ON THE GENERATING GRAPH OF DIRECT POWERS OF A SIMPLE GROUP

TIMOTHY C. BURNESS AND ELEONORA CRESTANI

ABSTRACT. Let S be a nonabelian finite simple group and let n be an integer such that the direct product S^n is 2-generated. Let $\Gamma(S^n)$ be the generating graph of S^n and let $\Gamma_n(S)$ be the graph obtained from $\Gamma(S^n)$ by removing all isolated vertices. A recent result of Crestani and Lucchini states that $\Gamma_n(S)$ is connected, and in this note we investigate its diameter. A deep theorem of Breuer, Guralnick and Kantor implies that $\mathrm{diam}(\Gamma_1(S)) = 2$, and we define $\Delta(S)$ to be the maximal n such that $\mathrm{diam}(\Gamma_n(S)) = 2$. We prove that $\Delta(S) \geq 2$ for all S, which is best possible since $\Delta(A_5) = 2$, and we show that $\Delta(S)$ tends to infinity as $|S|$ tends to infinity. Explicit upper and lower bounds are established for direct powers of alternating groups.

1. INTRODUCTION

Let G be a finite group that can be generated by two elements and let $\Gamma(G)$ be the generating graph of G; the vertices are the nontrivial elements of G, and two vertices are joined by an edge if and only if they generate G. This fascinating graph encodes many familiar generating properties. For example, G is said to be $\frac{3}{2}$-generated if every nontrivial element of G belongs to a generating pair; this is equivalent to the non-existence of isolated vertices in $\Gamma(G)$. More generally, G has spread at least k if for any k nontrivial elements $x_1, \ldots, x_k \in G$, there exists $y \in G$ such that $G = \langle x_i, y \rangle$ for all i (this notion was introduced by Brenner and Wiegold [3] in the 1970s). Visibly, G has spread at least 2 if and only if $\Gamma(G)$ is connected with diameter 2. Moreover, the graph-theoretic viewpoint suggests many new and natural questions. For instance, one can investigate the connectedness of $\Gamma(G)$ (and subsequently its diameter), its (co-)clique and chromatic numbers, the existence of a Hamiltonian cycle in $\Gamma(G)$, and so on.

Let S be a nonabelian finite simple group. It is well known that S can be generated by two elements, and there is a vast literature in this area. Indeed, many stronger results have been established in recent years. For example, a theorem of Guralnick and Kantor [17] states that S is $\frac{3}{2}$-generated (confirming a conjecture of Steinberg [28]), and a more recent result of the same authors (with Breuer) reveals that S has spread at least 2 (see [5]). In particular, it follows that the generating graph $\Gamma(S)$ has diameter 2. The clique number $\omega(S)$ of $\Gamma(S)$ (that is, the size of the largest complete subgraph) has also been investigated by several authors. In [22], Liebeck and Shalev prove that there is an absolute constant $c > 0$ such that $\omega(S) \geq c \cdot m(S)$ for any S, where $m(S)$ is the minimal index of a proper subgroup of S. In [1], Blackburn shows that if n is a sufficiently large even integer which is indivisible by 4 then $\omega(A_n) = 2^{n-2}$ (and he also proves that this coincides with the chromatic number of $\Gamma(A_n)$); see [7, 23] for related results. Another recent result reveals that $\Gamma(S)$ contains a Hamiltonian cycle if $|S|$ is sufficiently large (see [6]).

Date: August 8, 2012.

2010 *Mathematics Subject Classification.* Primary 20D05, 05E15; Secondary 05C12.

Key words and phrases. Finite simple groups; generating graph; diameter; spread.

Burness is supported by EPSRC grant EP/I019545/1, and he thanks the Dipartimento di Matematica at the Università degli Studi di Padova for their generous hospitality. Crestani is supported by a grant from Fondazione Ing. Aldo Gini. Both authors thank Andrea Lucchini and Pablo Spiga for helpful comments.

Let S^n denote the direct product of n copies of S, and let $\delta(S)$ be the largest positive integer n such that S^n is 2-generated. A formula of Philip Hall [18] states that

$$\delta(S) = \frac{\phi_2(S)}{|\mathrm{Aut}(S)|}$$

where $\phi_2(S)$ denotes the number of ordered pairs (x, y) such that $S = \langle x, y\rangle$. In particular, $\delta(S) = \mathbb{P}(S)|S|/|\mathrm{Out}(S)|$ where $\mathbb{P}(S)$ is the probability that two randomly chosen elements generate S. For example, $\delta(A_5) = 19$. By a striking theorem of Liebeck and Shalev [21] (see also [13, 19]), $\mathbb{P}(S)$ tends to 1 as $|S|$ tends to infinity, whence $\delta(S)$ also tends to infinity.

Let $n \leq \delta(S)$ be a positive integer and consider the generating graph $\Gamma(S^n)$. If $n \geq 2$ then this graph contains isolated vertices, so following [11] we define $\Gamma_n(S)$ to be the graph obtained from $\Gamma(S^n)$ by removing all the isolated vertices. By [11, Theorem 1.1], $\Gamma_n(S)$ is connected, so it is natural to consider its diameter $\mathrm{diam}(\Gamma_n(S))$. Clearly, if $n < \delta(S)$ then $\mathrm{diam}(\Gamma_n(S)) \leq \mathrm{diam}(\Gamma_{n+1}(S))$, and [11, Theorem 1.2] states that $\mathrm{diam}(\Gamma_n(S)) \leq 4n - 2$. In addition, we note that there are examples where the diameter of $\Gamma_{\delta(S)}(S)$ can be arbitrarily large. Indeed, [11, Theorem 1.3] states that if $S = \mathrm{SL}_2(2^p)$, where p is a prime, then $\mathrm{diam}(\Gamma_{\delta(S)}(S)) \geq 2^{p-2} - 1$ if p is sufficiently large.

We define

$$\Delta(S) = \max\{n : \mathrm{diam}(\Gamma_n(S)) = 2\}. \tag{1}$$

Note that $\mathrm{diam}(\Gamma_1(S)) = \mathrm{diam}(\Gamma(S)) = 2$ by the aforementioned theorem of Breuer, Guralnick and Kantor [5, Theorem 1.1], so $\Delta(S) \geq 1$. Our main result is the following:

Theorem 1. *Let S be a nonabelian finite simple group. Then $\mathrm{diam}(\Gamma_2(S)) = 2$, so $\Delta(S) \geq 2$. Moreover, $\Delta(S)$ tends to infinity as $|S|$ tends to infinity.*

In Proposition 3.8 we show that $\Delta(A_5) = 2$, so the lower bound $\Delta(S) \geq 2$ in Theorem 1 is best possible. The next theorem provides explicit bounds on $\Delta(S)$ when S is an alternating group.

Theorem 2. *Let $S = A_n$ be the alternating group of degree $n \geq 5$.*

(i) *If n is odd then*

$$\frac{1}{18}(n^2 - 3n + 2) \leq \Delta(S) \leq \frac{1}{2}(n^2 - 5n + 8).$$

(ii) *If n is even then*

$$\frac{n(n-1)(n-2)}{18(n^2/4 - 1)} \leq \Delta(S) \leq \frac{1}{2}(n^2 - 5n + 6).$$

Remark 1. Note that the lower bound in part (ii) of Theorem 2 is linear in n. We refer the reader to Proposition 3.11 for a quadratic lower bound in the special case where $n = 2p$ with p an odd prime. It would be interesting to know whether or not a quadratic lower bound exists for all even n.

As one might expect, it appears to be much more difficult to obtain explicit bounds when S is a simple group of Lie type. However, the proof of Theorem 1 does provide the following lower bound on $\Delta(S)$. (Here r denotes the untwisted Lie rank of S, which is the rank of the ambient simple algebraic group.)

Theorem 3. *There exists an absolute constant c such that if S is a finite simple group of Lie type of rank r over $\mathbb{F}_q$, where $q = p^f$ with p a prime, then either $S = \mathrm{Sp}_{2r}(2)$, or*

$$\Delta(S) \geq cf^{-1}q^r.$$

Remark 2. Let us make some remarks on the statement of Theorem 3:

(i) The proof of Theorem 1 shows that we can take $c = 1/100$ for the constant.

(ii) The family of symplectic groups over the field of two elements is an anomaly. Indeed, it is well known that this family of groups has some unique generation properties. For example, this is the only infinite family of simple groups with exact spread two (the only other examples are A_5, A_6 and $\Omega_8^+(2)$) – see [5, Corollary 1.3]. The proof of Proposition 5.5 shows that

$$\Delta(\mathrm{Sp}_{2r}(2)) \geq \frac{1}{2r}\phi(2^r+1),$$

where ϕ is the Euler totient function.

(iii) It is difficult to determine the accuracy of the lower bound in Theorem 3, but it is clear that better bounds hold in certain cases. For example, if $S = E_8(q)$ our proof yields $\Delta(S) \geq cf^{-1}q^{50}$ for some constant c (see Remark 5.3 for comments on the case where S is a classical group). Deriving good upper bounds on $\Delta(S)$ when S is a group of Lie type appears to be a difficult problem.

