GENERATING SETS OF FINITE GROUPS

PETER J. CAMERON, ANDREA LUCCHINI, AND COLVA M. RONEY-DOUGAL

Abstract. We investigate the extent to which the exchange relation holds in finite groups G. We define a new equivalence relation $\equiv_{\mathrm{m}}$, where two elements are equivalent if each can be substituted for the other in any generating set for G. We then refine this to a new sequence $\equiv_{\mathrm{m}}^{(r)}$ of equivalence relations by saying that $x \equiv_{\mathrm{m}}^{(r)} y$ if each can be substituted for the other in any r-element generating set. The relations $\equiv_{\mathrm{m}}^{(r)}$ become finer as r increases, and we define a new group invariant $\psi(G)$ to be the value of r at which they stabilise to $\equiv_{\mathrm{m}}$.

Remarkably, we are able to prove that if G is soluble then $\psi(G) \in \{d(G), d(G)+1\}$, where $d(G)$ is the minimum number of generators of G, and to classify the finite soluble groups G for which $\psi(G) = d(G)$. For insoluble G, we show that $d(G) \leq \psi(G) \leq d(G)+5$. However, we know of no examples of groups G for which $\psi(G) > d(G)+1$.

As an application, we look at the *generating graph* $\Gamma(G)$ of G, whose vertices are the elements of G, the edges being the 2-element generating sets. Our relation $\equiv_{\mathrm{m}}^{(2)}$ enables us to calculate $\mathrm{Aut}(\Gamma(G))$ for all soluble groups G of nonzero spread, and give detailed structural information about $\mathrm{Aut}(\Gamma(G))$ in the insoluble case.

1. Introduction

It is well known that generating sets for groups are far more complicated than generating sets for, say, vector spaces. The latter satisfy the exchange axiom, and hence any two irredundant sets have the same cardinality. According to the Burnside Basis Theorem, a similar property holds for groups of prime power order.

Our starting point is the observation that, in order to understand better the generating sets for arbitrary finite groups, we should investigate the extent to which the exchange property holds. We define an equivalence relation $\equiv_{\mathrm{m}}$ on a finite group G, in which two elements are equivalent if each can be substituted for the other in any generating set for G. Then two elements are equivalent if and only if they lie in the same maximal subgroups of G.

We refine this relation to a sequence of relations $\equiv_{\mathrm{m}}^{(r)}$ whose terms depend on a positive integer r, where two elements are equivalent if each can be

Date: January 9, 2017.

Key words and phrases. finite group, generation, generating graph.

The second and third authors were supported by Università di Padova (Progetto di Ricerca di Ateneo: Invariable generation of groups).

substituted for the other in any r-element generating set. The relations $\equiv_{\mathrm{m}}^{(r)}$ become finer as r increases; we observe in Lemma 2.4 that the smallest value of r for which $\equiv_{\mathrm{m}}^{(r)}$ is not the universal relation is the minimum number $d(G)$ of generators of G.

We define a new group invariant $\psi(G)$ to be the value of r at which the relations $\equiv_{\mathrm{m}}^{(r)}$ stabilise to $\equiv_{\mathrm{m}}$. Remarkably, it turns out (see Corollary 2.12) that if G is soluble then $\psi(G) \in \{d(G), d(G)+1\}$. In Theorem 2.21 we even succeed in giving a precise structural description of the finite soluble groups G for which $\psi(G) = d(G)$.

In the general case, we show in Corollary 2.13 and Proposition 2.14 that $\psi(G) \leq d(G)+5$, with tighter bounds when G is (almost) simple. However, we know of no examples of groups G for which $\psi(G) > d(G)+1$.

The relation $\equiv_{\mathrm{m}}$ can be a little tricky to work with, so in Section 3 we introduce a far simpler relation, by defining $x \equiv_{\mathrm{c}} y$ if $\langle x \rangle = \langle y \rangle$. This is clearly a refinement of $\equiv_{\mathrm{m}}$, and provides an easy-to-calculate upper bound on the number of $\equiv_{\mathrm{m}}$-classes, and lower bound on their sizes. In Theorem 3.4 we characterise the soluble groups G on which these two relations coincide; it would be very interesting to determine for which insoluble groups they are equal.

As an application, we notice that the relation $\equiv_{\mathrm{m}}^{(2)}$ is particularly interesting for two-generator groups. Such groups G have long been studied by means of the *generating graph*, whose vertices are the elements of G, the edges being the 2-element generating sets. The generating graph was defined by Liebeck and Shalev in [16], and has been further investigated by many authors: see for example [3, 5, 6, 12, 18, 19, 20, 23] for some of the range of questions that have been considered. Many deep structural results about finite groups can be expressed in terms of the generating graph.

We notice that two group elements are $\equiv_{\mathrm{m}}^{(2)}$-equivalent if and only if they have the same neighbours in the generating graph. By identifying the vertices in each equivalence class, we obtain a reduced graph $\overline{\Gamma}(G)$, which has many fewer vertices, but the same spread, clique number and chromatic number, amongst other properties. We conjecture that in a group G of nonzero spread, the equivalence relations $\equiv_{\mathrm{m}}$ and $\equiv_{\mathrm{m}}^{(2)}$ coincide.

The automorphism groups of generating graphs are extremely large, and their study has up to now seemed intractable. However, we show in Theorem 5.2 that the automorphism group of $\Gamma(G)$ has a very compact description in terms of the sizes of the $\equiv_{\mathrm{m}}^{(2)}$-classes of G, and the group $\mathrm{Aut}(\overline{\Gamma}(G))$. Using this, we are able to give a precise description of the automorphism groups of the generating graphs of all soluble groups of nonzero spread, and a detailed description in the insoluble case.

We have carried out many computational experiments on small insoluble groups G of nonzero spread. In each case we found that $\psi(G) = 2$, and that

$\mathrm{Aut}(\Gamma(G))$ is completely and straightforwardly determined by the sizes of the $\equiv_{\mathrm{m}}^{(2)}$-classes and $\mathrm{Aut}(G)$.

The paper is structured as follows. In Section 2 we study the relations $\equiv_{\mathrm{m}}$ and $\equiv_{\mathrm{m}}^{(r)}$, and the related invariant $\psi(G)$. In Section 3 we look at the relation $\equiv_{\mathrm{c}}$. In Section 4 we introduce the generating graph $\Gamma(G)$ and the reduced generating graph $\overline{\Gamma}(G)$, and then in Section 5 we study the group $\mathrm{Aut}(\Gamma(G))$ for groups G of nonzero spread.

2. A hierarchy of equivalences

2.1. **Definitions and elementary results.** We shall now introduce our main families of relations, and establish a few basic results concerning them.

Definition 2.1. Let G be a finite group. We define an equivalence relation $\equiv_{\mathrm{m}}$ (m for "maximal subgroups") on G by letting $x \equiv_{\mathrm{m}} y$ if and only if x and y lie in exactly the same maximal subgroups of G.

Note that the $\equiv_{\mathrm{m}}$-class containing the identity is precisely the Frattini subgroup of G, and any $\equiv_{\mathrm{m}}$-class is a union of cosets of the Frattini subgroup.

The equivalence relation $\equiv_{\mathrm{m}}$ can also be characterised by a substitution property:

Proposition 2.2. *Let G be a finite group, and let x and y be elements of G. Then $x \equiv_{\mathrm{m}} y$ if and only if*

$$(\forall r)(\forall z_1, \ldots, z_r \in G)((\langle x, z_1, \ldots, z_r\rangle = G) \Leftrightarrow (\langle y, z_1, \ldots, z_r\rangle = G)).$$

Proof. Suppose first that $\langle x, z_1, \ldots, z_r\rangle = G$ but $\langle y, z_1, \ldots, z_r\rangle \neq G$. Then there is a maximal subgroup M of G containing $y, z_1, \ldots, z_r$. Clearly $x \notin M$; so $x \not\equiv_{\mathrm{m}} y$.

Conversely, suppose that $x \not\equiv_{\mathrm{m}} y$, so that (without loss of generality) there is a maximal subgroup M containing y but not x. Choose generators $z_1, \ldots, z_r$ for M. Then $\langle y, z_1, \ldots, z_r\rangle = M$, but $\langle x, z_1, \ldots, z_r\rangle$ properly contains M, and so is equal to G. $\square$

This means that, when considering generating sets (of any cardinality) for a group G, we may restrict our attention to subsets of a set of $\equiv_{\mathrm{m}}$-class representatives.

