The non-isolated vertices in the generating graph of a direct powers of simple groups

Eleonora Crestani · Andrea Lucchini

Received: 19 July 2011 / Accepted: 16 March 2012 / Published online: 4 April 2012
© Springer Science+Business Media, LLC 2012

Abstract For a finite group G let $\Gamma(G)$ denote the graph defined on the non-identity elements of G in such a way that two distinct vertices are connected by an edge if and only if they generate G . Many deep results on the generation of the finite simple groups G can be equivalently stated as theorems that ensure that $\Gamma(G)$ is a rich graph, with several good properties. In this paper we want to consider $\Gamma(G^\delta)$ where G is a finite non-abelian simple group and G^δ is the largest 2-generated power of G , with the aim to investigate whether the good generation properties of G still affect the behaviour of $\Gamma(G^\delta)$. In particular we prove that the graph obtained from $\Gamma(G^\delta)$ by removing the isolated vertices is 1-arc transitive and connected and we investigate the diameter of this graph. Moreover, some intriguing open questions will be introduced and their solutions will be exemplified for $G = \text{Alt}(5)$.

Keywords Generating graph · Direct power of simple groups · Diameter

1 Introduction

For a finite group G , let $\Gamma(G)$ denote the graph defined on the non-identity elements of G in such a way that two distinct vertices are connected by an edge if and only if they generate G . The graph $\Gamma(G)$ is called the generating graph of G .

The graph $\Gamma(G)$ has “many” edges when G is a finite non-abelian simple group: indeed a finite non-abelian simple group G can be generated by 2 elements and the probability $P(G)$ that a random pair of vertices of $\Gamma(G)$ is connected by an edge tends to 1 as $|G|$ tends to infinity [10]. Many deep results about finite simple groups

E. Crestani · A. Lucchini (✉)
Dipartimento di Matematica, Università di Padova, Via Trieste 63, 35121 Padova, Italy
e-mail: lucchini@math.unipd.it

E. Crestani
e-mail: crestani@math.unipd.it

G can equivalently be stated as theorems on $\Gamma(G)$. For example, in [8] Guralnick and Kantor showed that there is no isolated vertex in $\Gamma(G)$ and Breuer, Guralnick, Kantor in [4] showed that the diameter of $\Gamma(G)$ is 2 for all G .

It is well known that if G is a finite non-abelian simple group, then G^n is still 2-generated if $n \leq \delta(G) = P(G)|G|/|\text{Out}(G)|$. The aim of this paper is to compare the properties of the graph $\Gamma(G)$ with those of $\Gamma(G^n)$, with particular attention to the case $n = \delta(G)$. It is no more true that $\Gamma(G^n)$ has no isolated vertices, so we will concentrate our attention on the subgraph $\Gamma_n(G)$ obtained from $\Gamma(G^n)$ by removing the isolated vertices. This graph has several interesting properties; in particular $\Gamma_{\delta(G)}(G)$ is 1-arc transitive. Although $P(G) \rightarrow 1$ as $|G| \rightarrow \infty$, since $\delta(G)$ increase with $|G|$, the probability that two vertices of $\Gamma_{\delta(G)}(G)$ are connected by an edge tends to zero as $|G|$ goes to infinity. Nevertheless, the abundance of edges in the graph $\Gamma(G)$ reflects on $\Gamma_{\delta(G)}(G)$ and allows us to prove:

Theorem 1.1 *If G is a non-abelian simple group, then the graph $\Gamma_n(G)$ is connected for $n \leq \delta(G)$.*

Once it is established that $\Gamma_n(G)$ is connected, the next step is to investigate the diameter of this graph. We obtained the following upper bound:

Theorem 1.2 *Let G be a finite non-abelian simple group and let $\delta = \delta(G)$.*

- (1) *If $i < \delta$, then the diameter of $\Gamma_i(G)$ is at most $2 + 4(i - 1)$.*
- (2) *The diameter of $\Gamma_{\delta}(G)$ is at most 4δ if $|G|$ is large enough.*

Is it not clear how sharp this bound is. However, we are able to construct an infinite family of simple groups for which $\text{diam}(\Gamma_{\delta(G)}(G)) \geq \frac{|G|^{1/3}}{8}$. In particular this ensures the existence of simple groups the diameter of whose associated graph $\Gamma_{\delta(G)}(G)$ is arbitrarily large.

Theorem 1.3 *Let $G = \text{SL}(2, 2^p)$ with p an odd prime. We have $\text{diam}(\Gamma_{\delta(G)}(G)) \geq 2^{p-2} - 1$ if p is large enough.*

In the final section of the paper we propose some questions about the clique number $\omega(\Gamma_{\delta(G)}(G))$. If G is a finite non-abelian simple group, then the generating graph $\Gamma(G)$ contains “large” complete subgraphs. Indeed Liebeck and Shalev proved that $\omega(\Gamma_{\delta(G)}(G)) \rightarrow \infty$ as $|G| \rightarrow \infty$. However it seems an open and difficult question to decide whether $\omega(\Gamma_{\delta(G)}(G))$ increases with $|G|$. It can be easily seen that $\omega(\Gamma_{\delta(G)}(G)) \geq 3$ but it is already quite difficult to establish the existence of a complete subgraph with four vertices. We discuss these and other related questions in the particular case $G = \text{Alt}(5)$. It is well known that $\delta(\text{Alt}(5)) = 19$. We prove $\omega(\Gamma_{19}(\text{Alt}(5))) = 4$.

2 Definition of $\Gamma_{\delta}(S)$: notations and main properties

Let S be a non-abelian finite simple group and denote by A the automorphism group $\text{Aut}(S)$ of S . As usual we identify S with the subgroup of A consisting of the inner

automorphisms. Define $\delta = \delta(S)$ to be the largest positive integer r such that S^r , the direct product of r copies of S , can be generated by two elements. The positive integer δ is well-defined. To see this first note that it is known that every non-abelian finite simple group can be generated by two elements [1, Theorem B]. Also, for any positive integer d , the group S^r cannot be generated by d elements whenever r is larger than the number of A -orbits on the set of d -tuples generating S . Actually, δ is equal to the number of A -orbits on ordered pairs of generators for S and, for arbitrary elements $x = (x_1, \dots, x_\delta)$ and $y = (y_1, \dots, y_\delta)$ of S^δ , we have $S^\delta = \langle x, y \rangle$ if and only if the pairs (x_i, y_i) are distinct representatives for these orbits for i with $1 \leq i \leq \delta$.

Let $K = \text{Aut}(S^\delta)$. Recall that $K \cong A \wr \text{Sym}(\delta)$. Clearly $K \leq \text{Aut}(\Gamma_\delta(S))$. The following easy remark will play a crucial role in our discussion.

Lemma 2.1 *Assume $S^\delta = \langle x, y \rangle$. If $S^\delta = \langle \bar{x}, \bar{y} \rangle$, then there exists $k \in K$ with $(\bar{x}, \bar{y}) = (x^k, y^k)$.*

Proof Assume $x = (x_1, \dots, x_\delta)$, $y = (y_1, \dots, y_\delta)$, $\bar{x} = (\bar{x}_1, \dots, \bar{x}_\delta)$ and $\bar{y} = (\bar{y}_1, \dots, \bar{y}_\delta)$. Both $(x_1, y_1), \dots, (x_\delta, y_\delta)$ and $(\bar{x}_1, \bar{y}_1), \dots, (\bar{x}_\delta, \bar{y}_\delta)$ form a set of representatives for the A -orbits of the set of generating pairs for S . So there exist $\pi \in \text{Sym}(\delta)$ and $(a_1, \dots, a_\delta) \in A^\delta$ such that $(\bar{x}_{i\pi}, \bar{y}_{i\pi}) = (x_i, y_i)^{a_i}$ for each $i \in \{1, \dots, \delta\}$. It follows that $(\bar{x}, \bar{y}) = (x^k, y^k)$ for $k = (a_1, \dots, a_\delta)\pi \in K$. $\square$

We want to study the graph $\Gamma_\delta(S)$ obtained from the generating graph $\Gamma(S^\delta)$ just by removing all isolated vertices.