2. Preliminaries

2.1. **Uniform spread.** Let G be a finite group and let X be a subset of G. We say that X has the *uniform spread two* (UST) property if for any two nontrivial elements $a, b \in G$ there exists an $x \in X$ such that $G = \langle a, x\rangle = \langle b, x\rangle$. The main theorem of [5] states that if S is a nonabelian finite simple group then there is at least one conjugacy class in S with the UST property. The basic idea is to choose an element $z \in S$ so that the set $\mathcal{M}(z)$ of maximal subgroups of S containing z is small and can be determined. As explained in [5, Section 2], the class $C = z^S$ has the UST property if

$$\sum_{H\in\mathcal{M}(z)} \mathrm{fpr}(x, S/H) < \frac{1}{2}$$

for all elements $x \in S$ of prime order, where

$$\mathrm{fpr}(x, S/H) = \frac{|x^S \cap H|}{|x^S|} \tag{2}$$

denotes the fixed point ratio of x in its natural action on the set of right cosets S/H. In this way, upper bounds on fixed point ratios play an essential role in the proof of [5, Theorem 1.1].

For the remainder of this preliminary section, let S be a nonabelian finite simple group with automorphism group $A = \mathrm{Aut}(S)$. Define the integer $\Delta(S)$ as in (1).

Proposition 2.1. *Let $C_1, \ldots, C_t$ be distinct A-classes in S with the UST property. Then $\Delta(S) \geq t$.*

Proof. This is entirely straightforward. Let $x = (x_1, \ldots, x_t)$ and $y = (y_1, \ldots, y_t)$ be distinct vertices in the graph $\Gamma_t(S)$. Then each x_i, y_i is nontrivial, so there exists $z_i \in C_i$ such that $S = \langle x_i, z_i\rangle = \langle y_i, z_i\rangle$. Set $z = (z_1, \ldots, z_t) \in S^t$ and consider $L = \langle x, z\rangle$. By construction, $\pi_i(L) = S$ for all i, where π_i denotes the i-th projection map. Moreover, L is not contained in a diagonal subgroup of S^t since z_i and z_j are not A-conjugate, for all $i \neq j$. Therefore $L = S^t$. Similarly, $\langle y, z\rangle = S^t$ and the result follows. □

Let X be a subset of S and let $S^\#$ be the set of nontrivial elements in S. For $a, b \in S^\#$ we define

$$\eta(X, a, b) = \frac{|x \in X \,:\, S = \langle a, x\rangle = \langle b, x\rangle\}|}{|X|}$$

and

$$\eta(X) = \min\{\eta(X,a,b) \,:\, a,b \in S^{\#}\}. \tag{3}$$

Then X has the UST property if and only if $\eta(X) > 0$. By [5, Theorem 1.1], with the exception of a short list of known cases, there exists an S-class $C = z^S$ with $\eta(C) \geq 1/3$. Note that if $C' = z^A$ then C' has the UST property and $\eta(C') = \eta(C)$.

The next result plays a key role in the proof of our main theorems.

Proposition 2.2. *Let $C_i = z_i^A$, $1 \leq i \leq t$, be distinct A-classes in S with the UST property. For each i, set $f_i = \eta(C_i)$ and let k_i be a positive integer such that*

$$f_i|C_i| - 2(k_i - 1)\alpha(S) > 0 \tag{4}$$

where $\alpha(S) = \max\{|C_A(x)| \,:\, x \in S^{\#}\}$. Then $\Delta(S) \geq \sum_i k_i$.

Proof. We may assume $t = 1$. Set $C = C_1$, $z = z_1$, $f = f_1$ and $k = k_1$. It suffices to prove the following claim:

Claim. If k satisfies (4) then any two vertices in $\Gamma_k(S)$ are connected to a vertex of the form $(u_1, \ldots, u_k) \in \Gamma_k(S)$, with $u_i \in C$ for all i.

We proceed by induction on k. Since C has the UST property and $\Gamma_1(S) = \Gamma(S)$, the claim holds when $k = 1$. Now assume $k > 1$, and let $(x_1, \ldots, x_k)$ and $(y_1, \ldots, y_k)$ be vertices in $\Gamma_k(S)$. By induction, the vertices $(x_1, \ldots, x_{k-1})$ and $(y_1, \ldots, y_{k-1})$ in $\Gamma_{k-1}(S)$ are connected to a vertex $(u_1, \ldots, u_{k-1})$, where $u_i \in C$ for all i. In particular, the following conditions hold:

(i) $S = \langle x_i, u_i\rangle = \langle y_i, u_i\rangle$ for all $1 \leq i \leq k-1$;
(ii) For all distinct $i, j \in \{1, \ldots, k-1\}$, the pairs (x_i, u_i) and (x_j, u_j) in S^2 are not A-conjugate, and nor are the pairs (y_i, u_i) and (y_j, u_j).

By definition, there are at least $f|C|$ elements $u \in C$ such that $S = \langle x_k, u\rangle = \langle y_k, u\rangle$. Fix $i < k$ and suppose (x_i, u_i) is A-conjugate to (x_k, u) for some $u \in C$. Then $x_k = x_i^a$ for some $a \in A$ and we deduce that there are precisely $|C_A(x_i)|$ elements $u \in C$ with this property. Similarly, if y_i and y_k are A-conjugate then there are exactly $|C_A(y_i)|$ elements $u \in C$ such that (y_i, u_i) is A-conjugate to (y_k, u). It follows that there are at least

$$f|C| - \sum_{i=1}^{k-1} (|C_A(x_i)| + |C_A(y_i)|) \geq f|C| - 2(k-1)\alpha(S)$$

choices for $u \in C$ such that $(u_1, \ldots, u_{k-1}, u)$ is connected to $(x_1, \ldots, x_k)$ and $(y_1, \ldots, y_k)$. The result now follows since our choice of k ensures that $f|C| - 2(k-1)\alpha(S) > 0$. □

2.2. **Computational methods.** Let S be a nonabelian finite simple group. In some specific cases (see Proposition 2.3, for example) we can use Magma [2] to find S-classes with the UST property. Here we briefly outline our methodology.

First some notation. Let z be a nontrivial element of S and set $C = z^S$. Our aim is to determine whether or not C has the UST property. As above, let $\mathcal{M}(z)$ denote the set of maximal subgroups of S containing z. For $H \in \mathcal{M}(z)$ and $x \in S$ let $\mathrm{fpr}(x, S/H)$ be the fixed point ratio of x (see (2)), and let $\mathbb{P}(x, z)$ be the probability that x and a randomly chosen element of C do *not* generate S. Note that

$$\mathbb{P}(x,z) \leq \sum_{H \in \mathcal{M}(z)} \mathrm{fpr}(x, S/H) =: \sigma(x,z). \tag{5}$$

We start with the standard permutation representation of S used by Magma (so for example, if $S = \mathrm{PSL}_n(q)$ then this representation has degree $(q^n - 1)/(q-1)$). Using the commands MaximalSubgroups and ConjugacyClasses, we can determine the maximal

subgroups of S which contain a conjugate of z; if H is such a subgroup then we can compute the fixed point ratio $\mathrm{fpr}(z, S/H) = |z^S \cap H|/|z^S|$, and we note that z belongs to exactly $|S : H| \cdot \mathrm{fpr}(z, S/H)$ distinct S-conjugates of H. In this way we can determine the subgroups in $\mathcal{M}(z)$, and we can subsequently compute $\sigma(x, z)$ for any $x \in S$.

Now, if $x_1, x_2 \in S$ and $\sigma(x_i, z) < 1/2$ for $i = 1, 2$ then (5) implies that $\mathbb{P}(x_i, z) < 1/2$, so there is some element $z \in C$ such that $S = \langle x_1, z\rangle = \langle x_2, z\rangle$. As previously remarked, if $\sigma(x, z) < 1/2$ for all nontrivial $x \in S$ (equivalently, for all $x \in S$ of prime order), then C has the UST property and we are done. So let us assume that there are some nontrivial S-classes $C_i = x_i^S$, $1 \leq i \leq k$, with $\sigma(x_i, z) \geq 1/2$. For each x_i we compute $\mathbb{P}(x_i, z)$ as follows (see Breuer's notes [4, p.14]). First, we construct a set of $(C_S(z), C_S(x_i))$-double coset representatives. If $r \in S$ is a representative then $\langle x_i, z^{srt}\rangle = \langle x_i, z^r\rangle^t$ for all $s \in C_S(z)$, $t \in C_S(x_i)$, so we only need to test (non)generation for representatives. More precisely, if $r_1, \ldots, r_\ell$ are the representatives with $S \neq \langle x_i, z^{r_j}\rangle$ then

$$\mathbb{P}(x_i, z) = |S|^{-1} \sum_{j=1}^{\ell} |C_S(z) r_j C_S(x_i)|.$$

Subsequently, we define $m = \max\{\mathbb{P}(x_i, z) : 1 \leq i \leq k\}$.

As before, if $m < 1/2$ then C has the UST property, so let us assume $m \geq 1/2$. Note that $\mathbb{P}(x, z) \leq m$ for all $x \in S^\#$. Of course, if $m = 1$ then there exists $x \in S^\#$ such that $S \neq \langle x, z\rangle$ for all $z \in C$, so in this situation C does not have the UST property. Suppose $m < 1$ and let $y_1, y_2 \in S$ be nontrivial elements such that $\sigma(y_1, z) < 1 - m$. Then $\mathbb{P}(y_1, z) < 1 - m$ and $\mathbb{P}(y_2, z) \leq m$, so there exists an element $z \in C$ such that $S = \langle y_i, z\rangle$ for $i = 1, 2$. Therefore, it remains to consider the conjugacy classes $C_i = x_i^S$, $1 \leq i \leq v$, such that $\sigma(x_i, z) \geq 1 - m$. Fix i, j such that $1 \leq i \leq j \leq v$, and let $\{y_1, \ldots, y_t\}$ be a set of representatives of the $C_S(x_i)$-orbits on C_j. For each y_s we have to decide if there exists an element $g \in S$ such that $S = \langle x_i, z^g\rangle = \langle y_s, z^g\rangle$. In practice, the existence of g can usually be established by testing a few randomly chosen elements, but exhaustive searches are required to prove non-existence. If we can always find such elements $g \in S$, for all possible i, j, then $C = z^S$ has the UST property.