Definition 2.3. For any positive integer r, define equivalence relations $\equiv_{\mathrm{m}}^{(r)}$ by the rule that $x \equiv_{\mathrm{m}}^{(r)} y$ if and only if

$$(\forall z_1, \ldots, z_{r-1} \in G)((\langle x, z_1, \ldots, z_{r-1}\rangle = G) \Leftrightarrow (\langle y, z_1, \ldots, z_{r-1}\rangle = G)).$$

Lemma 2.4. (1) *The relations $\equiv_{\mathrm{m}}^{(r)}$ get finer as r increases.*

(2) *The smallest value of r for which $\equiv_{\mathrm{m}}^{(r)}$ is not the universal relation is $d(G)$. For $r = d(G)$, there are at least $r + 1$ equivalence classes.*

(3) *The limit value of this sequence of relations is $\equiv_{\mathrm{m}}$.*

Proof. (1) Choosing z_{r-1} to be the identity we see that $x \equiv_{\mathrm{m}}^{(r)} y$ implies $x \equiv_{\mathrm{m}}^{(r-1)} y$.

(2) The first claim is clear, for this second, notice that the identity and the elements of any $d(G)$-element generating set are pairwise inequivalent.

(3) This is clear. □

Definition 2.5. Let $\psi(G)$ be the value of r for which the equivalences $\equiv_{\mathrm{m}}^{(r)}$ stabilise, that is, the least r such that $\equiv_{\mathrm{m}}^{(r)}$ coincides with the limiting relation $\equiv_{\mathrm{m}}$.

2.2. **Bounds on $\psi(G)$.** In this subsection, we prove various upper and lower bounds on $\psi(G)$ in terms of other numerical invariants of G. We start with some straightforward lower bounds on $\psi(G)$.

Lemma 2.6. *Let G be a finite group, and let $d = d(G)$. Then $\psi(G) \geq d$, and if G has a normal subgroup N such that $N \not\leq \mathrm{Frat}(G)$ and $d(G/N) = d$, then $\psi(G) \geq d + 1$.*

Proof. The first claim is immediate from Lemma 2.4(2). For the second, notice that elements of N lie in no d-element generating set of G, and so are $\equiv_{\mathrm{m}}^{(d)}$-equivalent to the identity. However, the $\equiv_{\mathrm{m}}$-equivalence class of the identity is $\mathrm{Frat}(G)$. □

These lower bounds are best possible in a very strong sense: we know of no groups that do not attain them.

Problem 2.7. Is it true that if G is a finite group, then $\psi(G) \in \{d(G), d(G)+1\}$?

Whilst we are not able to answer this question in general, in the rest of this subsection we prove some upper bounds on $\psi(G)$. In particular, in Corollary 2.12 we show that if G is soluble then $\psi(G) \leq d(G) + 1$.

Definition 2.8. Let G be a finite group and let M be a core-free maximal subgroup of G. For every $g \in G \setminus M$, let $\delta_{G,M}(g)$ be the smallest cardinality of a subset X of M with the property that $G = \langle g, X \rangle$ and let

$$\nu_M(G) = \sup_{g \notin M} \delta_{G,M}(g).$$

Notice that $\nu_M(G) \leq d(M)$.

Definition 2.9. Let $\tilde{m}(G)$ be the maximum of $\nu_{M/N}(G/N)$ over all maximal subgroups M of G, where $N = \mathrm{Core}_G(M)$.

Theorem 2.10. $\psi(G) \leq \max\{\tilde{m}(G), d(G)\} + 1$.

Before proving this result, we briefly recall a necessary definition and result. Given a subset X of a finite group G, we will denote by $d_X(G)$ the smallest cardinality of a set of elements of G generating G together with the elements of X. The following generalizes a result originally obtained by W. Gaschütz [10] for $X = \emptyset$.

Lemma 2.11 ([6] Lemma 6)**.** *Let X be a subset of G and N a normal subgroup of G and suppose that $\langle g_1, \ldots, g_k, X\rangle N = G$. If $k \geq d_X(G)$, then there exist $n_1, \ldots, n_k \in N$ so that $\langle g_1 n_1, \ldots, g_k n_k, X\rangle = G$.*

Proof of Theorem 2.10. Let $t = \max\{\tilde{m}(G), d(G)\}$. Since the relations $\equiv_{\mathrm{m}}^{(r)}$ become finer with r, it suffices to prove that if x and y are two elements of G and $x \not\equiv_{\mathrm{m}} y$, then $x \not\equiv_{\mathrm{m}}^{(t+1)} y$. So assume that $x \not\equiv_{\mathrm{m}} y$. It is not restrictive to assume that there exists a maximal subgroup M of G such that $x \notin M$ and $y \in M$. Let $N = \mathrm{Core}_G(M)$ and let $X = \{x\}$. Since $t \geq \tilde{m}(G)$, we have $t \geq \nu_{M/N}(G/N)$, hence there exist $g_1, \ldots, g_t \in M$ such that $\langle x, g_1, \ldots, g_t\rangle N = G$. Moreover $t \geq d(G) \geq d_X(G)$. So we deduce from Lemma 2.11 that there exist $n_1, \ldots, n_t \in N$ such that $G = \langle x, g_1 n_1, \ldots, g_t n_t\rangle$. On the other hand $\langle y, g_1 n_1, \ldots, g_t n_t\rangle \leq M$. Hence $x \not\equiv_{\mathrm{m}}^{(t+1)} y$. □

We are now able to prove a tight upper bound on $\psi(G)$ for all finite soluble groups G.

Corollary 2.12. *If G is a finite soluble group, then $\psi(G) \leq d(G) + 1$.*

Proof. Let M be a maximal subgroup of G, and let $K = \mathrm{Core}_G(M)$. Then $\tilde{G} = G/K$ is a soluble group with a faithful primitive action on the cosets of M/K, and $d(\tilde{G}) \leq d(G)$. Moreover M/K is a complement in $\tilde{G}$ of $\mathrm{Soc}(\tilde{G})$, so $\nu_{M/K}(G/K) \leq d(M/K) = d(\tilde{G}/\mathrm{Soc}(\tilde{G})) \leq d(\tilde{G}) \leq d(G)$. This holds for every maximal subgroup of G, so $\tilde{m}(G) \leq d(G)$ and the conclusion follows from Theorem 2.10. □

Now we prove an upper bound on $\psi(G)$ for an arbitrary finite group G.

Corollary 2.13. *If G is a finite group, then $\psi(G) \leq d(G)+5$. Furthermore, if G is simple, then $\psi(G) \leq 5$, and if G is almost simple then $\psi(G) \leq 7$.*

Proof. Burness, Liebeck and Shalev prove (see [4, Theorem 7]) that the point stabiliser of a d-generated finite primitive permutation group can be generated by $d + 4$ elements. Hence if G is a finite group, then $\tilde{m}(G) \leq d(G) + 4$ and our first claim follows from Theorem 2.10.

In the same paper (see [4, Theorems 1 and 2]) they show that any maximal subgroup of a finite simple group can be generated by 4 elements, and that any maximal subgroup of an almost simple group can be generated by 6 elements. Hence our final two claims follow in the same way. □

We conclude this subsection by mentioning a relationship with another well-known parameter, $\mu(G)$, the maximum size of a minimal generating set for G (a generating set for which no proper subset generates), studied by Diaconis and Saloff-Coste, Whiston, Saxl, and others [9, 14, 27].

Proposition 2.14. *Let G be a finite group. Then $\psi(G) \leq \mu(G)$. Hence if $G = \mathrm{PSL}_2(p)$ with $p \notin \{7, 11, 19, 31\}$ then $\psi(G) \leq 3$, and $\psi(\mathrm{PSL}_2(p)) \leq 4$ in the remaining cases.*

Proof. To prove that $\psi(G) \leq \mu(G)$, we show that if $\mu = \mu(G)$, and $x \equiv_{\mathrm{m}}^{(\mu)} y$, then $x \equiv_{\mathrm{m}} y$. So suppose that $x \equiv_{\mathrm{m}}^{(\mu)} y$, and let $G = \langle x, z_1, \ldots, z_{r-1}\rangle$.

Case $r \leq \mu$. Since the relations $\equiv_{\mathrm{m}}^{(r)}$ get finer as r increases, in this case $G = \langle y, z_1, \ldots, z_{r-1}\rangle$.

Case $r > \mu$. In this case, our generating set is larger than μ, and so some element is redundant. If x is redundant, then $G = \langle z_1, \ldots, z_{r-1}\rangle = \langle y, z_1, \ldots, z_{r-1}\rangle$, as required. Suppose that x is not redundant. Then G is generated by a subset of the given generators of size μ including x, without loss of generality $\{x, z_1, \ldots, z_{\mu-1}\}$. Since, by assumption, $x \equiv_{\mathrm{m}}^{(\mu)} y$, we have $G = \langle y, z_1, \ldots, z_{\mu-1}\rangle = \langle y, z_1, \ldots, z_{r-1}\rangle$.