Proposition 2.2 *$\Gamma_\delta(S)$ satisfies the following properties:*

- (1) $\Gamma_\delta(S)$ is vertex-transitive and edge-transitive.
- (2) $\Gamma_\delta(S)$ is symmetric (1-arc transitive).
- (3) $\Gamma_\delta(S)$ is not 2-arc transitive.
- (4) $\Gamma_\delta(S)$ has girth 3.

Proof It follows immediately from Lemma 2.1 that the graph $\Gamma_\delta(S)$ is vertex-transitive and edge-transitive. On the other hand if $S^\delta = \langle x, y \rangle$ then clearly $S^\delta = \langle y, x \rangle$ so, again by Lemma 2.1, $\Gamma_\delta(S)$ is symmetric. Moreover if $S^\delta = \langle x, y \rangle$, then also (x, xy) and (y, xy) are generating pairs for S^δ , so $\{x, y, xy\}$ is a triangle of Γ , hence the girth of Γ is 3. Now to conclude that Γ is not 2-arc transitive it suffices to exhibit a 2-arc (x_1, x_2, x_3) in Γ with x_1 and x_3 non connected. This follows from the fact that if $x = (x_1, \dots, x_\delta)$ and $y = (y_1, \dots, y_\delta)$ generate S^δ , then (x, y, xy^2) is a 2-arc, but $\langle x, xy^2 \rangle = \langle x, y^2 \rangle \neq S^\delta$. Indeed (see for example [8]) there exists a generating pair (s, t) for the simple group S with $|s| = 2$, hence there exists $i \in \{1, \dots, \delta\}$ with $y_i^2 = 1$, but then $\langle x_i, y_i^2 \rangle = \langle x_i \rangle \neq S$. $\square$

Now we will introduce other notations, useful in our study of the graph $\Gamma_\delta(S)$. Fix a vertex x of $\Gamma_\delta(S)$ and consider $C = C_K(x)$. The number of vertices in $\Gamma_\delta(S)$ is $|K|/|C|$ and the number of edges is $|K|/2$ (since the action of K on the pairs of generators is regular and 2 in the denominator comes from the fact that the edges of Γ are

unoriented). Moreover every vertex of Γ has degree $|C|$. To describe more precisely C we need the following information. Let $s_1, \dots, s_u$ be a set of representatives for the A -orbits of $S \setminus \{1\}$. For each $1 \leq i \leq u$, let $\gamma_i = |C_A(s_i)|$ and let $d_i = d(\Gamma(S), s_i)$ be the degree of s_i in the generating graph $\Gamma(S)$ of S (it is proved in [8] that $d_i \neq 0$ for each $1 \leq i \leq u$). There are precisely $\delta_i = d_i/\gamma_i$ pairs (s_i, t) generating S and not pairwise A -conjugate and this means that every vertex $x = (x_1, \dots, x_\delta)$ in $\Gamma_\delta(S)$ has precisely δ_i entries that are A -conjugate to s_i . In particular x is K -conjugate to $\bar{x}$ with

$$\bar{x} = (\underbrace{s_1, \dots, s_1}_{\delta_1 \text{ terms}}, \underbrace{s_2, \dots, s_2}_{\delta_2 \text{ terms}}, \dots, \underbrace{s_u, \dots, s_u}_{\delta_u \text{ terms}}).$$

It follows that $C \cong C_K(\bar{x}) = \prod_{1 \leq i \leq u} C_A(s_i) \wr \text{Sym}(\delta_i)$ and consequently:

- (1) $\Gamma_\delta(S)$ has $\frac{|A|^{\delta} \delta!}{2}$ edges and $\frac{|A|^{\delta} \delta!}{\prod_{1 \leq i \leq u} \gamma_i^{\delta_i} \delta_i!}$ vertices;
- (2) every vertex of $\Gamma_\delta(S)$ has degree $\prod_{1 \leq i \leq u} \gamma_i^{\delta_i} \delta_i!$.

3 $\Gamma_\delta(S)$ is connected

The first question that we want to discuss is whether the graph $\Gamma_\delta(S)$ is connected. We give an affirmative answer.

Theorem 3.1 *The graph $\Gamma_\delta(S)$ is connected.*

Proof The proof depends on the following result, proved in [8] using the classification of the finite simple groups: there is a conjugacy class s^S of S such that each nontrivial element of S generates S together with a suitable member of s^S . It is not restrictive to assume $s = s_1$ (in the notation of the previous section) and this has the following consequence.

(*) If $(y_1, \dots, y_\delta)$ is connected to $\bar{x}$ in $\Gamma_\delta(S)$, then for each $i \in \{1, \dots, u\}$ there exists $j \in \{1, \dots, \delta_1\}$ such that y_j and s_i are A -conjugate.

Now let Δ be the connected component of Γ which contains the vertex $\bar{x}$. Denote by V the set of vertices of $\Gamma_\delta(S)$ and by W the set of vertices of Δ . The set W is a block for the action of K on V . In particular the setwise stabilizer H of W in K contains the point stabilizer $C = C_K(\bar{x}) = \prod_{1 \leq i \leq u} C_A(s_i) \wr \text{Sym}(\delta_i)$. We identify K with $A \wr \text{Sym}(\delta)$: in particular every element $k \in A$ can be written in the form $k = (a_1, \dots, a_\delta)\sigma$ with $a_i \in A$ and $\sigma \in \text{Sym}(\delta)$ and the map $\pi : k \mapsto \sigma$ is a group homomorphism from K to $\text{Sym}(\delta)$. We first prove

(**) $H^\pi = \text{Sym}(\delta)$.

Since $C \leq H$, we have $C^\pi = \prod_{1 \leq i \leq u} \text{Sym}(\delta_i) \leq H^\pi$. The orbits of C^π are $\Omega_1 = \{1, \dots, \delta_1\}$, $\Omega_2 = \{\delta_1 + 1, \dots, \delta_1 + \delta_2\}$, $\dots$, $\Omega_u = \{\delta - \delta_u + 1, \dots, \delta\}$. Choose $\bar{y} = (y_1, \dots, y_\delta) \in S^\delta$ with the property that $S^\delta = \langle \bar{x}, \bar{y} \rangle$: as we noticed before $\bar{y} = \bar{x}^k$ for some $k \in K$. In particular $\bar{y} \in W \cap W^k$ so, since W is a block, $W = W^k$ and $k \in H$. Let $\sigma = k^\pi$. Notice that, by (*), for each $1 \leq i \leq u$ there exists $j \in \Omega_1$ with $j^\sigma \in \Omega_i$.

This means that $\langle \sigma, C^\pi \rangle = \langle k, C \rangle^\pi$, and consequently H^π is a transitive subgroup of $\text{Sym}(\delta)$. Assume now that B is a non trivial block for the action of H^π on $\{1, \dots, \delta\}$ with $1 \in B$ and $|B| \neq 1$. Since $C^\pi \leq H^\pi$ we find that, for each $1 \leq j \leq u$ and each $\tau \in \text{Sym}(\delta)$, if $\Omega_j \cap B^\tau \neq \emptyset$ then $\Omega_j \subseteq B^\tau$. In particular $1 \in B$ implies $\Omega_1 \subseteq B$, hence $\Omega_1^\sigma \subseteq B^\sigma$. On the other hand, as we noticed before, $\Omega_1^\sigma \cap \Omega_j \neq \emptyset$ and hence $\Omega_j \subseteq B^\sigma$ for each $1 \leq j \leq u$. This implies that $B^\sigma = B = \{1, \dots, \delta\}$ and H^π is a primitive permutation group. Since $\delta_1 > 1$ and $\text{Sym}(\delta_1) \leq C^\pi \leq H^\pi$, we conclude that $H^\pi = \text{Sym}(\delta)$ (see for example [6, Theorem 3.3E]).