By implementing the above procedure in Magma, we obtain the following result (note that the final statement follows immediately from Proposition 2.1).

Proposition 2.3. *Let S be one of the following simple groups:*

$$\mathrm{PSL}_2(q)\ (q < 29,\ q \neq 9),\ \mathrm{PSL}_3^\epsilon(q)\ (q < 11),\ \mathrm{PSL}_4^\epsilon(q)\ (q < 5),\ \mathrm{PSL}_5^\epsilon(2),\ \mathrm{PSL}_6^\epsilon(2),$$

$$\mathrm{Sp}_4(4),\ \mathrm{Sp}_6(2),\ \Omega_7(3),\ \Omega_8^\pm(2),\ {}^2B_2(8),\ A_7$$

Then there are at least two distinct A-classes in S with the UST property. In particular, in each case $\Delta(S) \geq 2$.

Remark 2.4. Let S be one of the groups in the statement of Proposition 2.3. In Table 1 we present an explicit list of S-classes with the UST property (we adopt the Atlas [10] labelling of classes). In all but three cases, the given list is complete. In the third column we implicitly exclude the trivial class, and all classes of involutions. Note that there is a unique class in $\mathrm{PSL}_2(9) \cong A_6$ with the UST property.

3. Alternating groups

Let $S = A_n$ be the alternating group of degree $n \geq 5$. Recall that we define

$$\alpha(S) = \max\{|C_A(x)| : x \in S^\#\},$$

S	Conditions	S-classes with the UST property
$\mathrm{PSL}_2(q)$	$11 < q < 29$	all
	$q = 7, 8$	all
	$q = 5, 11$	all except 3A
	$q = 9$	4A
$\mathrm{PSL}_3(q)$	$q = 3, 4$	all except 3A
	$q = 5$	all except 4A-B, 5A
	$q = 7$	all except 7A
	$q = 8$	all except 7A-F
	$q = 9$	all except 3A, 4A-B, 8A-D
$\mathrm{PSL}_4(q)$	$q = 2$	6B, 15A-B
	$q = 3$	including 4C, 5A, 6A-B, 9A-B, 10A, 12A-C, 13A-D, 20A-B
	$q = 4$	including 4B, 5E, 7A-B, 9A-B, 10A-D, 15E-H, 17A-D, 21A-D, 30A-D, 63A-L, 85A-P
$\mathrm{PSL}_5(2)$		5A, 6B, 8A, 12A, 14A-B, 15A-B, 21A-B, 31A-F
$\mathrm{PSL}_6(2)$		including 7E, 9A, 12A, 14A-B, 15C-E, 21A-B, 31A-F, 63A-F
$\mathrm{PSU}_3(q)$	$q = 3$	6A, 7A-B, 8A-B, 12A-B
	$q = 4$	all except 5A-D
	$q = 5$	all except 3A, 5A
	$q = 7$	all except 4A-B, 7A, 8A-D,
	$q = 8$	all except 3A-B
	$q = 9$	all except 3A, 5A-D, 10A-D
$\mathrm{PSU}_4(q)$	$q = 2$	9A-B, 12A-B
	$q = 3$	5A, 6B-C, 7A-B, 8A, 9A-D, 12A
	$q = 4$	4B, 5M, 6A-B, 10I-P, 13A-D, 15E-P, 17A-D, 20A-D, 30A-D, 51A-H, 65A-P
$\mathrm{PSU}_5(2)$		5A, 6N, 8A, 9C-D, 11A-B, 12E-I, 15A-B, 18A-B
$\mathrm{PSU}_6(2)$		7A, 8B-D, 9C, 10A, 11A-B, 12F-H, 15A, 18A-B
$\mathrm{Sp}_4(4)$		5E, 15A-D, 17A-D
$\mathrm{Sp}_6(2)$		7A, 9A, 12C, 15A
$\Omega_7(3)$		7A, 8B, 9C-D, 12F-G, 13A-B, 14A, 15A, 20A
$\Omega_8^+(2)$		9A-C, 10A-C, 12A-C, 12E-G, 15A-C
$\Omega_8^-(2)$		all except 3A-C, 4A-C, 5A, 6A-C
${}^2B_2(8)$		all
A_7		6A, 7A-B

TABLE 1. Conjugacy classes with the UST property

where A is the automorphism group of S. The next lemma is easily checked (in general, $|C_A(x)|$ is maximal when x is a 3-cycle).

Lemma 3.1. *We have*

$$\alpha(A_5) = 8,\ \alpha(A_6) = 32,\ \alpha(A_8) = 384,\ \alpha(A_n) = 3(n-3)!\ (n \geq 7, n \neq 8).$$

First we handle the alternating groups of small degree.

Proposition 3.2. *If* $n \in \{5, 6, 7, 8\}$ *then* $\mathrm{diam}(\Gamma_2(A_n)) = 2$.

Proof. Set $S = A_n$ and $A = \mathrm{Aut}(S)$. If $n = 7$ or 8 then Proposition 2.3 applies (note that $A_8 \cong \mathrm{PSL}_4(2)$), so let us assume $n = 5$ or 6. In both cases there is a unique A-class of elements in S with the UST property (comprising the elements of order 5 and 4, respectively). Set $G = S \times S$ and let $V \subset G$ be the set of vertices in $\Gamma_2(S)$. First assume $n = 5$. Using MAGMA [2] it is easy to check that $|V| = 59^2$ and V is the union of 16 G-classes, with representatives $\{x_1, \ldots, x_{16}\}$. By random search, for each x_i and $v \in V$ we can find an element $w \in V$ such that $G = \langle x_i, w\rangle = \langle v, w\rangle$, hence $\mathrm{diam}(\Gamma_2(S)) = 2$. The same method applies when $n = 6$ (here $|V| = 359^2$ and V comprises 36 distinct G-classes). □

Proposition 3.3. *If $n \geq 9$ is odd then*

$$\Delta(S) \geq \left\lceil \frac{(n-1)(n-2)}{18} \right\rceil \geq 2.$$

Proof. Let $z \in S$ be an n-cycle and set $C = z^A$. By [5, Proposition 6.7], C has the UST property with corresponding constant $\eta(C) \geq 1/3$ (see (3)). Now $|C| = (n-1)!$ and $\alpha(S) = 3(n-3)!$ (see Lemma 3.1), so the result follows from Proposition 2.2 (setting $t = 1$, $C_1 = C$ and $f_1 = 1/3$). □

Proposition 3.4. *Suppose $n \geq 10$ is even and set $\epsilon = (2, n/2 - 1)$. Then*

$$\Delta(S) \geq \left\lceil \frac{n(n-1)(n-2)}{18(n^2/4 - \epsilon^2)} \right\rceil \geq 2.$$

Proof. Let $z \in S$ be an element with exactly two cycles, of lengths $n/2 \pm \epsilon$, where $\epsilon = (2, n/2 - 1)$. By [5, Proposition 6.3], $C = z^A$ has the UST property and $\eta(C) \geq 1/3$. Now $|C| = n!/(n^2/4 - \epsilon^2)$, $\alpha(S) = 3(n-3)!$ and once again the result follows from Proposition 2.2. □

Corollary 3.5. *The conclusion to Theorem 1 holds if S is an alternating group.*

Remark 3.6. The lower bounds obtained in Propositions 3.3 and 3.4 are respectively quadratic and linear in n. It is natural to ask whether or not a better lower bound can be obtained via Proposition 2.1. Let $z \in S$ be an element such that $C = z^A$ has the UST property. Clearly, if z has four or more cycles then $\langle z, (1,2,3)\rangle$ is intransitive, so z has at most three cycles. In particular, if n is odd then z is either an n-cycle (which is the class used in the proof of Proposition 3.3), or z has exactly three cycles, so there are less than n^2 possibilities for C. This shows that by simply counting classes we cannot do better than a quadratic function in n. Similarly, if n is even then z has exactly two cycles, and so in this situation we cannot improve on a linear bound in n.

Remark 3.7. It would be interesting to determine all the A-classes in S with the UST property, but this appears to be a difficult problem. Now, if $n \geq 15$ is odd and $z \in S$ has cycle-shape (n_1, n_2, n_3), with $n_i \geq 3$ for all i, and $(n_i, n_j) = 1$ for $i \neq j$, then one can show that z^A has the UST property. Indeed, in this situation the analysis is simplified by the fact that z belongs to exactly three maximal subgroups of S, each of which is intransitive (see the proof of [17, Proposition 7.1]), so $S = \langle x, z\rangle$ if and only if $\langle x, z\rangle$ is transitive. Similarly, if $n \geq 10$ is even and $z \in S$ has cycle-shape (n_1, n_2), where n_1 and n_2 are coprime, then z^A has the UST property.

