as claimed.

Suppose instead that $y_1 \in M_f \cup P$. Since $y_1 \neq x$ and $p \geqslant 5$, there exists $c \in \mathrm{Supp}(x)$ with $c \neq a, b$ such that $c^{y_1} \neq c^x$. By sharp 2-transitivity, there exists $y_2 \in M$ such that $a^{y_2} = a^x$ and $c^{y_2} = c^x$. If $y_2 \notin M_f \cup P$, then the result follows as for y_1 with $a, c \in \mathrm{Fix}(y_2^{-1}x)$.

Suppose that $y_1, y_2 \in M_f \cup P$. It follows from $c^{y_1} \neq c^{y_2}$ that $y_1 \neq y_2$. Therefore because $a^{y_1} = a^{y_2}$, by sharp 2-transitivity, it follows that $b^{y_2} \neq b^{y_1} = b^x$. There is a unique element of M_f, and a unique element of P, sending a to a^x. Let Y_1 and Y_2 be the maximal cyclic subgroups containing y_1 and y_2. Then $Y_1 \cup Y_2 = M_f \cup P$.

Since M is sharply 2-transitive, there exists $y_3 \in M$ such that $b^{y_3} = b^x$ and $c^{y_3} = c^x$. Since y_1 is the unique element of Y_1 sending b to b^x, and $c^{y_1} \neq c^{y_3}$, it follows that $y_3 \notin Y_1$. Since y_2 is the unique element of Y_2 sending c to c^x and $b^{y_2} \neq b^{y_3}$, it follows that $y_3 \notin Y_2$. Hence $y_3 \notin Y_1 \cup Y_2 = M_f \cup P$. Thus let $y \in M$ be a $(p-1)$-cycle such that $y^t = y_3$ for some $t \in \mathbb{N}$. Then y satisfies the claim with $b, c \in \mathrm{Fix}(y^{-t}x) = \mathrm{Fix}(y_3^{-1}x)$. Therefore the claim and the theorem follow. □