The next step is to prove

$$(***) \quad H = K.$$

We identify S with $\text{Inn}(S) \leq \text{Aut}(S)$. Let $z \in A$. It follows from the classification of the finite simple groups that there exists $\bar{s} \in S$ with $1 \neq \bar{s}$ and $\bar{s}^z = \bar{s}$ (see for example [13]). Now, from (*) and (**), we deduce that there exist $y = (y_1, \dots, y_\delta) \in W$ and $a \in A$ with the property that $y_1 = \bar{s}^a$. In particular, if $t = (z^a, 1, \dots, 1)$, then $y = y^t \in W \cap W^t$, hence $W = W^t$ and $t \in H$. Let $X = \{x \in A \mid (x, 1, \dots, 1) \in A^\delta \cap H\}$. We see that X is a subgroup of A which contains a representative for every conjugacy class, hence $A = \bigcup_{a \in A} X^a$. As is well known, this implies $X = A$. But then H contains $(x, 1, \dots, 1)$ for every $x \in A$: together with (**) this implies that $H = K$.

Now we have $V = \bar{x}^K = \bar{x}^H \leq W$, hence $W = V$ and $\Gamma_\delta(S)$ is a connected graph. $\square$

4 An upper bound for the diameter of $\Gamma_\delta(S)$

In this section we want to study the diameter of the graph $\Gamma_\delta(S)$ for $\delta = \delta(S)$. Our main result will be obtained as a corollary of a more general theorem, dealing with the diameter of the graph $\Gamma_i(S)$ of the non-isolated vertices in the generating graph $\Gamma(S^i)$ for $i \leq \delta$.

If $i \leq \delta$, then S^i is 2-generated: more precisely $(x_1, \dots, x_i)$ and $(y_1, \dots, y_i)$ generate S^i if and only if $(x_1, y_1), \dots, (x_i, y_i)$ are not pairwise A -conjugate pairs of generators of S . Let us introduce some notations, useful in the study of the graph $\Gamma_i(S)$. Let $C_1, \dots, C_u$ be the A -orbits of $S \setminus \{1\}$. For $x = (x_1, \dots, x_i) \in S^i$ and $j \in \{1, \dots, u\}$, define

$$\Omega(x, j) = \{k \in \{1, \dots, i\} \mid x_k \in C_j\} \quad \text{and} \quad \omega(x, j) = |\Omega(x, j)|.$$

Clearly an element $x \in S^i$ is a vertex of $\Gamma_i(S)$ if and only if $\omega(x, j) \leq \delta_j$ for each $j \in \{1, \dots, u\}$. In particular the map $\pi : S^\delta \rightarrow S^i$, $(x_1, \dots, x_\delta) \mapsto (x_1, \dots, x_i)$ induces a graph epimorphism from $\Gamma_\delta(S)$ to $\Gamma_i(S)$ and therefore, by Theorem 3.1, $\Gamma_i(S)$ is connected. Our aim is now to obtain a bound on the diameter of $\Gamma_i(S)$. Before giving our main result, we will collect a series of preliminary results.

Theorem 4.1 [4, Theorem 1.2] *If $a, b \in S \setminus \{1\}$, then there exists $c \in S$ with $S = \langle a, c \rangle = \langle b, c \rangle$.*

Lemma 4.2 Let $\alpha = (x_1, \dots, x_{i-1}, a)$ and $\beta = (x_1, \dots, x_{i-1}, b)$ be two vertices of $\Gamma_i(S)$. If a and b are not A -conjugate, then $d_{\Gamma_i(S)}(\alpha, \beta) \leq 2$.

Proof Assume $a \in C_r$ and $b \in C_s$ with $r \neq s$. Let $J = \{1, \dots, i-1\}$, $J_1 = \{j \in J \mid x_j \in C_r\}$, $J_2 = \{j \in J \mid x_j \in C_s\}$. By Theorem 4.1, there exists $c \in S$ with $S = \langle a, c \rangle = \langle b, c \rangle$. Now, since α and β are vertices of $\Gamma_i(S)$, there exist $y_1, \dots, y_{i-1} \in S$ with the properties:

- $\langle x_j, y_j \rangle = S$ for each $j \in J$;
- (x_{j_1}, y_{j_1}) and (x_{j_2}, y_{j_2}) are not A -conjugate if $j_1 \neq j_2$;
- (x_j, y_j) is not A -conjugate to (a, c) if $j \in J_1$;
- (x_j, y_j) is not A -conjugate to (b, c) if $j \in J_2$.

Let $\gamma = (y_1, \dots, y_{i-1}, c)$. The previous properties ensure that $\langle \alpha, \gamma \rangle = \langle \gamma, \beta \rangle = S^i$, so (α, γ, β) is a 2-arc in the graph $\Gamma_i(S)$ and $d_{\Gamma_i(S)}(\alpha, \beta) \leq 2$. $\square$

Lemma 4.3 Assume that $i < \delta$ and let $\alpha = (x_1, \dots, x_i)$, $\beta = (y_1, \dots, y_i)$ be distinct vertices of $\Gamma_i(S)$. If $d_{\Gamma_i(S)}(\alpha, \beta) \leq d$, then there exist $a, b \in S$ such that $\bar{\alpha} = (x_1, \dots, x_i, a)$ and $\bar{\beta} = (y_1, \dots, y_i, b)$ are vertices of Γ_{i+1} and $d_{\Gamma_{i+1}}(\bar{\alpha}, \bar{\beta}) \leq d$.

Proof It suffices to notice that if $S^i = \langle (a_1, \dots, a_i), (b_1, \dots, b_i) \rangle$, then there exist a, b in S with $S^{i+1} = \langle (a_1, \dots, a_i, a), (b_1, \dots, b_i, b) \rangle$. Indeed we take (a, b) with the properties that $\langle a, b \rangle = S$ and (a, b) is not A -conjugate to (a_k, b_k) for each $k \in \{1, \dots, i\}$. $\square$

Theorem 4.4 If $i < \delta$, then the diameter of $\Gamma_i(S)$ is at most $2 + 4(i-1)$.

Proof The proof is by induction on i . It follows immediately from Theorem 4.1 that the diameter of $\Gamma_1(S) = \Gamma(S)$ is 2. So assume that $i > 1$ and let $\alpha = (x_1, \dots, x_i)$, $\beta = (y_1, \dots, y_i)$ be distinct vertices of $\Gamma_i(S)$. Since $i < \delta$, there exist $j \in \{1, \dots, u\}$ and $k \in \{1, \dots, i\}$ such that $\omega(\alpha, j) < \delta_j$ and $x_k \notin C_j$. We want to prove $d_{\Gamma_i(S)}(\alpha, \beta) \leq 2 + 4(i-1)$. Since $d_{\Gamma_i(S)}(\alpha, \beta) = d_{\Gamma_i(S)}((x_{1\sigma}, \dots, x_{i\sigma}), (y_{1\sigma}, \dots, y_{i\sigma}))$ for any $\sigma \in \text{Sym}(i)$, it is not restrictive to assume $k = i$. By induction and Lemma 4.3, there exists $s \in S$ such that, if $\gamma = (x_1, \dots, x_{i-1}, s)$, then $d_{\Gamma_i(S)}(\gamma, \beta) \leq 2 + 4(i-2)$. To conclude our proof we have to show that $d_{\Gamma_i(S)}(\alpha, \gamma) \leq 4$. If s and x_i are not A -conjugate, then $d_{\Gamma_i(S)}(\alpha, \gamma) \leq 2$ by Lemma 4.2. Assume that s, x_i are A -conjugate. There exists $l \neq j$ with $s, x_i \in C_l$. Choose $t \in C_j$ and let $\eta = (x_1, \dots, x_{i-1}, t)$. Clearly $\omega(\eta, v) \leq \omega(\alpha, v) \leq \delta_v$ if $v \neq j$ while $\omega(\eta, j) \leq \omega(\alpha, j) + 1 \leq \delta_j$, hence η is a vertex of $\Gamma_i(S)$. By Lemma 4.2 we conclude $d_{\Gamma_i(S)}(\alpha, \gamma) \leq d_{\Gamma_i(S)}(\alpha, \eta) + d_{\Gamma_i(S)}(\eta, \gamma) \leq 2 + 2 = 4$. $\square$