Next we show that the lower bound $\Delta(S) \geq 2$ in Theorem 1 is best possible. We note that $S = A_5$ is the only finite simple group for which the exact value of $\Delta(S)$ is currently known.

Proposition 3.8. *We have* $\mathrm{diam}(\Gamma_3(A_5)) = 3$*, so* $\Delta(A_5) = 2$.

Proof. Let $S = A_5$, $A = S_5$ and set $x = (x_1, x_2, x_3) \in S^3$ and $y = (y_1, y_2, y_3) \in S^3$, where $x_i = (1,2,3)$ and $y_i = (1,3)(4,5)$ for all i. It is easy to check that x and y are non-isolated vertices in $\Gamma(S^3)$. There are exactly 16 elements $s \in S$ such that $S = \langle x_1, s\rangle = \langle y_1, s\rangle$, each of which is a 5-cycle, namely

$$\{(1,2,4,3,5)^i, (1,2,4,5,3)^i, (1,2,5,3,4)^i, (1,2,5,4,3)^i \,:\, 1 \leq i \leq 4\}$$

It is straightforward to check that if z_1, z_2 and z_3 are distinct 5-cycles with this property then two of the z_i are either $C_A(x_1)$-conjugate or $C_A(y_1)$-conjugate. We conclude that there is no $z \in S^3$ such that $S^3 = \langle x, z\rangle = \langle y, z\rangle$, whence $\mathrm{diam}(\Gamma_3(A_5)) \geq 3$ and thus $\Delta(A_5) = 2$, as claimed.

To see that $\mathrm{diam}(\Gamma_3(S)) = 3$ we have to work harder. Let $z_1 = (1,2,3,4,5)$, $z_2 = (1,2,3)$ and $z_3 = (1,2)(3,4)$. Set $C_i = z_i^A$ and note that $S^\# = C_1 \cup C_2 \cup C_3$. Let d_i be the degree of z_i in $\Gamma(S)$ (that is, $d_i = |\{x \in S \,:\, S = \langle x, z_i\rangle\}|$) and set $\delta_i = d_i/|C_A(z_i)|$. In addition, let α_i (respectively β_i, γ_i) be the number of elements z in C_1 (respectively C_2, C_3) such that $S = \langle z, z_i\rangle$. It is straightforward to check that these parameters take the following values:

i	$\lvert C_i\rvert$	δ_i	α_i	β_i	γ_i
1	24	10	20	20	10
2	20	6	24	6	6
3	15	3	16	8	0

Note that $(x_1, \ldots, x_n) \in \Gamma(S^n)$ is non-isolated if and only if $|\{x_r \,:\, x_r \in C_i\}| \leq \delta_i$ for $i = 1,2,3$. In particular, every vertex in $(S^\#)^3$ is non-isolated. We also note the following:

($\star$) Every pair of elements in $C_1 \times C_2$ generates S, while $(u, v) \in C_1 \times C_1$ is a pair of generators if and only if $\langle u\rangle \neq \langle v\rangle$.

Let $x = (x_1, x_2, x_3)$ and $y = (y_1, y_2, y_3)$ be any two vertices of $\Gamma_3(S)$. To complete the proof of the proposition, it suffices to establish the following:

(i) x is connected to two vertices $u = (u_1, u_2, u_3)$ and $v = (u_1, u_2, u_3')$ in $C_1 \times C_2 \times C_1$ with $\langle u_3\rangle \neq \langle u_3'\rangle$;
(ii) y is connected to a vertex in $C_2 \times C_1 \times C_1$;
(iii) Every vertex in $C_2 \times C_1 \times C_1$ is connected to u or v.

First consider (i). A vertex $t = (t_1, t_2, t_3)$ in $C_1 \times C_2 \times C_1$ is connected to x if and only if $S = \langle x_i, t_i\rangle$ for all i and (x_1, t_1) is not A-conjugate to (x_3, t_3) (since t is in $C_1 \times C_2 \times C_1$, (x_2, t_2) cannot be A-conjugate to (x_1, t_1) or (x_3, t_3)). As recorded in the above table, any nontrivial element in S generates with at least 16 elements in C_1 and with at least 6 elements in C_2. Hence, there are at least $16 \cdot 6 = 96$ choices for $(t_1, t_2) \in C_1 \times C_2$ such that $S = \langle x_1, t_1\rangle = \langle x_2, t_2\rangle$.

Let $(u_1, u_2) \in C_1 \times C_2$ be one of these choices and set

$$T_{u_1,u_2} = \{u \in C_1 \,:\, S^3 = \langle x, (u_1, u_2, u)\rangle\},$$

so $u \in T_{u_1,u_2}$ if and only if $u \in C_1$, $S = \langle x_3, u\rangle$ and the pairs (x_1, u_1), (x_3, u) are not A-conjugate. If x_1 and x_3 are not A-conjugate then $|T_{u_1,u_2}| \geq 16$ (in this situation, $u \in T_{u_1,u_2}$ if and only if $u \in C_1$ and $S = \langle x_3, u\rangle$). On the other hand, if $x_3 = x_1^\alpha$ for some $\alpha \in A$ then there are $|C_A(x_1)|$ choices for $y \in C_1$ such that (x_1, u_1) is A-conjugate to (x_3, y). Since x_3 generates with at least 16 elements in C_1, and $|C_A(x_1)| \leq 8$, it follows that $|T_{u_1,u_2}| \geq 8$. Therefore, in every case we have $|T_{u_1,u_2}| \geq 8$, so we can find $u_3, u_3' \in T_{u_1,u_2}$ such that $\langle u_3\rangle \neq \langle u_3'\rangle$. This establishes (i), with $u = (u_1, u_2, u_3)$ and $v = (u_1, u_2, u_3')$. By symmetry, (ii) also holds.

Finally, let us turn to (iii). Let $t = (t_1, t_2, t_3)$ be a vertex in $C_2 \times C_1 \times C_1$. Then u is connected to t if and only if $S = \langle t_i, u_i \rangle$ for all i, so $(\star)$ implies that u is connected to every vertex in the set $\{(t_1, t_2, t_3) \in C_2 \times C_1 \times C_1 : t_3 \notin \langle u_3 \rangle\}$. Similarly, v is connected to every vertex in the set $\{(t_1, t_2, t_3) \in C_2 \times C_1 \times C_1 : t_3 \notin \langle u_3' \rangle\}$. Therefore, (iii) holds and the proof of the proposition is complete. □

We now consider upper bounds on $\Delta(A_n)$, with the aim of establishing Theorem 2.

Proposition 3.9. *Let $S = A_n$ with $n \geq 6$. Set $\xi = 6$ if n is even, otherwise $\xi = 8$. Then*

$$\Delta(S) \leq \frac{1}{2}(n^2 - 5n + \xi).$$

Proof. Let $s = (1, 2, 3) \in S$ and suppose $\sigma \in S$ is a permutation such that $S = \langle s, \sigma \rangle$. Let $\mathrm{fix}(\sigma)$ be the set of fixed points of σ. Since $\langle s, \sigma \rangle$ is transitive, $|\mathrm{fix}(\sigma)| \leq 2$ and σ has at most $3 - |\mathrm{fix}(\sigma)|$ cycles.

First assume n is even. The following three cases arise:

(i) If $|\mathrm{fix}(\sigma)| = 0$ then σ has exactly two cycles (since n is even).
(ii) If $|\mathrm{fix}(\sigma)| = 1$ then σ is an $(n-1)$-cycle, and the fixed point is $1, 2$ or 3.
(iii) If $|\mathrm{fix}(\sigma)| = 2$ then σ has to be an $(n-2)$-cycle, but there are no such permutations in S (since n is even).

Let k be the number of pairwise non-A-conjugate pairs (s, σ) such that $S = \langle s, \sigma \rangle$ and $|\mathrm{fix}(\sigma)| = 0$. Then $k = |F|/|C_A(s)|$, where F is the set of fixed-point-free permutations $\sigma \in S$ with $S = \langle s, \sigma \rangle$. Note that $F \subseteq T$, where

$$T = \{\sigma \in S : |\mathrm{fix}(\sigma)| = 0, \langle s, \sigma \rangle \text{ is transitive}\}.$$

As observed above, if $\langle s, \sigma \rangle$ is transitive and $|\mathrm{fix}(\sigma)| = 0$ then σ has exactly two cycles. Let $1 < a \leq n/2$ be an integer and let T_a be the set of permutations $\sigma \in S$ of shape $(a, n-a)$ such that $\langle s, \sigma \rangle$ is transitive. Note that $T = \bigcup_{a=2}^{n/2} T_a$. It is easy to check that if $a < n/2$ then

$$|T_a| = 3\binom{n-3}{a-1}(a-1)!(n-a-1)! + 3\binom{n-3}{a-2}(a-1)!(n-a-1)! = 3(n-2)!$$

and similarly

$$|T_{n/2}| = \left(\binom{n-3}{n/2-1} + 2\binom{n-3}{n/2-2}\right)(n/2-1)!(n/2-1)! = \frac{3}{2}(n-2)!$$

We conclude that

$$|T| = \sum_{a=2}^{n/2} |T_a| = \sum_{a=2}^{n/2-1} 3(n-2)! + \frac{3}{2}(n-2)! = \frac{3}{2}(n-2)!(n-3).$$