The final claim follows from [14], where the stated bounds on $\mu(\mathrm{PSL}_2(p))$ are determined. □

In general $\mu(G)$ can be much larger than $d(G)$. For example, if G is soluble, then $\mu(G) - d(G) \geq \pi(G) - 2$ (see [17, Corollary 3]), where $\pi(G)$ is the number of distinct primes dividing the order of G. For all G, the value of $\mu(G)$ is at least the number of complemented factors in a chief series of G (see [17, Theorem 1]). Hence the difference $\mu(G) - d(G)$ (and consequently, by Corollary 1.10, the difference $\mu(G) - \psi(G)$) can be arbitrarily large.

2.3. **Groups with $\psi(G) = d(G)$.** In this subsection, we study groups G for which $\psi(G) = d(G)$; in particular in Theorem 2.21 we describe the structure of such soluble groups G.

Definition 2.15. A finite group G is *efficiently generated* if for all $x \in G$, $d_{\{x\}}(G) = d(G)$ implies that $x \in \mathrm{Frat}(G)$.

Lemma 2.16. *If $\psi(G) = d(G)$, then G is efficiently generated.*

Proof. Let $d = d(G)$. If G is not efficiently generated, then there exists $x \notin \mathrm{Frat}(G)$ such that $d_{\{x\}}(G) = d$. This implies in particular $x \equiv_{\mathrm{m}}^{(d)} 1$. However since $x \notin \mathrm{Frat}(G)$, we have $x \not\equiv_{\mathrm{m}} 1$, hence $\psi(G) > d$. □

Lemma 2.17. *If G is efficiently generated and $\tilde{m}(G) < d(G)$, then $\psi(G) = d(G)$.*

Proof. Let $d = d(G)$. By Theorem 2.10, our assumption that $\tilde{m}(G) < d(G)$ implies that $\psi(G) \leq d + 1$, and hence that $\equiv_{\mathrm{m}}^{(d+1)}$ coincides with $\equiv_{\mathrm{m}}$. It therefore suffices to prove that if $x \not\equiv_{\mathrm{m}}^{(d+1)} y$, then $x \not\equiv_{\mathrm{m}}^{(d)} y$.

Assume that $x \not\equiv_{\mathrm{m}}^{(d+1)} y$ and let $d_x = d_{\{x\}}(G)$ and $d_y = d_{\{y\}}(G)$. It is clear that $d_x, d_y \geq d - 1$. If $d_x = d_y = d$, then our assumption that G is efficiently generated implies that $x, y \in \mathrm{Frat}(G)$, and hence that $x \equiv_{\mathrm{m}} y$, a contradiction. Therefore we may assume that $d_x = d - 1$; in particular $G = \langle x, g_1, \ldots, g_{d-1}\rangle$ for some $g_1, \ldots, g_{d-1} \in G$. If $d_y = d$, then $G \neq \langle y, g_1, \ldots, g_{d-1}\rangle$ and therefore $x \not\equiv_{\mathrm{m}}^{(d)} y$, and we are done.

So assume that $d_x = d_y = d - 1$. Since $x \not\equiv_{\mathrm{m}} y$, without loss of generality there exists a maximal subgroup M of G such that $x \notin M$, $y \in M$. Let

$N = \mathrm{Core}_G(M)$. Since $d-1 \geq \tilde{m}(G)$, there exist $g_1, \dots, g_{d-1} \in M$ such that $\langle x, g_1, \dots, g_{d-1} \rangle N = G$. As $d_x = d-1$, we deduce from Lemma 2.11 that there exist $n_1, \dots, n_{d-1} \in N$ such that $G = \langle x, g_1 n_1, \dots, g_{d-1} n_{d-1} \rangle$. On the other hand $\langle y, g_1 n_1, \dots, g_{d-1} n_{d-1} \rangle \leq M$. Hence $x \not\equiv_{\mathrm{m}}^{(d)} y$. □

Notice that if $d(M) < d(G)$ for every maximal subgroup M of G, then G is efficiently generated. Indeed if $x \notin \mathrm{Frat}(G)$, then there exists a maximal subgroup M of G with $x \notin M$ and consequently $d_{\{x\}}(G) \leq d(M) < d(G)$. But then from Lemma 2.17 we deduce the following result.

Corollary 2.18. *If $d(M) < d(G)$ for every maximal subgroup M of G, then $\psi(G) = d(G)$.*

Lemma 2.19. *Let G be a finite soluble group. If G is efficiently generated then $\tilde{m}(G) < d(G)$.*

Proof. It suffices to prove that for every maximal subgroup M of G, we have $d(M/\mathrm{Core}_G(M)) < d(G) = d$. Assume otherwise. Then there exists a maximal subgroup M of G such that $d(M/N) = d$ (where $N = \mathrm{Core}_G(M)$). Furthermore, there exists a normal subgroup A of G such that G/N is a split extension of the form $A/N : M/N$ and $\mathrm{Frat}(G) \leq N$. Let $a \in A \setminus \mathrm{Frat}(G)$. Then $d_{\{a\}}(G) = d$, contradicting the assumption that G is efficiently generated. □

The following result is now immediate from Lemmas 2.16, 2.17 and 2.19.

Corollary 2.20. *Let G be a finite soluble group. Then $\psi(G) = d(G)$ if and only if G is efficiently generated.*

Theorem 2.21. *A finite soluble group G satisfies $\psi(G) = d(G)$ if and only if either G is a finite p-group or there exist a finite vector space V, a nontrivial irreducible soluble subgroup H of $\mathrm{Aut}(V)$ and an integer $d > d(H)$ such that*

$$G/\mathrm{Frat}(G) \cong V^{r(d-2)+1} : H,$$

where r is the dimension of V over $\mathrm{End}_H(V)$ and H acts in the same way on each of the $r(d-2)+1$ factors.

Proof. Assume that G is a soluble group with $\psi(G) = d(G) = d$ and let $F = \mathrm{Frat}(G)$. By Corollary 2.20, G is efficiently generated. If N is a normal subgroup of G properly containing F, then $d(G/N) < d$ (otherwise we would have $d_{\{n\}}(G) = d$ for every $n \in N$). So G/F has the property that every proper quotient can be generated by $d-1$ elements, but G/F cannot. The groups with this property have been studied in [8]. By [8, Theorem 1.4 and Theorem 2.7] either G/F is an elementary abelian p-group of rank d (and consequently G is a finite p-group) or there exist a finite vector space V and a nontrivial irreducible soluble subgroup H of $\mathrm{Aut}(V)$ such that $d(H) < d$ and $G/\mathrm{Frat}(G) \cong V^{r(d-2)+1} : H$, where r is the dimension of V over $\mathrm{End}_H(V)$.

Conversely, if G is a finite p-group it follows immediately from Burnside's basis theorem that G is efficiently generated, and so $\psi(G) = d(G)$

by Corollary 2.20. Clearly a group G is efficiently generated if and only if $G/\operatorname{Frat}(G)$ is efficiently generated. So to conclude the proof it suffices to prove that if H is a $(d-1)$-generated soluble irreducible subgroup of $\operatorname{Aut}(V)$ and r is the dimension of V over $F = \operatorname{End}_H(V)$, then $X = V^{r(d-2)+1} : H$ is efficiently generated. Notice that $d(X) = d$, so we have to prove that $d_{\{x\}}(X) \leq d-1$ for every $x \neq 1$. Let $n = r(d-2)+1$. Fix a nontrivial element $x = (v_1, \ldots, v_n)h \in X$ and let $a = \dim_F C_V(h)$ and $b = n - \dim_F \langle [V,h], v_1, \ldots, v_n \rangle + \dim_F [V,h]$. By [7, Lemma 5] we have $d_{\{x\}}(X) \leq d-1$ if and only if $a + b - 1 < r(d-1)$. If $h \neq 1$, then $a \leq r-1$ and $b \leq n$; if $h = 1$, then $a \leq r$ and $b \leq n-1$. In any case $a + b - 1 \leq r + n - 2 = r + r(d-2) - 1 < r(d-1)$. □

Apart from p-groups, there are many examples of soluble groups that are efficiently generated. The smallest example of a soluble group which is not efficiently generated is S_4 (we have $d_{\{x\}}(\mathrm{S}_4) = 2$ for every x in the Klein subgroup): by the previous results we can conclude that $\psi(\mathrm{S}_4) = 3$.

Problem 2.22. Characterise the insoluble groups that are efficiently generated.

2.4. **Calculating $\equiv_{\mathrm{m}}$.** Whilst we have not been able to determine $\psi(G)$ for an arbitrary group G, we have calculated it for many small almost simple groups G with $d(G) = 2$. It is computationally expensive to repeatedly calculate whether various sets of elements generates a group. In this subsection we describe an efficient way to calculate $\equiv_{\mathrm{m}}$- and $\equiv_{\mathrm{m}}^{(2)}$-classes in a group, and present a theorem summarising the results of these calculations.