A more careful work is required in order to obtain a similar bound for the diameter of $\Gamma_\delta(S)$. In particular the set Δ_x , defined as follows, plays a crucial role. Given $x \in S$ with $x \neq 1$, let

$$\Delta_x = \bigcup_{y \in S, \langle x, y \rangle = S} C_A(y) \quad \text{and} \quad D_x = C_A(x) \Delta_x.$$

Lemma 4.5 *There exists an absolute constant $\rho \in \mathbb{N}$ with the following property: if S is a non-abelian simple group, then there exists $x \in S$, $x \neq 1$, with $D_x^\rho = A$. If $|S|$ is large enough, one can take $\rho = 3$.*

Before giving the proof of the Lemma 4.5, we need to recall some known results.

Proposition 4.6 [2, Theorem 5.1] *For every $\epsilon > 0$ there exist $\kappa > 0$ and a threshold n_0 such that, for every $n \geq n_0$, if $x \in \text{Alt}(n)$ has fewer than κn fixed points, then the probability that x and a random element $y \in \text{Alt}(n)$ generate $\text{Alt}(n)$ is at least $1 - \epsilon$.*

Proposition 4.7 [7] *There exists a universal positive constant c such that for an arbitrary non-identity element x in a finite simple group S of Lie type the probability is at least c that $S = \langle x, y \rangle$ for a random $y \in S$.*

Proposition 4.8 [12, Corollary 1] *Let G be a finite group and let k be the minimal degree of a nontrivial complex character of G . Suppose B is a subset of G such that $|B| > |G|/k^{1/3}$. Then $G = B^3$.*

Proof of Lemma 4.5 It is an easy consequence of the classification of the finite simple groups that there exists $1 \neq x \in S$ with the property that $SC_A(x) = A$ (and clearly if $S = \text{Alt}(n)$ then such an element can be chosen with at most 1 fixed point). Let $\Omega_x = \{y \in S \mid \langle x, y \rangle = S\}$: by Propositions 4.6 and 4.7, $|\Omega_x| \geq c^*|S|$ for a suitable constant c^* . Let k be the minimal degree of a nontrivial complex character of S . If we take $|S|$ large enough, we have $k > (1/c^*)^3$ and therefore, by Proposition 4.8, $\Omega_x^3 = S$. On the other hand $\Omega_x \subseteq \Delta_x$ hence $D_x^3 \supseteq C_A(x)\Delta_x^3 \supseteq C_A(x)\Omega_x^3 = C_A(x)S = A$. Thus we proved that there exists $\bar{n} \in \mathbb{N}$ such that $D_x^3 = A$ whenever $|S| \geq \bar{n}$. Notice that in any case $\Omega_x \neq \emptyset$ and D_x contains $\Omega_x \cup C_A(x)$. But then $A = \langle D_x \rangle$ and therefore $D_x^{\rho_S} = A$ for some $\rho_S \in \mathbb{N}$. If we take $\rho = \max\{3, \rho_S \mid |S| \leq \bar{n}\}$, we are ensured that $D_x^\rho = A$ for every choice of S . $\square$

We will say that $(w_0, z_1, w_1, \dots, z_r, w_r)$ is a *symmetric r -path* in the generating graph of S if for each $i \in \{1, \dots, r\}$ there exists $a_i \in C_A(z_i)$ with $w_i = w_{i-1}^{a_i}$ and $\langle z_i, w_i \rangle = \langle z_i, w_{i-1} \rangle = S$.

Lemma 4.9 *Let $w \in S$ with $w \neq 1$ and let $a \in A$. There exists a symmetric r -path in the generating graph of S joining w to w^a if and only if $a \in D_w^r$.*

Proof We make induction on r . So assume that $(w_0, z_1, w_1, \dots, z_r, w_r)$ is a symmetric r -path with $w_0 = w$ and $w_r = w^a$. By induction $w_{r-1} = w^b$ for some $b \in D_w^{r-1}$ and there exists $y \in S$ with $z_r = y^b$. By definition, there is $c \in A$ with $y^{bc} = y^b$ and $w^a = w^{bc}$. In particular $c \in C_A(y^b) = C_A(y)^b$ and $a \in C_A(w)bc \subseteq C_A(w)bcC_A(y)^b = C_A(w)C_A(y)b \subseteq C_A(w)C_A(y)D_w^{r-1}$. To conclude it suffices to notice that $C_A(y) \subseteq \Delta_w$ since $S = \langle w_{r-1}, z_r \rangle = \langle w^b, y^b \rangle = \langle w, y \rangle^b$. $\square$

Lemma 4.10 *Assume that $\alpha = (x_1, \dots, x_{\delta-1}, a)$ and $\beta = (x_1, \dots, x_{\delta-1}, b)$ are two distinct vertices of $\Gamma_\delta(S)$. If there exists a symmetric r -path from a to b , then $d_{\Gamma_\delta(S)}(\alpha, \beta) \leq 2r$.*

Proof We prove the statement by induction on r . First assume $r = 1$ and that (a, c, b) is a symmetric 1-path. In particular (a, c) and (b, c) are A -conjugate. Since α is a vertex of $\Gamma_i(S)$, there exist $y_1, \dots, y_{\delta-1} \in S$ with the properties that, for each $j \in \{1, \dots, \delta - 1\}$, $\langle x_j, y_j \rangle = S$ and (x_j, y_j) is not A -conjugate to (a, c) (and consequently is not A -conjugate to (b, c)). This implies that $S^\delta = \langle \alpha, \gamma \rangle = \langle \beta, \gamma \rangle$, with $\gamma = (y_1, \dots, y_{\delta-1}, c)$. Hence $d_{\Gamma_\delta(S)}(\alpha, \beta) \leq d_{\Gamma_\delta(S)}(\alpha, \gamma) + d_{\Gamma_\delta(S)}(\gamma, \beta) = 1 + 1 = 2$. Now assume that $(w_0, z_1, w_1, \dots, z_r, w_r)$ is a symmetric r -path with $r > 1$, $w_0 = a$ and $w_r = b$. Let $\gamma = (y_1, \dots, y_{\delta-1}, w_{r-1})$. By induction $d_{\Gamma_\delta(S)}(\alpha, \beta) \leq d_{\Gamma_\delta(S)}(\alpha, \gamma) + d_{\Gamma_\delta(S)}(\gamma, \beta) = 2(r - 1) + 2 = 2r$. $\square$

Theorem 4.11 *The diameter of $\Gamma_\delta(S)$ is at most $2 + 4(\delta - 2) + 2\rho$, where ρ is the constant which appears in the statement of Lemma 4.5. In particular $\text{diam}(\Gamma_\delta(S)) \leq 4\delta$ if $|S|$ is large enough.*