In particular, since $|C_A(s)| = 3(n-3)!$, it follows that

$$k \leq \frac{3}{2}(n-2)!(n-3)/3(n-3)! = \frac{1}{2}(n^2 - 5n + 6).$$

Let $x = (x_1, \ldots, x_k, x_{k+1}) \in \Gamma_{k+1}(S)$ and $y = (y_1, \ldots, y_k, y_{k+1}) \in \Gamma_{k+1}(S)$, where $x_i = (1, 2, 3)$ and $y_i = (4, 5, 6)$ for all i. (Note that x (and also y) is a non-isolated vertex in $\Gamma(S^{k+1})$; indeed, by definition of k there exists $z = (z_1, \ldots, z_{k+1}) \in S^{k+1}$ with $S^{k+1} = \langle x, z \rangle$, where each z_i with $i \leq k$ is a fixed-point-free permutation, and z_{k+1} has a single fixed point.) Since x_i and y_i have disjoint support, there is no element $\sigma \in S$ with fixed points such that $S = \langle x_i, \sigma \rangle = \langle y_i, \sigma \rangle$. In particular, if $z = (z_1, \ldots, z_{k+1}) \in S^{k+1}$ and

$S^{k+1} = \langle x, z\rangle = \langle y, z\rangle$ then each z_i must be fixed-point-free, but the definition of k implies that $\langle x, z\rangle$ is a proper subgroup of S^{k+1}, a contradiction. We conclude that

$$\Delta(S) \leq k \leq \frac{1}{2}(n-2)(n-3).$$

A similar argument applies when n is odd. Here the following three cases arise:

(i) If $|\mathrm{fix}(\sigma)| = 0$ then σ has at most three cycles, so either σ is an n-cycle, or σ has exactly three cycles.
(ii) If $|\mathrm{fix}(\sigma)| = 1$ then σ has exactly two cycles, and the fixed point is $1, 2$ or 3.
(iii) If $|\mathrm{fix}(\sigma)| = 2$ then σ is an $(n-2)$-cycle and $\mathrm{fix}(\sigma) = \{1,2\}, \{1,3\}$ or $\{2,3\}$.

Define k, F and T as before, and set

$$P = \{\sigma \in S \,:\, |\mathrm{fix}(\sigma)| = 0,\ \langle s, \sigma\rangle \text{ is primitive}\} \subseteq T.$$

Note that if $n = 3m$ and σ is a permutation with precisely three cycles of length m then $\langle s, \sigma\rangle$ is contained in a maximal imprimitive subgroup of S of type $S_3 \wr S_m$.

In order to define certain subsets of P and T, set

$$I = \{a \in \mathbb{Z} \,:\, 0 \leq a \leq (n-3)/2,\ a \neq 1,\ a \neq n/3\}$$

and

$$J = \{(a,b) \in \mathbb{Z}^2 \,:\, 2 \leq a \leq \lfloor (n-3)/3\rfloor,\ a+1 \leq b \leq \lfloor (n-a-1)/2\rfloor\}.$$

For $a \in I$, let $P_{a,a}$ (respectively $T_{a,a}$) be the set of permutations $\sigma \in S$ of shape $(a, a, n-2a)$ such that $\langle s, \sigma\rangle$ is primitive (respectively transitive). Similarly, for $(a,b) \in J$ let $P_{a,b}$ (respectively $T_{a,b}$) be the set of permutations $\sigma \in S$ of shape $(a, b, n-a-b)$ such that $\langle s, \sigma\rangle$ is primitive (respectively transitive). Note that

$$P = \bigcup_{a\in I} P_{a,a} \cup \bigcup_{(a,b)\in J} P_{a,b} \subseteq \bigcup_{a\in I} T_{a,a} \cup \bigcup_{(a,b)\in J} T_{a,b}.$$

It is straightforward to check that $|T_{0,0}| = (n-1)!$ and

$$|T_{a,a}| = 3\binom{n-3}{a-1}(a-1)!\binom{n-a-2}{a-1}(a-1)!(n-2a-1)! = 3(n-3)!$$

if $a \in I$ is non-zero. Similarly, if $(a,b) \in J$ then

$$|T_{a,b}| = 6\binom{n-3}{a-1}(a-1)!\binom{n-a-2}{b-1}(b-1)!(n-(a+b)-1)! = 6(n-3)!$$

and we calculate that

$$|I| = \begin{cases} \frac{1}{2}(n-3) - 1 & \text{if 3 divides } n \\ \frac{1}{2}(n-3) & \text{otherwise} \end{cases}$$

and

$$|J| = \sum_{a=2}^{\lfloor (n-3)/3\rfloor} (\lfloor (n-a-1)/2\rfloor - a) = \begin{cases} \frac{1}{12}(n^2 - 12n + 39) & \text{if 3 divides } n \\ \frac{1}{12}(n^2 - 12n + 35) & \text{otherwise.} \end{cases}$$

Therefore,

$$|P| \leq \sum_{a\in I} |T_{a,a}| + \sum_{(a,b)\in J} |T_{a,b}| = (n-1)! + 3(n-3)!(|I|-1) + 6(n-3)!|J|$$

and thus

$$k = |F|/3(n-3)! \leq |P|/3(n-3)! \leq \begin{cases} \frac{1}{6}(3n^2 - 15n + 22) & \text{if 3 divides } n \\ \frac{1}{6}(3n^2 - 15n + 24) & \text{otherwise} \end{cases}$$

since $|C_A(s)| = 3(n-3)!$. We now complete the argument as in the n even case to get

$$\Delta(S) \leq k \leq \frac{1}{2}(n^2 - 5n + 8)$$

as required. □

By combining Propositions 3.3 and 3.9, we obtain the following quadratic bounds on $\Delta(S)$ when S is an alternating group of odd degree.

Corollary 3.10. *If $n \geq 9$ is odd then*

$$\frac{1}{18}(n^2 - 3n + 2) \leq \Delta(A_n) \leq \frac{1}{2}(n^2 - 5n + 8).$$

This completes the proof of Theorem 2. Note that when n is even, Proposition 3.4 provides a linear lower bound on $\Delta(A_n)$. As the next result demonstrates, a quadratic lower bound can be established in some special cases.

Proposition 3.11. *Suppose $S = A_n$, where $n = 2p$ with $p > 3$ a prime. Then*

$$\Delta(S) \geq \frac{1}{48}(n^2 - 8n + 12).$$

Proof. Let C_h be the S_n-class of permutations in S of shape $(a, 2p-a)$, where $a = 2h+1$ is odd and $1 \leq h \leq (p-3)/2$. Let $\sigma_1, \sigma_2 \in S$ be nontrivial permutations and set

$$\zeta(C_h, \sigma_1, \sigma_2) := \{z \in C_h \,:\, S = \langle z, \sigma_1\rangle = \langle z, \sigma_2\rangle\}$$

and

$$\zeta(C_h) = \min\{|\zeta(C_h, \sigma_1, \sigma_2)| \,:\, \sigma_1, \sigma_2 \in S^{\#}\}.$$

Note that $\zeta(C_h) = |C_h|\eta(C_h)$ (see (3)). Since a is odd and $a \leq p-2$, it follows that the integers a and $2p-a$ are coprime, whence $S = \langle z, \sigma_i\rangle$ if and only if $\langle z, \sigma_i\rangle$ is transitive. We claim that

$$\zeta(C_h) \geq 3\binom{n-4}{a-2}(a-1)!(n-a-1)! \tag{6}$$

Clearly, in order to establish this lower bound, we may assume that each σ_i has prime order. Write $\sigma_1 = \sigma_{1,1}\ldots\sigma_{1,r}$ and $\sigma_2 = \sigma_{2,1}\ldots\sigma_{2,s}$ as disjoint cycles, where each $\sigma_{i,j}$ has prime length. There are two cases to consider.

First suppose $\sigma_{1,a} = \sigma_{2,b}$ for some a, b. In this case,

$$|\zeta(C_h, \sigma_1, \sigma_2)| \geq 2\binom{n-2}{a-1}(a-1)!(n-a-1)! \geq 2(n-2)! \geq 3(n-4)!(a-1)(n-a-1)$$

and the desired bound follows.

Now assume $\sigma_{1,a} \neq \sigma_{2,b}$ for all a, b. Given $\pi \in S_n$ let $\mathrm{supp}(\pi)$ denote the support of π. Then there exists $\{x_1, x_2\} \in \mathrm{supp}(\sigma_{1,1})$ and $\{y_1, y_2\} \in \mathrm{supp}(\sigma_{2,1})$ such that either $\{x_1, x_2\} \cap \{y_1, y_2\} = \emptyset$ or $\{x_1, x_2\} \cap \{y_1, y_2\} = \{x_1\} = \{y_1\}$. In the former situation we have

$$|\zeta(C_h, \sigma_1, \sigma_2)| \geq 4\binom{n-4}{a-2}(a-1)!(n-a-1)!$$

while in the latter case we calculate that

$$|\zeta(C_h, \sigma_1, \sigma_2)| \geq \left(\binom{n-3}{a-1} + \binom{n-3}{a-2}\right)(a-1)!(n-a+1)! \geq 3\binom{n-4}{a-2}(a-1)!(n-a-1)!$$

This establishes the lower bound in (6).