The equivalence relation $\equiv_{\mathrm{m}}$ can be thought of another way. Construct the permutation action of G which is the disjoint union of the actions on the cosets of maximal subgroups, one for each conjugacy class. Let Ω be the domain of this action. For brevity, we call this the *m-universal action* of G.

Lemma 2.23. *Let G be a finite group, and let $x, y \in G$ and $S \subseteq G$.*
(1) *$x \equiv_{\mathrm{m}} y$ if and only if x and y have the same fixed point sets in the m-universal action of G.*
(2) *$G = \langle S \rangle$ if and only if the intersection of the fixed point sets of elements of S in the m-universal action of G is empty.*

Proof. Notice that in the orbit corresponding to a non-normal maximal subgroup M, the point stabilisers are the conjugates of M; whereas, if M is normal, then its elements fix every point in the corresponding orbit, while the elements outside M fix none. Hence the fixed point set of an element x describes precisely which maximal subgroups of G contain x, and (1) follows. For (2), notice that $G = \langle S \rangle$ if and only if S is contained in no maximal subgroup of G. □

Definition 2.24. A permutation group action has *property $\mathcal{G}$* if it satisfies: each set S of group elements generates the group if and only if the fixed-point sets of elements of S have empty intersection.

Lemma 2.25. *The m-universal action is the smallest degree permutation action of G with property $\mathcal{G}$.*

Proof. First notice that by Lemma 2.23(2), the m-universal action has property $\mathcal{G}$. Now suppose that we have an action of G with property $\mathcal{G}$. We must show that it contains the m-universal action. So let M be a maximal subgroup of G. Choose generators $g_1, \ldots, g_r$ of M. Since these elements do not generate G, property $\mathcal{G}$ implies that they have a common fixed point, say ω. Thus $M \leq G_\omega < G$, and maximality of M implies that $M = G_\omega$. So the coset space of M is contained in the given action. Since this holds for all maximal subgroups M, we are done. □

Our algorithm to test whether $\psi(G) = 2$ proceeds as follows, on input a finite group G.

(1) Construct the maximal subgroups of G, and hence the m-universal action of G.
(2) For each $g \in G$, compute the fixed point set $\mathrm{Fix}(g)$ of g in the m-universal action, and hence construct a set of equivalence class representatives for the $\equiv_{\mathrm{m}}$-classes of G.
(3) For each pair x, y of distinct $\equiv_{\mathrm{m}}$-class representatives, check that there exists a $z \in G$ such that either $\mathrm{Fix}(x) \cap \mathrm{Fix}(z) = \emptyset$ and $\mathrm{Fix}(y) \cap \mathrm{Fix}(z)$ is non-empty, or *vice versa*.

If the test in Step 3 succeeds for all distinct x and y, then the set of distinct $\equiv_{\mathrm{m}}$-class representatives is also a set of distinct $\equiv_{\mathrm{m}}^{(2)}$-class representatives. That is, $\psi(G) = 2$.

We have implemented the algorithm in MAGMA [2], and used it to prove the following:

Theorem 2.26. *Let G be an almost simple group with socle of order less than* 10000 *such that all proper quotients of G are cyclic. Then $\psi(G) = 2$.*

The socle of such a group G is one of: A_n for $5 \leq n \leq 7$, $\mathrm{PSL}_2(q)$ for $q \leq 27$ a prime power, $\mathrm{PSL}_3(3)$, $\mathrm{PSU}_3(3)$ or the sporadic group M_{11}.

The only almost simple groups with socle of order less than 10000 with a proper non-cyclic quotient are $\mathrm{A}_6.2^2$ and $\mathrm{PSL}_2(25).2^2$. Using similar ideas to the above we were able to show that $\psi(\mathrm{A}_6.2^2) = 3$.

Notice that in all of these instances, the lower bounds from Lemma 2.6 are attained.

3. c-EQUIVALENCE

In this section we define another equivalence relation, which can be used to give an easy-to-calculate upper bound on the number of $\equiv_{\mathrm{m}}$-classes, and investigate when this new relation coincides with $\equiv_{\mathrm{m}}$.

Definition 3.1. Let G be a finite group, and let $x, y \in G$. We define $x \equiv_{\mathrm{c}} y$ if $\langle x \rangle = \langle y \rangle$. We use c for *cyclic*.

The following is clear.

Lemma 3.2. *Let G be a finite group. For all $x, y \in G$, if $x \equiv_{\mathrm{c}} y$ then $x \equiv_{\mathrm{m}} y$. Hence if n is the order of an element of G, then at least one $\equiv_{\mathrm{m}}$-class of G contains at least $\phi(n)$ elements.*

The converse implication of the first statement holds for many groups (including S_n and A_n for $n \in \{5, 6\}$, and $\mathrm{PSL}_2(q)$ for $q \in \{7, 11, 13\}$), but not for all groups.

Proposition 3.3. *Let G be a finite group. If the relations $\equiv_{\mathrm{m}}$ and $\equiv_{\mathrm{c}}$ coincide, then*

(1) $\mathrm{Frat}(G) = 1$;
(2) *if G is soluble then every minimal normal subgroup of G is cyclic;*
(3) *if G is soluble then G is metabelian.*

Proof. (1) All of the elements of $\mathrm{Frat}(G)$ are $\equiv_{\mathrm{m}}$-equivalent.
(2) Let G be soluble and let N be a minimal normal subgroup of G. Every maximal subgroup of G either contains or complements N. This implies that all the elements of $N \setminus \{1\}$ are $\equiv_{\mathrm{m}}$ equivalent, and consequently N is cyclic (of prime order).
(3) Let G be soluble and let $F = \mathrm{Fit}(G)$. Since $\mathrm{Frat}(G) = 1$, it follows from [24, 5.2.15] that $\mathrm{Fit}(G) = \mathrm{Soc}(G)$, and hence $F = C_G(F) = \cap_{N \in \mathcal{N}} C_G(N)$, where $\mathcal{N}$ is the set of the minimal normal subgroups of G. But then

$$\frac{G}{F} = \frac{G}{\bigcap_N C_G(N)} \leq \prod_N \mathrm{Aut}(N)$$

is abelian. □

The conditions listed in the previous proposition are not sufficient to ensure that the relations $\equiv_{\mathrm{m}}$ and $\equiv_{\mathrm{c}}$ coincide on soluble groups G. In order to obtain a more precise result, let us fix some notation. Assume that G is soluble and satisfies the conclusions of Proposition 3.3. We set $F = \mathrm{Fit}(G)$ and $Z = Z(G)$. Then

$$F = V_1^{r_1} \times \cdots \times V_t^{r_t} \times Z,$$

where $V_1^{r_1}, \ldots, V_t^{r_t}$ are the non-central homogeneous components of F as a G-module. In particular, V_i is cyclic of prime order for every i. Moreover $G = F : H$, where H is a subdirect product of $\prod_i H_i$, with $H_i \leq \mathrm{Aut}(V_i)$. Finally, for $h = (h_1, \ldots, h_t) \in H$, define $\Omega(h) = \{i \in \{1, \ldots, t\} \mid h_i = 1\}$.

Theorem 3.4. *Let $G = F : H$ as above be a soluble group satisfying the conclusions of Proposition 3.3. The relations $\equiv_{\mathrm{m}}$ and $\equiv_{\mathrm{c}}$ coincide on G if and only if the following property is satisfied, for all $(z_1, h_1), (z_2, h_2) \in Z \times H$*

$(*)$ *if $\langle (z_1, h_1) \rangle \, \mathrm{Frat}\, H = \langle (z_2, h_2) \rangle \, \mathrm{Frat}\, H$ and $\Omega(h_1) = \Omega(h_2)$, then $\langle (z_1, h_1) \rangle = \langle (z_2, h_2) \rangle$.*

Proof. Let $x_1 = (z_1, h_1)$, $x_2 = (z_2, h_2) \in Z \times H$, with $h_1 = (\alpha_1, \dots, \alpha_t)$ and $h_2 = (\beta_1, \dots, \beta_t)$. Assume that $\langle x_1\rangle \operatorname{Frat} H = \langle x_2\rangle \operatorname{Frat} H$ and $\Omega(h_1) = \Omega(h_2)$. We claim that a maximal subgroup M of G contains x_1 if and only if it contains x_2, and hence that $x_1 \equiv_{\mathrm{m}} x_2$.