Proof Let $\alpha = (x_1, \dots, x_\delta)$, $\beta = (y_1, \dots, y_\delta)$ be distinct vertices of $\Gamma_\delta(S)$. By Lemma 4.5, there exists $j \in \{1, \dots, u\}$ such that $\Delta_x^\rho = \text{Aut}(S)$ for every $x \in C_j$. Since $\omega(\alpha, l) = \delta_l \neq 0$ for each $l \in \{1, \dots, u\}$, it is not restrictive to assume $x_\delta \in C_j$. By Theorem 4.4 and Lemma 4.3, there exists $s \in S$ such that, if $\gamma = (x_1, \dots, x_{\delta-1}, s)$, then $d_{\Gamma_\delta(S)}(\gamma, \beta) \leq 2 + 4(\delta - 2)$. To conclude our proof we have to show that $d_{\Gamma_\delta(S)}(\alpha, \gamma) \leq 2\rho$. Since $\omega(\alpha, j) = \omega(\gamma, j) = \delta_j$ and $x_\delta \in C_j$, we must have $s \in C_j$. By Lemma 4.9, there exists a symmetric ρ -path joining x_δ and s . Therefore by Lemma 4.10, $d_{\Gamma_\delta(S)}(\alpha, \gamma) \leq 2\rho$. $\square$

5 A lower bound for the diameter of $\Gamma_\delta(S)$

We proved in the previous section that $\text{diam}(\Gamma_\delta(S)) \leq 4\delta$ if $|S|$ is large enough. Recall that $\delta = \delta(S) = \frac{P(S)|S|}{|\text{Out}(S)|}$, with $P(S)$ the probability of generating S with two elements. By [10], $P(S)$ tends to 1 as $|S|$ tends to infinity, so our upper bound increases almost linearly with $|S|$. It is not clear how sharp this bound is and it seems an hard problem to find a general good lower bound. However we are able to construct an infinite family of simple groups for which $\text{diam}(\Gamma_\delta(S)) \geq \frac{|S|^{1/3}}{8}$. In particular this ensures the existence of simple groups S the diameter of whose associate graph $\Gamma_\delta(S)$ is arbitrarily large.

Before describing this construction, we need some other general remarks on the graph $\Gamma_\delta(S)$ and its diameter.

Assume, as in the previous section, $S^\delta = \langle x, y \rangle$ and take $C = C_K(x)$. Since $\Gamma_\delta(S)$ is 1-arc transitive, there exists $k \in K$ such that $y = x^k$ and $x = y^k$; in particular $k^2 \in C$. As is well known, $\Gamma_\delta(S)$ is isomorphic to the graph $\Gamma^* = \Gamma(K, C, B = CkC)$ whose vertices are the right cosets of C in K and in which the vertices Ck_1 and Ck_2 are connected if and only if $k_2k_1^{-1} \in B$.

Corollary 5.1 *$d_{\Gamma_\delta(S)}(x, z) \leq r$ if and only if $z = x^h$ with $h \in \bigcup_{1 \leq v \leq r} (kC)^v$.*

Corollary 5.2 *The diameter of the graph $\Gamma_\delta(S)$ is the smallest integer r with the property that $K = \bigcup_{1 \leq v \leq r} C(kC)^v$.*

Corollary 5.3 *Let d be the diameter of the Cayley Graph $\text{Cay}(K, C \cup \{k\})$. We have*

$$\frac{d-1}{2} \leq \text{diam}(\Gamma_\delta(S)) \leq \frac{d+1}{2}.$$

Proof Let $D = C \cup \{k\}$. For $h \in K$, let t be the smallest positive integer with the property that there exist $x_1, x_2, \dots, x_t \in D$ such that $h = x_1 x_2 \cdots x_t$. If $i \leq t-1$ and $x_i = k$, then $x_{i+1} \neq k$ (otherwise $x_i x_{i+1} = k^2 \in C$ could be replaced by an element of D and h could be expressed in a shorter way), hence $h \in C(kC)^v$ for $v \leq (t+1)/2$. Therefore $\text{diam}(\Gamma_\delta(S)) \leq (d+1)/2$. Conversely for each $v \in \mathbb{N}$ we have $C(kC)^v \subseteq D^{2v+1}$, hence $d \leq 2 \text{diam}(\Gamma_\delta(S)) + 1$. $\square$

Now we are ready to prove the main result of this section.

Theorem 5.4 *Let $S = \text{SL}(2, 2^p)$ with p an odd prime. We have $\text{diam}(\Gamma_\delta(S)) \geq 2^{p-2} - 1$ if p is large enough.*

Proof Let $q = 2^p$. We have $|S| = (q^2 - 1)q$ and $A = \text{Aut}(S) = S \rtimes \langle \phi \rangle$ with ϕ the Frobenius automorphism. Note that if $p \neq 3$, then p does not divide $|S|$; in particular $\langle \phi \rangle$ is a Sylow p -subgroup of A . Assume now that $x \in S$ has the property that $|C_A(x)|$ is divisible by p . By Sylow Theorem, $\phi \in C_A(x)^y = C_A(x^y)$ for some $y \in A$. It follows that $x^y \in C_S(\phi) = \text{SL}(2, 2) \cong \text{Sym}(3)$. In particular, exactly two of the u representatives $s_1, \dots, s_u$ for the A -orbits of $S \setminus \{1\}$ satisfy the condition that p divides $|C_A(s_i)|$. More precisely we may assume:

- (1) $|s_1| = 2$ and $|C_A(s_1)| = p \cdot q$;
- (2) $|s_2| = 3$ and $|C_A(s_2)| = p \cdot (q+1)$;
- (3) $C_A(s_i) \leq S$ if $i \geq 3$.

By [10], the probability $P(S)$ of generating a simple group with 2 elements tends to 1 as $|S|$ tends to infinity. In particular if p is large enough, then $\delta = \delta(S) = |S|^2 P(S)/|A| \geq q^3/2p$. Moreover

$$\delta_1 + \delta_2 \leq \frac{d(\Gamma(S), s_1)}{p \cdot q} + \frac{d(\Gamma(S), s_2)}{p(q+1)} \leq \frac{2|S|}{p \cdot q} \leq \frac{2q^2}{p}. \quad (5.1)$$

Recall that $C = \prod_{1 \leq i \leq u} C_A(s_i) \wr \text{Sym}(\delta_i) \leq \text{Aut}(S^\delta) = A \wr \text{Sym}(\delta)$. It follows:

(*) *If $(u_1, \dots, u_\delta)\pi \in C$, then the number of $i \in \{1, \dots, \delta\}$ with $u_i \notin S$ is at most $2q^2/p$.*

Now, as above, assume $S^\delta = \langle x, y \rangle$ with $x = (x_1, \dots, x_\delta)$ and $(y_1, \dots, y_\delta)$. We may choose x and y with the property: if (x_i, y_i) and (y_i, x_i) are not A -conjugate, then there exists i^* such that $x_{i^*} = y_i$ and $y_{i^*} = x_i$. Now let $J = \{i \mid (x_i, y_i) \text{ and } (y_i, x_i) \text{ are not } A\text{-conjugate}\}$. We have already noticed that there exists $k = (a_1, \dots, a_\delta)\sigma \in \text{Aut}(S^\delta)$ such that $y = x^k$ and $x = y^k$. Clearly k can be chosen so that:

- (1) if $i \in J$, then $i\sigma = i^*$ and $a_i = 1$;
- (2) if $i \notin J$, then $i\sigma = i$ and $(x_i, y_i)^{a_i} = (y_i, x_i)$.

If $i \notin J$, then $x_i^{a_i^2} = x_i$ and $y_i^{a_i^2} = y_i$, hence, since $S = \langle x_i, y_i \rangle$, we have $a_i^2 = 1$. Since 2 does not divide $|A/S| = p$, it must be $a_i \in S$. We can conclude:

(**) $a_i \in S$ for each $i \in \{1, \dots, \delta\}$.