Now Lemma 3.1 states that $\alpha(S) = 3(n-3)!$, so Proposition 2.2 yields

$$\Delta(S) \geq \sum_{h=1}^{\frac{1}{2}(p-3)} \frac{\zeta(C_h)}{6(n-3)!}.$$

Finally, by using the lower bound on $\zeta(C_h)$ in (6), we calculate that

$$\Delta(S) \geq \sum_{h=1}^{\frac{1}{2}(p-3)} \frac{3\binom{2p-4}{2h-1}(2h)!(2p-2h-2)!}{6(2p-3)!} = \frac{(p-1)(p-3)(2p-1)}{12(2p-3)} > \frac{1}{48}(n-2)(n-6)$$

as required. □

4. Sporadic groups

Proposition 4.1. *The conclusion to Theorem 1 holds if S is a sporadic group.*

Proof. Let S be a sporadic simple group and let $z \in S$ be an element in the S-class recorded in the second column of [5, Table 7]. Then [5, Lemma 6.1] states that $C = z^A$ has the UST property with corresponding constant $\eta(C) \geq 1/3$ (see (3)) and the desired bound $\Delta(S) \geq 2$ quickly follows from Proposition 2.2. (Note that $\alpha(S)$ can be easily calculated from the character table of S – see [10].) For example, if $S = \mathrm{M}_{11}$ and we take $C = z^S$ to be the class `11A` then $|C| = 720$, $\eta(C) = 1/3$, $\alpha(S) = 48$ and we deduce that $\Delta(S) \geq 3$. The remaining cases are entirely similar. □

5. Classical groups

In this section we establish Theorems 1 and 3 for classical groups.

Proposition 5.1. *Let S be a finite simple classical group over $\mathbb{F}_q$ with automorphism group A. Write $q = p^f$ where p is a prime. Then $\alpha(S) \leq \Lambda$, where Λ is given in Table 2.*

Proof. Let $G = \mathrm{Inndiag}(S)$ be the group of inner-diagonal automorphisms of S. Define d and Q as in Table 2. Let $x \in S$ be an element of prime order and define the integer $\nu(x)$ as in [8, Definition 3.16] (so $\nu(x)$ is the codimension of the largest eigenspace of a lift $\hat{x} \in \mathrm{GL}(V)$ of x on $V \otimes \bar{\mathbb{F}}_q$, where V is the natural S-module). Note that $C_A(x) \subseteq C_A(x^i)$ for all $i \geq 1$, so we only need to consider elements of prime order.

First assume $S = \mathrm{PSL}_n(q)$. If $n = 2$ then it is easy to check that $|C_G(x)| \leq d(q+1)$ and thus $|C_A(x)| \leq df(q+1)$ since $|A:G| = f$. If $n \geq 3$ then [8, Corollary 3.38] implies that $|x^G| > \frac{1}{2}q^{2n-2}$, so $|C_G(x)| < 2q^{n^2-2n+1}$ (since $|G| < q^{n^2-1}$) and we deduce that $|C_A(x)| < 4fq^{n^2-2n+1}$ since $|A:G| = 2f$. An entirely similar argument applies when S is a unitary group.

Next suppose $S = \mathrm{PSp}_n(q)'$. First observe that if x is a transvection then

$$|x^G| = \frac{|\mathrm{Sp}_n(q)|}{|\mathrm{Sp}_{n-2}(q)|q^{2n-1}} = q^n - 1.$$

Now, if $n = 4$ and q is even then it is easy to check that $|C_G(x)|$ is maximal when x is a transvection, so $|C_G(x)| \leq q^4(q^2-1)$ and thus $|C_A(x)| \leq fq^4(q^2-1)$ (note that a transvection is not centralized by a graph automorphism of S). On the other hand, if $n = 4$ and q is odd then $|C_G(x)| \leq 2|\mathrm{Sp}_2(q)|^2 = 2q^2(q^2-1)^2$, so $|C_A(x)| \leq 2fq^2(q^2-1)^2$. Now assume $n \geq 6$. If x is not a transvection then $\nu(x) \geq 2$ and thus [8, Corollary 3.38] yields $|x^G| > \frac{1}{4}Q^{-1}q^{2n-4}$. We deduce that transvections have the largest centralizers, so $|C_G(x)| < q^{n(n-1)/2}$ and thus $|C_A(x)| < fq^{n(n-1)/2}$.

S	Conditions	Λ
$\mathrm{PSL}_n(q)$	$n \geq 3$	$4fq^{n^2-2n+1}$
$\mathrm{PSL}_2(q)$		$df(q+1)$
$\mathrm{PSU}_n(q)$	$n \geq 3$	$4fQq^{n^2-2n+1}$
$\mathrm{PSp}_n(q)$	$n \geq 6$	$fq^{\frac{1}{2}n(n-1)}$
$\mathrm{PSp}_4(q)'$		$2fq^2(q^2-1)^2$
$\mathrm{P}\Omega_n^\epsilon(q)$	$n \geq 8$, n even, $(n,\epsilon) \neq (8,+)$	$8fQq^{\frac{1}{2}n^2-\frac{5}{2}n+6}$
$\mathrm{P}\Omega_8^+(q)$		$6fq^{18}$
$\Omega_n(q)$	nq odd, $n \geq 7$	$4fq^{\frac{1}{2}n^2-\frac{3}{2}n+1}$

$d = (2, q-1)$, $f = \log_p q$, $Q = (q+1)/q$

TABLE 2. Upper bounds $\alpha(S) \leq \Lambda$, S classical

Finally, let us assume S is an orthogonal group. If n is even and $(n,\epsilon) \neq (8,+)$ then we apply [8, Corollary 3.38] as before, noting that $\nu(x) \geq 2$ since $x \in S$. Similarly, if $(n,\epsilon) = (8,+)$ then $|x^G|$ is minimal when x is a long root element, in which case $|C_G(x)| = q^{12}(q^2-1)^3$ and thus $|C_A(x)| < 6fq^{18}$ since $|A:G| = 6f$. Finally, suppose n is odd. We claim that $|C_G(x)| < 2q^{n^2/2-3n/2+1}$. If $\nu(x) \geq 2$ then [8, Corollary 3.38] gives $|x^G| > \frac{1}{4}Q^{-1}q^{2n-6}$ and the claim follows. On the other hand, if $\nu(x) = 1$ then x is an involution and $|C_G(x)| \leq 2|\mathrm{SO}_{n-1}^-(q)| < 2q^{n^2/2-3n/2+1}$. This justifies the claim and we conclude that $|C_A(x)| < 4fq^{n^2/2-3n/2+1}$. □

Proposition 5.2. *The conclusions to Theorems 1 and 3 hold when $S = \mathrm{PSL}_n(q)$.*

Proof. First assume $n = 2$. If $q < 29$ (and $q \neq 9$) then Proposition 2.3 applies, so we may assume $q \geq 29$ (note that $\mathrm{PSL}_2(9) \cong A_6$, so Proposition 3.2 applies in this case). Then Proposition 5.1 states that $\alpha(S) \leq df(q+1)$, and [5, Proposition 5.24] provides an A-class C with $\eta(C) \geq 1/3$ (see (3)) and $|C| \geq q(q-1)$. Therefore, by applying Proposition 2.2, we deduce that

$$\Delta(S) \geq \left\lceil \frac{q(q-1)}{6df(q+1)} \right\rceil \geq 2.$$

Now consider the general case $n \geq 3$. Here $\alpha(S) \leq 4fq^{n^2-2n+1}$ and by inspecting [5, Table 5 and Section 5.12] we see that there exists an A-class C of regular semisimple elements with $\eta(C) \geq 1/3$. Therefore, $|C| > \frac{1}{2}q^{n(n-1)}$ and thus Proposition 2.2 implies that

$$\Delta(S) \geq \left\lceil \frac{q^{n-1}}{48f} \right\rceil.$$

This bound is sufficient unless $n = 3$ (with $q < 11$), $n = 4$ (with $q < 5$) or $(n,q) = (5,2)$, $(6,2)$. In each of these exceptional cases, Proposition 2.3 applies. □

Remark 5.3. The lower bounds obtained in the proof of Proposition 5.2 are good enough to establish Theorems 1 and 3 when $S = \mathrm{PSL}_n(q)$, but they can be improved. For example, suppose $S = \mathrm{PSL}_n(q)$ with $n \geq 12$. Let $z \in S$ be a regular semisimple element which lifts to an element $\hat{z} \in \mathrm{SL}_n(q)$ of order $\mathrm{lcm}(q^e-1, q^{n-e}-1)/(q-1)$, where

$$e = \begin{cases} (n+1)/2 & \text{if } n \text{ is odd} \\ n/2+2 & \text{if } n \equiv 2 \pmod 4 \\ n/2+1 & \text{if } n \equiv 0 \pmod 4. \end{cases}$$

(Here $\hat{z}$ preserves a decomposition $V = U \oplus W$ of the natural $\mathrm{SL}_n(q)$-module V, acting irreducibly on both U and W, with $\dim U = e$. Also note that $(e, n-e) = 1$.) By [5, Proposition 5.23], the S-class $C = z^S$ has the UST property, with $\eta(C) \geq 1/2$. Indeed, $\hat{z}$ is contained in exactly two maximal subgroups of $\mathrm{SL}_n(q)$; namely, the stabilizers of the subspaces U and W. Let N be the number of distinct A-classes in S containing regular semisimple elements of this form. By considering the possible eigenvalues of $\hat{z}$ (in $\overline{\mathbb{F}}_q$), it is easy to see that

$$N \geq \frac{\phi((q^e-1)/(q-1))}{e} \cdot \frac{\phi((q^{n-e}-1)/(q-1))}{n-e} \cdot \frac{1}{|\mathrm{Out}(S)|} =: N'$$

where ϕ is the Euler totient function. Therefore, by arguing as in the proof of Proposition 5.2, using Proposition 2.2, we obtain the better lower bound

$$\Delta(S) \geq \left\lceil \frac{q^{n-1}N'}{48f} \right\rceil.$$

By carefully inspecting [5, Section 5], similar lower bounds on the number of A-classes with the UST property can be derived for any classical group S. However, we do not have a good *upper* bound on $\Delta(S)$ when S is a group of Lie type, so the accuracy of the improved lower bounds is difficult to determine.