Let $W = V_1^{r_1} \times \cdots \times V_t^{r_t}$ and let $L = \operatorname{Frat}(Z \times H) = \operatorname{Frat}(H)$. If $W \le M$, then $W : L \le M$, so $\langle x_i\rangle \subseteq M$ if and only if $\langle x_i\rangle L \subseteq M$. Since $\langle x_1\rangle L = \langle x_2\rangle L$, we deduce that $x_1 \in M$ if and only if $x_2 \in M$. If $W \not\le M$, then there exists $i \in \{1, \dots, t\}$, a maximal H-invariant subgroup U_i of $V_i^{r_i}$ and $w_i \in V_i^{r_i}$ such that

$$M = (V_1^{r_1} \times \cdots \times V_{i-1}^{r_{i-1}} \times U_i \times V_{i+1}^{r_{i+1}} \times \cdots \times V_t^{r_t} \times Z) : H^{w_i}.$$

Notice in particular that if $(\gamma_1, \dots, \gamma_r) \in H$, then $(\gamma_1, \dots, \gamma_r) \in M$ if and only if $\gamma_i \in U_i H_i^{w_i}$. In this case we can write $\gamma_i = u_i[w_i, h_i^{-1}]h_i = h_i$, so that $[w_i, \gamma_i^{-1}] \in U_i$. Since $V_i^{r_i}/U_i \cong_{H_i} V_i$, we have that if $[w_i, \gamma_i^{-1}] \in U_i$ then either $\gamma_i = 1$ or $w_i \in U_i$. If $w_i \in U_i$ then $x_1, x_2 \in M$. So assume $w_i \notin U_i$. Since $\Omega(h_1) = \Omega(h_2)$, we have that $\alpha_i = 1$ if and only if $\beta_i = 1$, hence $x_1 \in M$ if and only if $x_2 \in M$. We have proved that if $\equiv_{\mathrm{m}}$ and $\equiv_{\mathrm{c}}$ coincide, then $(*)$ holds.

For the converse, let $x_1 = w_1 z_1 h_1$, $x_2 = w_2 z_2 h_2$ be two elements of G with $h_1, h_2 \in H$, $z_1, z_2 \in Z$ and $w_1, w_2 \in W$. Assume that $x_1 \equiv_{\mathrm{m}} x_2$. Since $w_1 h_1$ and h_1 are conjugate in G, it is not restrictive to assume that $x_1 = z_1 h_1$. We claim that this implies that $w_2 = 1$. Indeed, assume that $w_2 = (v_1, \dots, v_t) \neq 1$. Then there exists an i such that $v_i \neq 1$, and consequently there exists a maximal H-invariant subgroup U_i of $V_i^{r_i}$ with $v_i \notin U_i$. This leads to a contradiction, since the maximal subgroup

$$M = (V_1^{r_1} \times \cdots \times V_{i-1}^{r_{i-1}} \times U_i \times V_{i+1}^{r_{i+1}} \times \cdots \times V_t^{r_t} \times Z) : H$$

contains x_1 but not x_2.

Having $w_1 = w_2 = 1$, the argument used in the first part of this proof shows that the condition $\Omega(h_1) = \Omega(h_2)$ is equivalent to saying that a maximal subgroup of G not containing W contains x_1 if and only if it contains x_2. On the other hand the maximal subgroups of G containing W are in bijective correspondence with those of $G/\operatorname{Frat} H$, hence the condition $\langle x_1\rangle \operatorname{Frat} H = \langle x_2\rangle \operatorname{Frat} H$ is equivalent to saying that a maximal subgroup of G containing W contains x_1 if and only if it contains x_2. We have therefore proved that $x_1 \equiv_{\mathrm{m}} x_2$ implies that $\Omega(h_1) = \Omega(h_2)$ and $\langle x_1\rangle \operatorname{Frat} H = \langle x_2\rangle \operatorname{Frat} H$, and therefore if $(*)$ holds, then $x_1 \equiv_{\mathrm{c}} x_2$. □

Here are two examples of groups which satisfy the conclusions of Proposition 3.3, but do not satisfy condition $(*)$. Hence $\equiv_{\mathrm{c}}$-equivalence is finer than $\equiv_{\mathrm{m}}$-equivalence.

(1) Let G be the sharply 2-transitive group of degree 17, the semidirect product of C_{17} with a Singer cycle C_{16}. The maximal subgroups are $C_{17} : C_8$ and the conjugates of C_{16}. In particular, we see that

elements of orders 2, 4 and 8 in a fixed complement C_{16} are all $\equiv_{\mathrm{m}}$-equivalent. However, $\equiv_{\mathrm{c}}$-equivalent elements have the same order.
(2) A second example is $(\langle x\rangle : \langle y\rangle) \times \langle z\rangle$ with $|x| = 19, |y| = 9, |z| = 3$ (indeed $(y^3, z) \equiv_{\mathrm{m}} (y^6, z)$).

Proposition 3.5. *Assume that a finite group G contains a minimal normal subgroup $N = S_1 \times \cdots \times S_t$, with $S_i \cong S$ a finite nonabelian simple group. If either $t \geq 3$, or $t = 2$ and S is not isomorphic to $\mathrm{P}\Omega_8^+(q)$ with $q = 2$ or 3, then the relations $\equiv_{\mathrm{m}}$ and $\equiv_{\mathrm{c}}$ do not coincide on G.*

Proof. It is standard (see, for example, [1, Remark 1.1.040]) that if a maximal subgroup M of G does not contain N, then one of the following occurs:
(1) $M \cap N = 1$;
(2) M is of *product type*: in this case there exist $\alpha_2, \ldots, \alpha_t \in \mathrm{Aut}(S)$, independent of the choice of M, $s_2, \ldots, s_t \in S$ and a proper subgroup K of S such that $M \cap N \leq K \times K^{s_2\alpha_2} \times \cdots \times K^{s_t\alpha_t}$;
(3) M is of *diagonal type*: in this case there exists a partition $\Phi := \{B_1, \ldots, B_u\}$ of $\{1, \ldots, t\}$ into blocks of the same size such that $M \cap N \leq \prod_{B\in\Phi} D_B$ where D_B is a full diagonal subgroup of $\prod_{j\in B} S_j$.

By [15, Theorem 5.1] or [11, Theorem 7.1], there exist $a, b \in S$ with the property that $\langle a^\gamma, b^\delta\rangle = S$ for each choice of $\gamma, \delta \in S$. Moreover if $S \neq \mathrm{P}\Omega_8^+(q)$, $q = 2$ or 3, then a and b are not conjugate in $\mathrm{Aut}(S)$.

Let $x, y \in S$ and consider

$$g_{x,y} = \begin{array}{ll} (a^x, b^{y\alpha_2}, a, \ldots, a, 1) & \text{if } t > 2 \\ (a^x, b^{y\alpha_2}) & \text{otherwise.} \end{array}$$

There is no maximal subgroup of product type containing $g_{x,y}$. Otherwise we would have $a^x \in K$, $b^{y\alpha_2} \in K^{s_2\alpha_2}$, hence $S = \langle a^x, b^{ys_2^{-1}}\rangle \leq K$, contradicting the fact that K is a proper subgroup of S. Moreover, since either $t \geq 3$ or a and b are not conjugate in $\mathrm{Aut}(S)$, no maximal subgroup of diagonal type contains $g_{x,y}$. Therefore $g_{x,y} \in M$ if and only if $N \leq M$, for all maximal subgroups M. Hence, all the elements of the subset $\{g_{x,y} \mid x, y \in S\}$ are $\equiv_{\mathrm{m}}$ equivalent, and therefore the relations $\equiv_{\mathrm{m}}$ and $\equiv_{\mathrm{c}}$ do not coincide on G. $\square$

Corollary 3.6. *Let G be a finite group. If the relations $\equiv_{\mathrm{m}}$ and $\equiv_{\mathrm{c}}$ coincide on G, then $G/\mathrm{Soc}(G)$ is soluble.*

Proof. Since the relations $\equiv_{\mathrm{m}}$ and $\equiv_{\mathrm{c}}$ coincide, $\mathrm{Frat}(G) = 1$ by Proposition 3.3(1), and consequently $\mathrm{Soc}(G) = F^*(G)$, where $F^*(G)$ is the generalized Fitting subgroup of G.

Let $F^*(G) = Z(G) \times N_1 \times \cdots \times N_t$, where $N_1, \ldots, N_t$ are non-central minimal normal subgroups. Since $Z(G) = C_G(F^*(G)) = \bigcap_i C_G(N_i)$, we have $G/Z(G) \leq \prod_i G/C_G(N_i)$. To conclude, notice that if N_i is abelian, then N_i is cyclic and $G/C_G(N_i)$ is abelian, while if N_i is nonabelian, then by Proposition 3.5 the group $N_i \cong S_i^{t_i}$ with $t_i \leq 2$ and $G/(N_iC_G(N_i)) \leq \mathrm{Out}\, S \wr \mathrm{Sym}(t_i)$, which is soluble. $\square$

Problem 3.7. Find an equivalence relation that is easier to calculate than $\equiv_{\mathrm{m}}$, but coarser than $\equiv_{\mathrm{c}}$. Determine for which insoluble groups G the relations $\equiv_{\mathrm{m}}$ and $\equiv_{\mathrm{c}}$ coincide.