By Corollary 5.2, there exist $r \leq \text{diam}(\Gamma_\delta(S))$ and $c_i = (u_{i1}, \dots, u_{i\delta})\sigma_i \in C$ such that $(\phi, \dots, \phi) = c_0kc_1 \cdots kc_r$. On the other hand, by (*) and (**), $c_0kc_1 \cdots kc_r = (w_1, \dots, w_\delta)\rho$ with $w_i \notin S$ for at most $(r+1)2q^2/p$ choices of i . This implies $(r+1)2q^2/p \geq \delta \geq q^3/2p$, hence $\text{diam}(\Gamma_\delta(S)) \geq r \geq \frac{q}{4} - 1$. $\square$

6 The clique number of $\Gamma_\delta(S)$. The case $S = \text{Alt}(5)$

For a given graph Γ , the clique number $\omega(\Gamma)$ of Γ is the size of a largest complete subgraph.

As demonstrated by Liebeck and Shalev [10, Corollary 1.7], Turán's Theorem [14] is useful in bounding the clique number $\omega(\Gamma(S))$ of the generating graph $\Gamma(S)$ when S is a finite simple group. Indeed the probability that a random pair of elements of S generates S tends to 1 as $|S|$ tends to infinity and loosely speaking this says that $\Gamma(S)$ has “many” edges for S a finite simple group. But if a graph has “many” edges, then by Turán's Theorem, it should contain a “large” complete subgraph. More precisely Liebeck and Shalev proved that there exists a positive constant c_1 such that $c_1 \cdot m(S) \leq \omega(\Gamma(S))$ for any finite simple group S where $m(S)$ denotes the minimal index of a proper subgroup in S . The value of $\omega(\Gamma(S))$ has been studied for several classes of simple groups (see for example [3, 5, 9]). In general it is much larger than $m(S)$, for example $\omega(\Gamma(\text{Alt}(n))) = 2^{n-2}$ for n a sufficiently large even integer not divisible by 4. On the other hand, if $\delta = \delta(S)$, then $\omega(\Gamma(S^\delta)) = \omega(\Gamma_\delta(S))$ is at most $(1 + o(1))(m(S))$ [11] so $\omega(\Gamma_i(S))$ decreases drastically with i . However no good lower bound for $\omega(\Gamma_\delta(S))$ is known and it is also open the question whether there exist simple groups S for which $\omega(\Gamma_\delta(S))$ is arbitrarily large. As we noticed in Sect. 2 the girth of $\omega(\Gamma_\delta(S))$ is 3, hence $\omega(\Gamma_\delta(S)) \geq 3$, however it is quite difficult to exhibit complete subgraph of larger size and this led us to ask the following weaker question:

Question 6.1 Is there a non-abelian simple group S for which $\omega(\Gamma_\delta(S)) > 3$?

The following easy result explains why it is so difficult to find a large complete subgraph of $\Gamma_\delta(S)$.

Lemma 6.2 Assume that $g_1, \dots, g_r$ are the vertices of a complete subgraph of $\Gamma_\delta(S)$. In particular $S^\delta = \langle g_1, g_2 \rangle$ and for each $i \in \{3, \dots, r\}$ there exists a word $w_i(x_1, x_2)$ such that $g_i = w_i(g_1, g_2)$. The words $w_3, \dots, w_r$ have the following properties: (*) for each generating pair s_1, s_2 of S , the elements $s_1, s_2, w_3(s_1, s_2), \dots, w_r(s_1, s_2)$ are the vertices of a complete subgraph of the generating graph $\Gamma(S)$ of S .

Table 1 $\text{Aut}(\text{Alt}(5))$ -orbits of $\text{Alt}(5) \setminus \{1\}$

s_i	(12345)	(123)	(12) (34)
δ_i	10	6	3
γ_i	5	6	8

Proof For each $i \in \{1, \dots, \delta\}$, let $\pi_i : S^\delta \rightarrow S$ be the projection on the i th component. Let $\langle s_1, s_2 \rangle = S$. Since $S^\delta = \langle g_1, g_2 \rangle$, there exist $i \in \{1, \dots, \delta\}$ and $a \in \text{Aut}(S)$ such that $(s_1, s_2) = (g_1^{\pi_i}, g_2^{\pi_i})^a$. In particular

$$\begin{aligned} & \{s_1, s_2, w_3(s_1, s_2), \dots, w_r(s_1, s_2)\} \\ &= \{g_1^{\pi_i a}, g_2^{\pi_i a}, w_3(g_1^{\pi_i a}, g_2^{\pi_i a}), \dots, w_r(g_1^{\pi_i a}, g_2^{\pi_i a})\} \\ &= \{g_1^{\pi_i a}, g_2^{\pi_i a}, w_3(g_1, g_2)^{\pi_i a}, \dots, w_r(g_1, g_2)^{\pi_i a}\} \end{aligned}$$

is the set of vertices of a complete subgraph of $\Gamma(S)$. $\square$

One could ask whether a converse of Lemma 6.2 holds:

Question 6.3 Assume that the words $w_3, \dots, w_r$ satisfy property $(*)$ and that $S^\delta = \langle g_1, g_2 \rangle$; does this imply that $\{g_1, g_2, w_3(g_1, g_2), \dots, w_r(g_1, g_2)\}$ induces a complete subgraph of $\Gamma_\delta(S)$?

Another related question concerns the study of the triangles in the graph $\Gamma_\delta(S)$. As we noticed in Sect. 2, if $S^\delta = \langle g_1, g_2 \rangle$ then $\{g_1, g_2, g_1 g_2\}$ induces a triangle in $\Gamma_\delta(S)$. More generally $\{g_1, g_2, w(g_1, g_2)\}$ induces a triangle in $\Gamma_\delta(S)$ whenever w belongs to the set W_S of the words $(x_1^{n_1} x_2^{n_2})^{n_3}$ with $n_1, n_2, n_3 \in \mathbb{Z}$ coprime with $|S|$.

Question 6.4 Is there a triangle $\{g_1, g_2, g_3\}$ in the graph $\Gamma_\delta(S)$ such that $g_3 \notin \{w(g_1, g_2) \mid w \in W_S\}$?

We consider now the particular case $S = \text{Alt}(5)$ with the aim to give an answer to the questions proposed above. In this case $A = \text{Aut}(S) = \text{Sym}(5)$. For positive integers r and s let us say that an element (x, y) of $\text{Alt}(5)^2$ is of type (r, s) if x has order r and y has order s . A set of representatives of the orbits of the conjugacy action of $\text{Sym}(5)$ on the set of (ordered) generating pairs for $\text{Alt}(5)$ consists of 19 elements: four elements of type $(5, 5)$, four elements of type $(5, 3)$, four elements of type $(3, 5)$, two elements of type $(5, 2)$, two elements of type $(2, 5)$, one element of type $(2, 3)$, one element of type $(3, 2)$, and one element of type $(3, 3)$. Hence $\delta = \delta(S) = 19$. There are three orbits for the conjugacy action of $\text{Sym}(5)$ on $\text{Alt}(5)$ and, in the notation introduced at the end of Sect. 2, the information we need to compute the number of vertices, the number of edges and the degree of $\Gamma_{19}(\text{Alt}(5))$ can be summarized in Table 1.

In particular $\Gamma_{19}(\text{Alt}(5))$ is a graph with $2^{45} \cdot 3^{14} \cdot 5^9 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$ vertices, whose degree is equal to $2^{28} \cdot 3^{13} \cdot 5^{13} \cdot 7$. These numbers are so huge that it is

extremely difficult to investigate the properties $\Gamma_{19}(\text{Alt}(5))$ even with the help of a computer.