Proposition 5.4. *The conclusions to Theorems 1 and 3 hold when $S = \mathrm{PSU}_n(q)$.*

Proof. If $n = 3$ (and $q < 11$), $n = 4$ (and $q < 5$) or $(n, q) = (5, 2), (6, 2)$ then Proposition 2.3 applies, so let us assume otherwise. By inspecting [5, Propositions 5.21, 5.22], it follows that there exists an A-class C with $\eta(C) \geq 1/3$ and

$$|C| \geq \frac{|\mathrm{GU}_n(q)|}{(q^{n-1}+1)(q+1)} > \frac{1}{2}\left(\frac{q^{n-1}}{q^{n-1}+1}\right) q^{n(n-1)}.$$

As before, by applying Proposition 2.2 and the upper bound on $\alpha(S)$ recorded in Table 2, we deduce that

$$\Delta(S) \geq \left\lceil \frac{1}{48f}\left(\frac{q}{q+1}\right)\left(\frac{q^{n-1}}{q^{n-1}+1}\right) q^{n-1} \right\rceil.$$

This bound is sufficient unless $(n, q) = (7, 2)$. Here

$$\alpha(S) = 2^{12}|\mathrm{GU}_5(2)|, \quad |C| \geq \frac{|\mathrm{GU}_7(2)|}{2^7+1}$$

(see [5, Proposition 5.21]) and by applying Proposition 2.2 we deduce that $\Delta(S) \geq 6$. □

Proposition 5.5. *The conclusions to Theorems 1 and 3 hold when $S = \mathrm{PSp}_n(q)'$.*

Proof. First assume $n = 4$. If $2 < q < 5$ then Proposition 2.3 applies (see Proposition 3.2 for the case $q = 2$, since $\mathrm{PSp}_4(2)' \cong A_6$). Suppose $q \geq 5$. By [5, Propositions 5.8, 5.12], there exists an A-class C with $|C| \geq q^4(q^2-1)^2$ and $\eta(C) \geq 1/3$. In the usual way, via Propositions 2.2 and 5.1, we deduce that $\Delta(S) \geq \lceil q^2/12f \rceil$ and the result follows.

Now assume $n \geq 6$. The case $q = 2$ requires special attention; indeed, this is one of the exceptional cases recorded in [5, Theorem 1.1]. By [5, Proposition 5.8], if $z \in S$ is an irreducible element of order $2^{n/2}+1$ then $C = z^S$ has the UST property. Now there are precisely $\phi(2^{n/2}+1)/n$ distinct A-classes of such elements, so Proposition 2.1 implies that

$$\Delta(S) \geq \frac{1}{n}\phi(2^{n/2}+1).$$

It is easy to check that this bound implies that $\Delta(S) \geq 2$ when $8 \leq n \leq 14$. In general, if we write $2^{n/2}+1 = \prod_i p_i^{a_i}$, where the p_i are distinct primes, then

$$\phi(2^{n/2}+1) = \prod_i \phi(p_i^{a_i}) = \prod_i p_i^{a_i-1}(p_i-1) \geq \prod_i p_i^{a_i/2} = (2^{n/2}+1)^{\frac{1}{2}}.$$

The subsequent bound

$$\Delta(S) \geq \left\lceil \frac{1}{n}(2^{n/2}+1)^{\frac{1}{2}} \right\rceil$$

is sufficient for all $n \geq 16$. The case $(n,q) = (6,2)$ is covered by Proposition 2.3.

Finally, let us assume $n \geq 6$ and $q \geq 3$. By inspecting [5, Propositions 5.8, 5.10, 5.12], we see that there exists an A-class C with $\eta(C) \geq 1/3$ and

$$|C| \geq \frac{|\mathrm{Sp}_n(q)|}{(q^{n/2-1}+1)(q+1)} > \frac{1}{2}\left(\frac{q^{n/2-1}}{q^{n/2-1}+1}\right) q^{\frac{1}{2}n^2}.$$

The desired result now follows in the usual way via Proposition 2.2, using the upper bound on $\alpha(S)$ given in Table 2. □

Proposition 5.6. *The conclusions to Theorems 1 and 3 hold when* $S = \mathrm{P}\Omega_n^\epsilon(q)$.

Proof. We may assume $n \geq 7$. First suppose $(n,\epsilon) = (8,+)$. If $q = 2$ then Proposition 2.3 applies. Now if $q = 3$ then [5, Table 3] indicates that there is an A-class $C = z^A$ in S with the UST property, where $|z| = 20$ and $\eta(C) \geq 2(1 - 195/455) = 67/455$ (here z preserves an orthogonal decomposition $8^+ = 4^- \perp 4^-$ of the natural S-module into nondegenerate 4-spaces of minus type). We calculate that

$$|C| = 3\frac{|\mathrm{SO}_8^+(3)|}{3^4-1}, \;\; \alpha(S) = 6|\mathrm{Sp}_2(3)||\mathrm{SO}_4^+(3)|3^9$$

and thus Proposition 2.2 implies that $\Delta(S) \geq 34$. Similarly, if $q = 4$ then [5, Table 3] provides an A-class $C = z^A$ in S with $|z| = 65$ (preserving a decomposition $8^+ = 2^- \perp 6^-$), $\eta(C) \geq 1/3$ and

$$|C| = 3\frac{|\mathrm{SO}_8^+(4)|}{(4^3+1)(4+1)}, \;\; \alpha(S) = 3|\mathrm{Sp}_2(4)||\mathrm{SO}_4^+(4)|4^9.$$

Once again, the desired result follows by applying Proposition 2.2.

Next assume $(n,\epsilon) = (8,+)$ and $q \geq 5$. By [5, Lemma 5.15], there is an A-class C with

$$|C| \geq \frac{|\mathrm{SO}_8^+(q)|}{(2,q)(q^2+1)^2} > \frac{1}{2}\left(\frac{q^2}{q^2+1}\right)^2 q^{24}$$

and $\eta(C) \geq 1/3$. According to Proposition 5.1, we have $\alpha(S) \leq 6fq^{18}$, so Proposition 2.2 implies that

$$\Delta(S) \geq \left\lceil \frac{1}{72f}\left(\frac{q^2}{q^2+1}\right)^2 q^6 \right\rceil.$$

It is easy to check that this bound is always sufficient.

For the remainder we may assume that $(n,\epsilon) \neq (8,+)$. We first deal with the case where n is odd and $q = 3$. Note that if $n \equiv 1 \pmod 4$ then S is one of the exceptional cases recorded in [5, Theorem 1.1]. In view of Proposition 2.3, we may assume that $n \geq 9$. By [5, Propositions 5.7, 5.19], there is an A-class C in S such that

$$|C| \geq \frac{|\mathrm{SO}_n(3)|}{3(3^{(n-3)/2}+1)} > \frac{1}{2}\left(\frac{3^{(n-3)/2}}{3^{(n-3)/2}+1}\right) 3^{\frac{1}{2}n^2-n+\frac{1}{2}}$$

and $\eta(C) \geq 1/3$. By combining this lower bound with the upper bound on $\alpha(S)$ given in Proposition 5.1, we quickly deduce that Proposition 2.2 yields

$$\Delta(S) \geq \left\lceil \frac{1}{48f}\left(\frac{3^{(n-3)/2}}{3^{(n-3)/2}+1}\right) 3^{\frac{1}{2}(n-1)} \right\rceil$$

S	$E_8(q)$	$E_7(q)$	$E_6(q)$	$F_4(q)$	$G_2(q)'$
Λ	$fq^{57}\lvert E_7(q)\rvert$	$fq^{33}\lvert \mathrm{SO}_{12}^+(q)\rvert$	$2fq^{21}\lvert \mathrm{SL}_6(q)\rvert$	$fq^{15}\lvert \mathrm{Sp}_6(q)\rvert$	$2f\lvert \mathrm{SU}_3(q)\rvert$

${}^2E_6(q)$	${}^2F_4(q)'$	${}^2G_2(q)'$	${}^2B_2(q)$, $q>2$	${}^3D_4(q)$
$2fq^{21}\lvert \mathrm{SU}_6(q)\rvert$	$fq^{10}\lvert {}^2B_2(q)\rvert$	fq^3	fq^2	$3fq^9\lvert \mathrm{SL}_2(q^3)\rvert$

$f=\log_p q$

TABLE 3. Upper bounds $\alpha(S)\leq \Lambda$, S exceptional

and this bound is sufficient unless $n=9$. Here $\alpha(S)=2|\mathrm{SO}_8^+(3)|$ and there is an A-class C such that $\eta(C)\geq 1/3$ and $|C|=|\mathrm{SO}_9(3)|/82$ (see [5, Proposition 5.7]). In the usual way, via Proposition 2.2, we deduce that $\Delta(S)\geq 7$.