3.1. **Asymptotics and enumeration.** We now briefly suggest some directions for further study of the asymptotics of our new relations.

Proposition 3.8. *Let G be S_n or A_n. Then for almost all elements $x, y \in G$ (all but a proportion tending to 0 as $n \to \infty$), the following are equivalent:*

(1) $x \equiv_{\mathrm{m}} y$;
(2) $x \equiv_{\mathrm{m}}^{(2)} y$;
(3) *the cycles of x and y induce the same partition of $\{1, \ldots, n\}$.*

Proof. This depends on a theorem of Łuczak and Pyber [21], which states that for almost all $x \in \mathrm{S}_n$, the only transitive subgroups of S_n containing x are S_n and (possibly) A_n. We restrict our attention to these elements x.

Consider first the case where $G = \mathrm{S}_n$. Then, apart from A_n, the maximal subgroups containing x are of the form $\mathrm{S}_k \times \mathrm{S}_{n-k}$, where the two orbits are unions of cycles of x. Moreover, the cycle lengths determine whether or not $x \in \mathrm{A}_n$. So (1) and (3) are equivalent.

In addition, for all $z \in G$, we see that $\langle x, z \rangle = G$ whenever $\langle x, z \rangle$ is transitive, and $z \notin \mathrm{A}_n$ if it happens that $x \in \mathrm{A}_n$. Membership of this set is also determined by the cycles of x: the transitivity condition requires that the hypergraph whose edges are the cycles of x and z is connected. So (2) is also equivalent to (3).

If $G = \mathrm{A}_n$, then only simple modifications are required; the argument is simpler because no parity conditions are necessary. $\square$

Shalev in [26] proved a similar result for $\mathrm{GL}_n(q)$ to Łuczak and Pyber's result for S_n: a random element of $\mathrm{GL}_n(q)$ lies in no proper irreducible subgroup not containing $\mathrm{SL}_n(q)$. This could be used to prove a similar statement for groups lying between $\mathrm{PSL}_n(q)$ and $\mathrm{PGL}_n(q)$.

Question 3.9. Are there only finitely many finite almost simple groups on which the relations $\equiv_{\mathrm{m}}$ and $\equiv_{\mathrm{c}}$ coincide?

Another very natural question is: how many $\equiv_{\mathrm{c}}$- and $\equiv_{\mathrm{m}}$-classes are there in the symmetric group S_n? The numbers of $\equiv_{\mathrm{c}}$-classes in the symmetric groups S_n form sequence A051625 in the On-line Encyclopedia of Integer Sequences [22]. The sequence of numbers of $\equiv_{\mathrm{m}}$ classes, which begins

$$1, 2, 5, 15, 67, 362, 1479, 12210, \ldots$$

has recently been added to the OEIS, where it appears as Sequence A270534.

If we cannot find a formula for these sequences, can we say anything about their asymptotics? We saw above that, for almost all elements of S_n, the $\equiv_{\mathrm{m}}$-equivalence class is determined by the cycle partition, which might suggest that the sequence grows like the Bell numbers (sequence A000110 in the OEIS). However, the elements not covered by this theorem can destroy this estimate.

For example, let p be a prime such that the only insoluble transitive groups of degree p are the symmetric and alternating groups. Then the above analysis applies to all elements whose cycle type is not a single p-cycle or a fixed point and l k-cycles (where $1 + kl = p$). It is easy to show that two elements x and y with one of these excluded cycle types satisfy $x \equiv_{\mathrm{m}} y$ if and only if they satisfy $x \equiv_{\mathrm{c}} y$. So there are $(p-2)!$ equivalence classes of p-cycles, for example; this number is much greater than the pth Bell number. (In this special case, we can write down a formula for the number of $\equiv_{\mathrm{m}}$-equivalence classes.)

4. The generating graph of a group

In the remainder of the paper, we use the relations that we have defined to study an object of general interest, the generating graph of a finite group.

Definition 4.1. The *generating graph* $\Gamma(G)$ of a finite group G is the graph with vertex set G, in which two vertices x and y are joined if and only if $\langle x, y\rangle = G$.

Of course this graph is null unless G is 2-generated. We adopt the convention that, if the group is cyclic, then any generator of the group carries a loop in the generating graph.

A useful concept when studying the generating graph is the spread of a group.

Definition 4.2. A group G has *spread* k if k is the largest number such that for any set S of k nonidentity elements, there exists x such that $\langle x, s\rangle = G$ for all $s \in S$.

Thus the spread is nonzero if and only if no vertex of the generating graph except the identity is isolated; and spread at least 2 implies diameter at most 2.

Among the graph-theoretic invariants which have been studied for this graph are the following.

(1) The spread.
(2) The *clique number*: the largest size of a set of group elements, any two of which generate the group.
(3) The *chromatic number*: the smallest number of parts in a partition of the group into subsets containing no 2-element generating set.
(4) The *total domination number*: the smallest size of a set S with the property that, for any element x, there exists $s \in S$ such that x and s generate the group.
(5) The isomorphism type: if $\Gamma(G) \cong \Gamma(H)$ for two groups G and H, then when is $G \cong H$?

Definition 4.3. In any graph X, we can define an equivalence relation $\equiv_\Gamma$ by the rule $x \equiv_\Gamma y$ if x and y have the same set of neighbours in the graph. (Think of Γ as meaning "graph", or "generating" if we are thinking of the generating graph.) Then we define a *reduced graph* $\overline{X}$ whose vertices are the $\equiv_\Gamma$-classes in X, two classes joined in $\overline{X}$ if their vertices are joined in X.

Alternatively, we can take the vertex set to be any set of equivalence class representatives, and the graph to be the induced subgraph on this set. (The term "reduced graph" was used by Hall [13] in his work on copolar spaces, and consequentially we term the process of producing it "reduction"; but we warn readers that the term "graph reduction" has a very different meaning in computer science.)

The reduction process preserves the graph parameters noted above:

Proposition 4.4. *The clique number, chromatic number, total domination number, and spread of the generating* $\Gamma(G)$ *are equal to the corresponding parameters of the reduced generating graph* $\overline{\Gamma}(G)$*. Furthermore, if* $\Gamma(G) \cong \Gamma(H)$ *then* $\overline{\Gamma}(G) \cong \overline{\Gamma}(H)$*.*

Proof. Clear. $\square$

The following is immediate from the definition of $\equiv_{\mathrm{m}}^{(r)}$.

Proposition 4.5. *Let G be a finite group. Then the relations $\equiv_\Gamma$ on $\Gamma(G)$ and $\equiv_{\mathrm{m}}^{(2)}$ on G coincide; hence $\equiv_{\mathrm{m}}$ is a refinement of $\equiv_\Gamma$, and is equal to $\equiv_\Gamma$ if and only if $\psi(G) \le 2$.*

Hence, in what follows, we shall write $\equiv_\Gamma$ to denote $\equiv_{\mathrm{m}}^{(2)}$.

Recall Definition 2.15 of efficient generation.

Theorem 4.6. *Let G be a finite group with $d(G) = 2$.*

(1) *G has nonzero spread if and only if G is efficiently generated and has trivial Frattini subgroup.*
(2) *If G is soluble and has nonzero spread, then $\psi(G) = 2$.*

Proof. (1) Since the spread of G is nonzero, every nonidentity element of G lies in a 2-element generating set of G, so $d_x(G) = 1$ unless $x = 1$. Hence G is efficiently generated and $\mathrm{Frat}(G) = 1$. The converse is clear.

(2) By Part (1), the assumption that G has nonzero spread implies that G is efficiently generated. Hence from Corollary 2.20, we see that $\psi(G) = d(G) = 2$. $\square$

Notice that it is immediate from Theorem 4.6 that if G is a 2-generator group of spread 0 and trivial Frattini subgroup, then $\psi(G) \ge 3$. For example, double transpositions are isolated vertices in $\Gamma(\mathrm{S}_4)$, and so are equivalent to the identity under $\equiv_\Gamma$, though clearly not under $\equiv_{\mathrm{m}}$. In fact this group has fourteen $\equiv_\Gamma$-classes but fifteen $\equiv_{\mathrm{m}}$-classes, and as previously noted $\psi(\mathrm{S}_4) = 3$.

We shall therefore proceed for much of the following section by restricting to groups with nonzero spread, despite that fact that we don't know whether Theorem 4.6(2) is also true without the solubility assumption.

Conjecture 4.7. Let G be a finite group of nonzero spread. Then $\psi(G) \leq 2$.