A first information obtained considering the case $S = \text{Alt}(5)$ is a negative answer to Question 6.3. Let $w = x_1^5 \cdot x_2^5 \cdot x_1^5 \cdot x_2^{11} \cdot x_1^{11} \cdot x_2^{15}$. It can be easily checked that if $\text{Alt}(5) = \langle s_1, s_2 \rangle$, then $\langle s_1, w(s_1, s_2) \rangle = \langle s_2, w(s_1, s_2) \rangle = \text{Alt}(5)$. However, given a pair of generators g_1, g_2 of $\text{Alt}(5)^{19}$, it turns out that neither $\langle g_1, w(g_1, g_2) \rangle$ nor $\langle g_2, w(g_1, g_2) \rangle$ coincides with $\text{Alt}(5)^{19}$.

It is not difficult to check that $\omega(\Gamma(\text{Alt}(5))) = 8$. For example any pair of distinct elements of the set $\{(1, 2, 3), (3, 4, 5), (1, 2, 3, 4, 5), (1, 2, 3, 5, 4), (1, 2, 4, 3, 5), (1, 2, 4, 5, 3), (1, 2, 5, 3, 4), (1, 2, 5, 4, 3)\}$ generates $\text{Alt}(5)$. The following result indicates that the value of $\omega(\Gamma_{19}(\text{Alt}(5)))$ is much smaller.

Lemma 6.5 $\omega(\Gamma_{19}(\text{Alt}(5))) \leq 4$.

Proof For a contradiction assume that $4 < \omega(\Gamma_{19}(\text{Alt}(5)))$. There exist five elements $y_1 = (x_{1,1}, \dots, x_{19,1})$, $y_2 = (x_{1,2}, \dots, x_{19,2})$, $y_3 = (x_{1,3}, \dots, x_{19,3})$, $y_4 = (x_{1,4}, \dots, x_{19,4})$, $y_5 = (x_{1,5}, \dots, x_{19,5})$ which pairwise generate $\text{Alt}(5)^{19}$. Consider the matrix $X = (x_{ij})$ with 19 rows and 5 columns. This matrix X has the following properties:

- (1) the five elements in each row of X pairwise generate $\text{Alt}(5)$ (in particular this implies that any row of X contains at most two elements of order 3);
- (2) any two columns of X correspond to two elements of $\text{Alt}(5)^{19}$ which together generate $\text{Alt}(5)^{19}$ (this implies that the 19 rows of X give a set of representatives for the orbits of the conjugacy action of $\text{Sym}(5)$ on the set of pairs of elements generating $\text{Alt}(5)$).

By property (2), each column of X contains six elements of order 3 and so X contains a total of 30 elements of order 3.

On the other hand, each row contains at most two elements of order 3 and there are at most $10 = \binom{5}{2}$ rows containing exactly two elements of order 3 (this latter statement follows from property (2): there is no 2×2 minor of X with all entries of order 3). This implies that there are at most $9 + 20 = 29 < 30$ elements of order 3 in X . A contradiction. $\square$

It remains to decide whether $\omega(\text{Alt}(5)^{19})$ is 3 or 4. If $\omega(\text{Alt}(5)^{19}) = 4$, then there exist four elements $y_1 = (x_{1,1}, \dots, x_{19,1})$, $y_2 = (x_{1,2}, \dots, x_{19,2})$, $y_3 = (x_{1,3}, \dots, x_{19,3})$, $y_4 = (x_{1,4}, \dots, x_{19,4})$ which pairwise generate $\text{Alt}(5)^{19}$. Consider the matrix $X = (x_{ij})$ with 19 rows and 4 columns. This matrix X has the following properties:

- (1) the four elements in each row of X pairwise generate $\text{Alt}(5)$;
- (2) if $1 \leq i_1 < i_2 \leq 19$ and $1 \leq j_1 \leq j_2 \leq 4$, then the pair $(x_{i_1 j_1}, x_{i_1 j_2})$ and $(x_{i_2 j_1}, x_{i_2 j_2})$ are not $\text{Sym}(5)$ -conjugate.

It took us a long time and several computations to decide whether such a matrix X exists. The first step in dealing with this question was to consider the matrix $Y = (y_{ij})$ defined by setting $y_{ij} = |x_{ij}|$. Easy considerations allowed us to conclude that, up to reordering the rows and the columns, there are only the two following choices for the matrix Y :

$$Y_1 = \begin{pmatrix} 5 & 5 & 5 & 5 \\ 5 & 5 & 3 & 2 \\ 5 & 5 & 3 & 3 \\ 5 & 5 & 2 & 3 \\ 5 & 3 & 5 & 3 \\ 5 & 3 & 2 & 5 \\ 5 & 3 & 3 & 5 \\ 5 & 3 & 5 & 2 \\ 5 & 2 & 5 & 3 \\ 5 & 2 & 3 & 5 \\ 3 & 5 & 3 & 5 \\ 3 & 5 & 2 & 5 \\ 3 & 5 & 5 & 3 \\ 3 & 5 & 5 & 2 \\ 3 & 3 & 5 & 5 \\ 3 & 2 & 5 & 5 \\ 2 & 5 & 5 & 3 \\ 2 & 5 & 3 & 5 \\ 2 & 3 & 5 & 5 \end{pmatrix}, \quad Y_2 = \begin{pmatrix} 5 & 5 & 5 & 2 \\ 5 & 5 & 3 & 2 \\ 5 & 5 & 3 & 3 \\ 5 & 5 & 2 & 3 \\ 5 & 3 & 5 & 3 \\ 5 & 3 & 2 & 5 \\ 5 & 3 & 3 & 5 \\ 5 & 3 & 5 & 5 \\ 5 & 2 & 5 & 3 \\ 5 & 2 & 3 & 5 \\ 3 & 5 & 3 & 5 \\ 3 & 5 & 2 & 5 \\ 3 & 5 & 5 & 3 \\ 3 & 5 & 5 & 5 \\ 3 & 3 & 5 & 2 \\ 3 & 2 & 5 & 5 \\ 2 & 5 & 5 & 3 \\ 2 & 5 & 3 & 5 \\ 2 & 3 & 5 & 5 \end{pmatrix}$$

The second step was to look for matrices X_1 and X_2 whose entries are elements of $\text{Alt}(5)$ satisfying the two conditions described above and whose orders are as described by the matrices Y_1 and Y_2 . The first two columns are easily and essentially uniquely determined: they must contain the entries of a prescribed pair of generators for $\text{Alt}(5)$ ¹⁹. But there are still 38 entries to be determined; using the information on the orders of the elements there are $24^{20} \cdot 20^{12} \cdot 15^6$ possible choices, too many even for approaching the question with the help of a computer. We made several attempts to find possible solutions. In some occasions, we arrived close to a solution determining almost all the entries of the matrix, however it turned out that these partial solutions could not be extended to a full solution. This has led us to conjecture that there were no solutions, but a final desperate attempt produced an unexpected positive solution. We considered a partial solution in which all the entries except 9 in the last column have been fixed and checked with a computer whether arbitrary choices of the remaining nine entries produce a solution. It turned out that these solutions, although rare, exist for both choices of Y . Here we give two of these solutions.