The remaining cases are very similar. By inspecting [5, Sections 5.6, 5.8, 5.9] it follows that there is an A-class $C=z^A$ in S of regular semisimple elements such that $\eta(C)\geq 1/3$ and

$$|C|\geq \frac{|\mathrm{SO}_n^\epsilon(q)|}{(2,q)(q+1)^3q^{r-3}}>\frac{1}{2}\left(\frac{q}{q+1}\right)^3 q^{\frac{1}{2}n^2-n+\iota},$$

where r denotes the rank of S, and $\iota=1/2$ if n is odd, otherwise $\iota=0$. The result now follows in the usual way, via Propositions 5.1 and 2.2. For example, if n is even then we deduce that

$$\Delta(S)\geq \left\lceil \frac{1}{96f}\left(\frac{q}{q+1}\right)^4 q^{\frac{3}{2}n-6}\right\rceil,$$

and this bound is sufficient unless $(n,q)=(8,2)$, which is one of the cases handled in Proposition 2.3. □

6. Exceptional groups

Here we complete the proof of Theorems 1 and 3 by dealing with the exceptional groups of Lie type.

Proposition 6.1. *Let S be a finite simple exceptional group of Lie type over $\mathbb{F}_q$, where $q=p^f$ with p a prime. Then $\alpha(S)\leq\Lambda$, where Λ is given in Table 3.*

Proof. Detailed information on the conjugacy classes in S can be found in the literature, and the result follows by inspecting the relevant lists of conjugacy class sizes. For example, let $S=E_8(q)$ and let $x\in S$ be an element of prime order. The sizes of the unipotent classes in S are conveniently listed in [20, Table 22.2.1], and it is easy to see that $|C_S(x)|\leq q^{57}|E_7(q)|$, with equality if and only if x is a long root element. For semisimple x, the possibilities for $|C_S(x)|$ are listed in [16] and it is easy to check that $|C_S(x)|\leq |E_7(q)||\mathrm{SL}_2(q)|$. Since $|A:S|=f$ (where $A=\mathrm{Aut}(S)$) we conclude that $\alpha(S)\leq fq^{57}|E_7(q)|$ as claimed. The other cases are very similar and we leave the reader to check the details. (See [15, 20] for the sizes of conjugacy classes in $E_7(q)$ and $E_6^\epsilon(q)$; [24, 26] for $F_4(q)$, [9, 14] for $G_2(q)$, [25] for ${}^2F_4(q)$, [30] for ${}^2G_2(q)$, [29] for ${}^2B_2(q)$ and [12, 27] for ${}^3D_4(q)$.) □

Proposition 6.2. *The conclusion to Theorem 1 holds when S is a finite simple exceptional group of Lie type.*

Proof. By [5, Lemma 6.2], there exists an A-class $C = z^A$ of regular semisimple elements in S with $\eta(C) \geq 1/3$ (see [17, Propositions 6.1, 6.2]). The desired result now follows via Proposition 2.2, using the upper bound on $\alpha(S)$ in Proposition 6.1 and a suitable lower bound on $|C|$. For example, suppose $S = G_2(q)'$. If $q = 2$ then $S \cong \mathrm{PSU}_3(3)$ and thus Proposition 5.4 applies. For $q > 2$ we have $|C| > \frac{1}{2}Q^{-2}q^{12}$ (where $Q = (q+1)/q$ as before) and $\alpha(S) < 2fq^8$, so Proposition 2.2 yields

$$\Delta(S) \geq \left\lceil \frac{1}{24f} \left(\frac{q}{q+1} \right)^2 q^4 \right\rceil.$$

It is easy to check that this bound gives the desired result. Similarly, if $S = {}^2G_2(q)'$ (so that $q = 3^{2m+1}$ for some positive integer m) then

$$|C| \geq \frac{|{}^2G_2(q)|}{(q^{1/2}+1)^2} > \frac{1}{2} \left(\frac{q^{1/2}}{q^{1/2}+1} \right)^2 q^6$$

and we deduce that

$$\Delta(S) \geq \left\lceil \frac{1}{12f} \left(\frac{q^{1/2}}{q^{1/2}+1} \right)^2 q^2 \right\rceil.$$

This bound is sufficient if $q > 3$, while Proposition 5.2 applies if $q = 3$ (since $S \cong \mathrm{PSL}_2(8)$). The remaining cases are entirely similar. □

This completes the proof of Theorems 1 and 3.

References

[1] S.R. Blackburn, *Sets of permutations that generate the symmetric group pairwise*, J. Combin. Theory Ser. A **113** (2006), 1572–1581.

[2] W. Bosma, J. Cannon and C. Playoust, *The* Magma *algebra system I: The user language*, J. Symbolic Comput. **24** (1997), 235–265.

[3] J.L. Brenner and J. Wiegold, *Two-generator groups* I, Michigan Math. J. **22** (1975), 53–64.

[4] T. Breuer, *GAP computations concerning the probabilistic generation of finite simple groups*, preprint (arXiv:07103267)

[5] T. Breuer, R.M. Guralnick and W.M. Kantor, *Probabilistic generation of finite simple groups,* II, J. Algebra **320** (2008), 443–494.

[6] T. Breuer, R.M. Guralnick, A. Lucchini, A. Maróti, and G.P. Nagy, *Hamiltonian cycles in the generating graph of finite groups*, Bull. London Math. Soc. **42** (2010), 621–633.

[7] J.R. Britnell, A. Evseev, R.M. Guralnick, P.E. Holmes and A. Maróti, *Sets of element that pairwise generate a linear group*, J. Combin. Theory Ser. A **115** (2008), 442–465.

[8] T.C. Burness, *Fixed point ratios in actions of finite classical groups,* II, J. Algebra **309** (2007), 80–138.

[9] B. Chang, *The conjugate classes of Chevalley groups of type* (G_2), J. Algebra **9** (1968), 190–211.

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

[11] E. Crestani and A. Lucchini, *The non-isolated vertices in the generating graph of direct powers of simple groups*, J. Alg. Combin., to appear.

[12] D. I. Deriziotis and G. Michler, *Character table and blocks of the finite simple triality groups* ${}^3D_4(q)$, Trans. Amer. Math. Soc. **303** (1987) 39–70.

[13] J.D. Dixon, *The probability of generating the symmetric group*, Math. Z. **110** (1969), 199–205.

[14] H. Enomoto, *The conjugacy classes of Chevalley groups of type* (G_2) *over finite fields of characteristic 2 or 3*, J. Fac. Sci. Univ. Tokyo **16** (1970), 497–512.

[15] P. Fleischmann and I. Janiszczak, *The semisimple conjugacy classes of finite groups of Lie type* E_6 *and* E_7, Comm. Alg. **21** (1993), 93–161.

[16] P. Fleischmann and I. Janiszczak, *The semisimple conjugacy classes and the generic class number of the finite simple groups of Lie type* E_8, Comm. Alg. **22** (1994), 2221–2303.

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

[18] P. Hall, *The Eulerian functions of a group*, Quarterly J. Math. **7** (1936), 134–151.
[19] W.M. Kantor and A. Lubotzky, *The probability of generating a finite classical group*, Geom. Dedicata **36** (1990), 67–87.
[20] M.W. Liebeck and G.M. Seitz, *Unipotent and nilpotent classes in simple algebraic groups and Lie algebras*, Amer. Math. Soc. Monographs and Surveys series, volume 180, 2012.
[21] M.W. Liebeck and A. Shalev, *The probability of generating a finite simple group*, Geom. Dedicata **56** (1995), 103–113.
[22] M.W. Liebeck and A. Shalev, *Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky*, J. Algebra **184** (1996), 31–57.
[23] A. Lucchini and A. Maróti, *On the clique number of the generating graph of a finite group*, Proc. Amer. Math. Soc. **137** (2009), 3207–3217.
[24] K. Shinoda, *The conjugacy classes of Chevalley groups of type* (F_4) *over finite fields of characteristic* 2, J. Fac. Sci. Univ. Tokyo **21** (1974), 133–159.
[25] K. Shinoda, *The conjugacy classes of the finite Ree groups of type* (F_4), J. Fac. Sci. Univ. Tokyo **22** (1975), 1–15.
[26] T. Shoji, *The conjugacy classes of Chevalley groups of type* (F_4) *over finite fields of characteristic* $p \neq 2$, J. Fac. Sci. Univ. Tokyo **21** (1974), 1–17.
[27] N. Spaltenstein, *Caractères unipotents de* ${}^3D_4(\mathbb{F}_q)$, Comment. Math. Helv. **57** (1982), 676–691.
[28] R. Steinberg, *Generators for simple groups*, Canad. J. of Math. **14** (1962), 277–283.
[29] M. Suzuki, *On a class of doubly transitive groups*, Annals of Math. **75** (1962), 105–145.
[30] H. N. Ward, *On Ree's series of simple groups*, Trans. Amer. Math. Soc. **121** (1966), 62–89.

Timothy C. Burness, School of Mathematics, University of Southampton, Southampton SO17 1BJ, UK

E-mail address: t.burness@soton.ac.uk

Eleonora Crestani, School of Mathematics, University of Southampton, Southampton SO17 1BJ, UK

Also affiliated with:

Dipartimento di Matematica, Università degli Studi di Padova, Via Trieste 63, 35121 Padova, Italy

E-mail address: crestani.eleonora@gmail.com