By Lemma 2.17, if G is a group with nonzero spread, then $\psi(G) = 2$ whenever for all maximal subgroups M, and for all $x \notin M$, there exists $z \in M$ such that $\langle x, z\rangle = G$. This approach can be applied to S_5, $\mathrm{PSL}_2(7)$, and $\mathrm{PSL}_2(11)$. However, it fails in the case of A_5 with respect to the smallest maximal subgroups (isomorphic to S_3). It also fails for $\mathrm{PSL}_2(q)$ for $q = 8, 9, 13$, even though $\psi(G) = 2$ for all of these groups.

5. Automorphism groups

A striking thing about generating graphs is that they have huge automorphism groups, and these groups are poorly understood. For example, the automorphism group of the generating graph of the alternating group A_5 has order $2^{31}3^{7}5$.

The reason is simple. Any nontrivial element of A_5 has order 2, 3 or 5. An element of order 3 or 5 can be replaced by a nonidentity power of itself in any generating set. Thus the sets of nonidentity powers can be permuted arbitrarily, and we find a group of order $2^{10}(4!)^6 = 2^{28}3^6$ of automorphisms fixing these sets. The quotient has order 120 and is isomorphic to $\mathrm{Aut}(\mathrm{A}_5) = \mathrm{S}_5$.

Hence, for $G = \mathrm{A}_5$, the automorphism group of the generating graph $\Gamma(G)$ has a normal subgroup which is the direct product of symmetric groups on the $\equiv_\Gamma$-classes, and the quotient is the automorphism group of the reduced graph $\overline{\Gamma}(G)$. In general, a similar statement holds, but to state it we require one further definition.

Definition 5.1. We define a *weighting* of the reduced generating graph, by assigning to each vertex a weight which is the cardinality of the corresponding $\equiv_\Gamma$-class. Now let $\overline{\Gamma}_{\mathrm{w}}(G)$ denote the weighted graph, and let $\mathrm{Aut}(\overline{\Gamma}_{\mathrm{w}}(G))$ be the group of *weight-preserving automorphisms* of $\overline{\Gamma}_{\mathrm{w}}(G)$.

Note that the restriction to $\mathrm{Aut}(\overline{\Gamma}_{\mathrm{w}}(G))$ is necessary, as in general an automorphism of $\overline{\Gamma}(G)$ can fail to lift to an automorphism of $\Gamma(G)$. For an example of this, take $G = \mathrm{PSL}_2(16)$. Then $\mathrm{Aut}(\overline{\Gamma}(G)) \cong 2 \times \mathrm{Aut}(\mathrm{PSL}_2(16))$. However, the central involution interchanges elements of order 3 with elements of order 5. The $\equiv_{\mathrm{m}}$-class of the elements of order 3 has size 2, and contains only the elements and their inverses. However, the $\equiv_{\mathrm{m}}$-class of elements of order 5 has size 4 (it clearly contains all nontrivial elements of the cyclic subgroup, but in fact contains no more than this).

The following theorem shows that to describe the automorphism group of $\Gamma(G)$, it suffices to know the multiset of sizes of the $\equiv_\Gamma$-classes of G, and the automorphism group of $\overline{\Gamma}_{\mathrm{w}}(G)$.

Theorem 5.2. *Let the $\equiv_\Gamma$-classes of a finite group G be of sizes $k_1, \ldots, k_n$. Then*

$$A := \mathrm{Aut}(\Gamma(G)) = (\mathrm{S}_{k_1} \times \cdots \times \mathrm{S}_{k_n}) : \mathrm{Aut}(\overline{\Gamma}_{\mathrm{w}}(G)).$$

Proof. Let $N := \prod_{i=1}^{n} \mathrm{S}_{k_i}$. First we show that $N \leq A$, then that A is an extension of N by a subgroup of $\mathrm{Aut}(\overline{\Gamma}_{\mathrm{w}}(G))$, and finally that the whole of $\mathrm{Aut}(\overline{\Gamma}_{\mathrm{w}}(G))$ is induced by A, and the extension splits.

For the first claim, let $x, y \in G$ such that $x \equiv_\Gamma y$. Then for all $z \in G$, there is an edge from x to z if and only if there is an edge from y to z. Hence the map interchanging x and y and fixing all other vertices in $\Gamma(G)$ is an automorphism of $\Gamma(G)$, so $N \leq A$.

For the second, we show that A acts on the $\equiv_\Gamma$-classes of $\Gamma(G)$. For $z \in G$, write $N(z)$ for the set of neighbours of z in $\Gamma(G)$. Suppose that $x \equiv_\Gamma y$, as before. Then for all $a \in A$ we see that

$$N(x^a) = N(x)^a = N(y)^a = N(y^a),$$

and so $x^a \equiv_\Gamma y^a$, as required. Hence A is an extension of N by a subgroup of $\mathrm{Aut}(\overline{\Gamma}_{\mathrm{w}}(G))$.

For the final claim, fix an ordering of the elements in each $\equiv_\Gamma$ class of G, and identify the vertices of $\Gamma(G)$ with the ordered pairs $\{(i,j) \ : \ 1 \leq j \leq n, \ 1 \leq i \leq k_j\}$. Let $\sigma \in \mathrm{Aut}(\overline{\Gamma}_{\mathrm{w}}(G))$, and let j_1, j_2 be adjacent vertices in $\overline{\Gamma}_{\mathrm{w}}(G)$, so that j_1^σ and j_2^σ are also adjacent. Then $k_{j_1} = k_{j_1^\sigma}$, and for $1 \leq i \leq k_{j_1}$ vertex (i, j_1) is adjacent to vertex (i, j_2). Hence we can define τ to be the map sending (i,j) to (i, j^σ), and then $\tau \in \mathrm{Aut}(\Gamma(G))$ induces σ. The result follows. $\square$

Note that $\mathrm{Aut}(G)$ preserves the generating graph $\Gamma(G)$, and hence automorphisms of G permute the $\equiv_\Gamma$-classes. We define $\mathrm{Aut}^*(G)$ to be the group induced by $\mathrm{Aut}(G)$ on $\overline{\Gamma}(G)$. The following is clear.

Proposition 5.3. *Let G be a group with $d(G) \leq 2$. Then*

$$\mathrm{Aut}^*(G) \leq \mathrm{Aut}(\overline{\Gamma}_{\mathrm{w}}(G)) \leq \mathrm{Aut}(\overline{\Gamma}(G)).$$

In the remainder of the paper we shall analyse these three automorphism groups, concentrating on the groups G with nonzero spread. Such a group G has no non-cyclic proper quotients. Moreover (see for example [20]), it satisfies one of the following:

(1) G is cyclic;
(2) $G \cong C_p \times C_p$ for some prime p;
(3) G is the semi-direct product of its unique minimal normal subgroup N (which is elementary abelian) by an irreducible subgroup C of a Singer cycle acting on N;
(4) G has a normal subgroup $N \cong T_1 \times \cdots \times T_r$, where $T_1, \ldots, T_r$ are isomorphic nonabelian simple groups; G/N has order rm for some m dividing $|\mathrm{Out}(T_1)|$, and induces a cyclic permutation of the factors.

We shall show that $\mathrm{Aut}^*(G)$ is trivial for groups of type (1), and is equal to $\mathrm{Aut}(G)$ for groups of type (3) and (4). Furthermore, we shall show that in type (1) there is a spectacularly large gap between $\mathrm{Aut}(\overline{\Gamma}(G))$ and $\mathrm{Aut}(\overline{\Gamma}_{\mathrm{w}}(G))$, whilst in type (2) and (3) we find that $\mathrm{Aut}^*(G) \neq \mathrm{Aut}(\overline{\Gamma}_{\mathrm{w}}(G))$.

First we consider the groups of type (1).

Proposition 5.4. *Let G be the cyclic group of order $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$. Then $\overline{\Gamma}(G)$ has 2^r vertices. The group $\mathrm{Aut}^*(G) = \mathrm{Aut}(\overline{\Gamma}_{\mathrm{w}}(G))$ is trivial, while $\mathrm{Aut}(\overline{\Gamma}(G)) \cong \mathrm{S}_r$. Hence $\mathrm{Aut}(\Gamma(G)) = \prod_{I \subseteq \{1,\ldots,r\}} \mathrm{S}_{n_I}$, where*

$$n_I = \frac{n}{p_1 p_2 \cdots p_r} \prod_{i \in I} (p_i - 1).$$

Proof. First, vertices in the same coset of the Frattini subgroup $\Phi(G)$ get identified when we reduce the generating graph, and the weights are multiplied by $|\Phi(G)| = \frac{n}{p_1 \cdots p_r}$. So we can assume that the Frattini subgroup is trivial, that is, $n = p_1 p_2 \cdots p_r$.