$$X_1 =$$

(1, 2, 3, 4, 5)	(1, 3, 4, 2, 5)	(1, 5, 3, 2, 4)	(1, 5, 2, 3, 4)
(1, 2, 3, 4, 5)	(1, 4, 5, 3, 2)	(3, 5, 4)	(1, 3)(2, 5)
(1, 2, 3, 4, 5)	(1, 5, 2, 4, 3)	(1, 4, 2)	(2, 3, 5)
(1, 2, 3, 4, 5)	(1, 2, 3, 5, 4)	(1, 3)(2, 5)	(2, 4, 3)
(1, 2, 3, 4, 5)	(3, 4, 5)	(1, 2, 4, 3, 5)	(1, 4, 2)
(1, 2, 3, 4, 5)	(2, 5, 3)	(1, 5)(3, 4)	(1, 2, 4, 5, 3)
(1, 2, 3, 4, 5)	(3, 5, 4)	(1, 2, 5)	(1, 5, 3, 2, 4)
(1, 2, 3, 4, 5)	(2, 3, 5)	(1, 3, 4, 2, 5)	(1, 2)(4, 5)
(1, 2, 3, 4, 5)	(1, 3)(2, 4)	(1, 4, 5, 3, 2)	(1, 2, 5)
(1, 2, 3, 4, 5)	(2, 3)(4, 5)	(1, 3, 5)	(1, 5, 3, 4, 2)
(1, 2, 3)	(1, 5, 4, 3, 2)	(3, 5, 4)	(1, 3, 5, 4, 2)
(1, 2, 3)	(1, 3, 5, 2, 4)	(1, 4)(2, 5)	(1, 4, 3, 2, 5)
(1, 2, 3)	(1, 2, 3, 5, 4)	(1, 3, 2, 5, 4)	(1, 5, 4)
(1, 2, 3)	(1, 4, 2, 5, 3)	(1, 5, 3, 4, 2)	(2, 4)(3, 5)
(1, 2, 3)	(3, 4, 5)	(1, 2, 4, 5, 3)	(1, 2, 3, 5, 4)
(1, 2, 3)	(2, 4)(3, 5)	(1, 4, 2, 5, 3)	(1, 2, 4, 3, 5)
(1, 2)(3, 4)	(1, 3, 5, 2, 4)	(1, 4, 5, 2, 3)	(1, 5, 3)
(1, 2)(3, 4)	(1, 2, 3, 4, 5)	(1, 3, 5)	(1, 3, 4, 5, 2)
(1, 2)(3, 4)	(2, 3, 5)	(1, 3, 4, 5, 2)	(1, 3, 5, 2, 4)

$$X_2 =$$

(1, 2, 3, 4, 5)	(1, 3, 4, 2, 5)	(1, 4, 5, 2, 3)	(1, 3)(2, 5)
(1, 2, 3, 4, 5)	(1, 5, 2, 4, 3)	(1, 2, 5)	(2, 3)(4, 5)
(1, 2, 3, 4, 5)	(1, 4, 5, 3, 2)	(2, 4, 5)	(1, 3, 5)
(1, 2, 3, 4, 5)	(1, 2, 3, 5, 4)	(1, 5)(3, 4)	(1, 2, 3)
(1, 2, 3, 4, 5)	(3, 4, 5)	(1, 3, 4, 5, 2)	(1, 4, 2)
(1, 2, 3, 4, 5)	(2, 5, 3)	(1, 3)(2, 4)	(1, 2, 5, 3, 4)
(1, 2, 3, 4, 5)	(3, 5, 4)	(1, 4, 2)	(1, 5, 3, 2, 4)
(1, 2, 3, 4, 5)	(2, 3, 5)	(1, 3, 5, 4, 2)	(1, 3, 4, 5, 2)
(1, 2, 3, 4, 5)	(1, 3)(2, 4)	(1, 5, 4, 2, 3)	(1, 5, 4)
(1, 2, 3, 4, 5)	(2, 3)(4, 5)	(1, 5, 2)	(1, 5, 4, 2, 3)
(1, 2, 3)	(1, 5, 4, 3, 2)	(1, 5, 4)	(1, 3, 4, 2, 5)
(1, 2, 3)	(1, 3, 5, 2, 4)	(1, 4)(2, 5)	(1, 5, 2, 3, 4)
(1, 2, 3)	(1, 2, 3, 5, 4)	(1, 5, 3, 2, 4)	(1, 4, 5)
(1, 2, 3)	(1, 4, 2, 5, 3)	(1, 2, 4, 5, 3)	(1, 4, 5, 2, 3)
(1, 2, 3)	(3, 4, 5)	(1, 2, 4, 3, 5)	(1, 4)(2, 5)
(1, 2, 3)	(2, 4)(3, 5)	(1, 5, 4, 3, 2)	(1, 3, 4, 5, 2)
(1, 2)(3, 4)	(1, 3, 5, 2, 4)	(1, 3, 4, 5, 2)	(1, 5, 4)
(1, 2)(3, 4)	(1, 2, 3, 4, 5)	(2, 5, 4)	(1, 2, 5, 4, 3)
(1, 2)(3, 4)	(2, 3, 5)	(1, 3, 2, 4, 5)	(1, 4, 2, 5, 3)

In particular this gives an affirmative solution to Question 6.1 and implies:

Proposition 6.6 $\omega(\Gamma_{19}(\text{Alt}(5))) = 4$.

Incidentally, we obtained also a solution to Question 6.4. Indeed consider the triangle $\{g_1, g_2, g_3\}$ where g_1, g_2 and g_3 correspond to the columns 1, 2 and 4 of the matrix X_2 . Assume, by contradiction, $g_3 = (g_1^{n_1} g_2^{n_2})^{n_3}$ with $(n_1 n_2 n_3, 30) = 1$. Since

$\pi_{15}(g_1) = (1, 2, 3)$, $\pi_{15}(g_2) = (3, 4, 5)$ and $\pi_{15}(g_3) = (1, 4)(2, 5)$, we would have $(1, 4)(2, 5) = (1, 2, 3)^{m_1}(3, 4, 5)^{m_2}$ with $m_1 m_2 = \pm 1$, but this is false.

Acknowledgement Research partially supported by MIUR-Italy via PRIN Group theory and applications.

References

1. Aschbacher, M., Guralnick, R.M.: Some applications of the first cohomology group. *J. Algebra* **90**(2), 446–460 (1984)
2. Babai, L., Hayes, T.P.: The probability of generating the symmetric group when one of the generators is random. *Publ. Math. (Debr.)* **69**(3), 271–280 (2006)
3. Blackburn, S.R.: Sets of permutations that generate the symmetric group pairwise. *J. Comb. Theory, Ser. A* **113**(7), 1572–1581 (2006)
4. Breuer, T., Guralnick, R.M., Kantor, W.M.: Probabilistic generation of finite simple groups. II. *J. Algebra* **320**(2), 443–494 (2008)
5. Britnell, J.R., Evseev, A., Guralnick, R.M., Holmes, P.E., Maróti, A.: Sets of elements that pairwise generate a linear group. *J. Comb. Theory, Ser. A* **115**(3), 442–465 (2008)
6. Dixon, J.D., Mortimer, B.: *Permutation Groups*. Graduate Texts in Mathematics, vol. 163. Springer, New York (1996)
7. Fulman, J., Guralnick, R.M.: The probability of generating an irreducible subgroup. Preprint (2010)
8. Guralnick, R.M., Kantor, W.M.: Probabilistic generation of finite simple groups. *J. Algebra* **234**(2), 743–792 (2000). Special issue in honor of Helmut Wielandt
9. Holmes, P.E., Maróti, A.: Pairwise generating and covering sporadic simple groups. *J. Algebra* **324**(1), 25–35 (2010)
10. Liebeck, M.W., Shalev, A.: Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky. *J. Algebra* **184**(1), 31–57 (1996)
11. Lucchini, A., Maróti, A.: On the clique number of the generating graph of a finite group. *Proc. Am. Math. Soc.* **137**(10), 3207–3217 (2009)
12. Nikolov, N., Pyber, L.: Product decompositions of quasirandom groups and a Jordan type theorem. *J. Eur. Math. Soc.* **13**(4), 1063–1077 (2011)
13. Wang, Y.M.: Finite groups admitting a fixed-point-free automorphism group. *Northeast. Math. J.* **9**(4), 516–520 (1993)
14. Turán, P.: An extremal problem in graph theory. *Mat. Fiz. Lapok* **48**, 436–452 (1941)