We know that in this case the $\equiv_\Gamma$- and $\equiv_{\mathrm{m}}$-relations coincide, and it is more convenient to use the latter. The group has r maximal subgroups (one of index p_i for each i) and the lattice of their intersections is the lattice of subsets of $\{1, \ldots, r\}$. So, for any subset I of $\{1, \ldots, r\}$, there is a unique vertex v_I of the reduced graph corresponding to the intersection of the subgroups of index p_i for $i \in I$; and v_I is joined to v_J if and only if $I \cap J = \emptyset$.

We claim that the automorphism group of $\overline{\Gamma}(G)$ is the symmetric group S_r. It is clear that S_r acts as automorphisms of the graph; it suffices to prove that there are no more.

There is a unique vertex $v_\emptyset$ joined to all others. Apart from this vertex, there are r vertices whose neighbour sets are maximal with respect to inclusion, namely $v_{\{i\}}$ for $i = 1, \ldots, r$, which must be permuted by the automorphism group. It suffices to show that only the identity fixes all these vertices. But any further vertex is uniquely specified by its neighbours within this set: v_I is joined precisely to $v_{\{j\}}$ for $j \notin I$.

What is the subgroup of S_r fixing the weights? Recall that the weight of a vertex v_I is the number of elements of G which are equivalent to this vertex of the reduced graph, that is, which lie in the maximal subgroups of index p_i for $i \in I$ and no others. This is the number of generators of the intersection of these maximal subgroups, which is

$$\prod_{j \notin I} (p_j - 1).$$

Now it can happen that two of these weights are equal, even for elements in the same S_r-orbit. (For example, let $n = 2.3.7.13 = 546$. The subgroups of orders 2.13 and 3.7 each have 12 generators.)

However, only the identity element of S_r preserves all the weights. For the minimal nonidentity elements C_{p_i} have distinct weights $p_i - 1$, and so all are fixed by the weight-preserving subgroup. $\square$

Proposition 5.5. *Let $G \cong C_p^2$. Then $\overline{\Gamma}(G)$ has $p+2$ vertices, with $\mathrm{Aut}(G) \cong \mathrm{GL}_2(p)$ and $\mathrm{Aut}^*(G) \cong \mathrm{PGL}_2(p)$. On the other hand, $\mathrm{Aut}(\overline{\Gamma}(G))$ and $\mathrm{Aut}(\overline{\Gamma}_{\mathrm{w}}(G))$ are both isomorphic to S_{p+1}, fixing the isolated vertex corresponding to the identity. Furthermore, the group $\mathrm{Aut}(\Gamma(G)) = \mathrm{S}_{p-1} \wr \mathrm{S}_{p+1}$.*

Proof. Thinking of G as a vector space, two nonidentity elements $x, y \in G$ fail to generate G if and only if they lie in the same 1-dimensional subspace. Furthermore, they lie in the same 1-dimensional subspace if and only if $x \equiv_\Gamma y$. Thus $\overline{\Gamma}(G)$ is the disjoint union of the complete graph K_{p+1} and a vertex representing the identity, and all weights in K_{p+1} are equal to $p - 1$. $\square$

Before considering the groups of type (3), we require a standard graph-theoretic definition.

Definition 5.6. The *categorical product* $X \times Y$ of two graphs X and Y is the graph whose vertex set is the cartesian product of the vertex sets, with (x_1, y_1) joined to (x_2, y_2) if and only if x_1 is joined to x_2 in X and y_1 is joined to y_2 in Y.

Proposition 5.7. *Let $G \cong C_p^k : C_n$ be nonabelian with all proper quotients cyclic, and let $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$. The graph $\overline{\Gamma}(G)$ has $(2^r - 1)p^k + 2$ vertices if n is squarefree, and $2^r p^k + 2$ otherwise. The groups $\mathrm{Aut}(G)$ and $\mathrm{Aut}^*(G)$ are both isomorphic to $C_p^k : \Gamma\mathrm{L}_1(p^k)$. Furthermore, $\mathrm{Aut}(\overline{\Gamma}_{\mathrm{w}}(G)) \cong \mathrm{S}_{p^k}$, whilst $\mathrm{Aut}(\overline{\Gamma}(G)) \cong \mathrm{S}_{p^k} \times \mathrm{S}_r$.*

Proof. The elementary abelian subgroup C_p^k is characteristic in the group G, so $\mathrm{Aut}(G) \leq \mathrm{AGL}_k(p)$. The cyclic subgroup must embed as an irreducible subgroup of a Singer cycle, and so its centraliser in $\mathrm{GL}_k(p)$ is the full Singer cycle C_{p^k-1}, and its normaliser is the normaliser of the Singer cycle, which is $\Gamma\mathrm{L}_1(p^k)$.

We claim that $\overline{\Gamma}(G)$ is obtained from the categorical product of $\overline{\Gamma}(C_n)$ and the complete graph K_{p^k} by the following procedure:

(1) (a) If n is squarefree, identify all the vertices whose first component corresponds to the identity in C_n.
   (b) Otherwise, add a vertex adjacent to all vertices whose first component corresponds to a generator in C_n.
   The vertex in either case corresponds to the nonidentity elements of the minimal normal subgroup of G.
(2) Then add an isolated vertex corresponding to the identity.

Note that generators of C_n carry loops in $\Gamma(C_n)$; these give rise to edges in the categorical product between any two elements whose first components are equal and correspond to generators of C_n.

The weights of the vertices are the weights of their first components in $\overline{\Gamma}(C_n)$, except for the identified or added vertex in Step (1), whose weight is p^k in case (1)(a) and $p^k(|\Phi(C_n)|-1)$ in case (1)(b), and the identity which has weight 1.

Now we demonstrate that this structure is correct.

First note that in $\Gamma(G)$ all the nonidentity elements of the normal subgroup C_p^k are adjacent to all (and only) the generators of the complements C_n; so they all have the same neighbour sets and are $\equiv_\Gamma$-equivalent. Elements outside the normal subgroup are joined if and only if they lie in different complements and their images in the C_n quotient generate C_n. So two such elements are $\equiv_\Gamma$-equivalent if they lie in the same complement and are Γ-equivalent in C_n. Thus the graph has the structure claimed.

We now use the results of Proposition 5.4, from which the number of vertices of $\overline{\Gamma}(G)$ follows immediately. The automorphism group of $\overline{\Gamma}(C_n)$ is S_r, so $\mathrm{Aut}(\overline{\Gamma}(G))$ is $\mathrm{S}_{p^k} \times \mathrm{S}_r$.

Conversely, the group $\mathrm{Aut}(\overline{\Gamma}_{\mathrm{w}}(C_n))$ is trivial, so the weight-preserving automorphisms of $\overline{\Gamma}(G)$ are just the permutations of the p^k vertices of the complete graph.

Finally, we prove the claims about $\mathrm{Aut}^*(G)$. If $\mathrm{Aut}^*(G) \neq \mathrm{Aut}(G)$, then the unique minimal normal subgroup C_p^k of $\mathrm{Aut}(G)$ must act trivially on $\overline{\Gamma}_{\mathrm{w}}(G)$. However, this is not possible, for the following reason: let g be any element of G that generates a complement to C_p^k in g, and let x be any nontrivial element of C_p^k. Then $\langle g\rangle$ is a maximal subgroup of G, so $g^x \notin \langle g\rangle$ and $\langle g, g^x\rangle = G$. Hence g and g^x are incident in $\Gamma(G)$, and so $g \not\equiv_\Gamma g^x$. Hence x acts nontrivially on $\Gamma(G)$. □

For groups G as in the previous result, the kernel of the homomorphism from $\mathrm{Aut}(\Gamma(G))$ to $\mathrm{Aut}(\overline{\Gamma}_w(G))$ is the direct product of symmetric groups whose degrees are implicit in the proof: p^k-1 once, and the sizes of the nontrivial $\equiv_\Gamma$-classes in C_n (which can be read off from Proposition 4.7) each p^k times. The action of S_{p^k} is to permute the factors apart from the S_{p^k-1}.

Example 5.8. Consider the case $G = C_5 : C_4$. The generating graph for $C_4 = \langle x\rangle$ is the complete graph K_4 with the edge $\{1, x^2\}$ deleted and loops at x and x^3. So the reduced graph identifies 1 and x^2, and also x and x^3, and is an edge with a loop at one end. Thus, the reduced generating graph for $C_5 : C_4$ has 12 vertices, say $a_1, \ldots, a_5, b_1, \ldots, b_5, c, d$, with all edges $\{a_i, a_j\}$, all edges $\{a_i, b_j\}$, and no edges $\{b_i, b_j\}$ for $i \neq j$, all edges $\{a_i, c\}$, and d isolated. (Here a_i corresponds to an inverse pair of elements of order 4, b_i to an element of order 2, c to the four elements of order 5, and d to the identity.) Here the kernel of the homomorphism from $\mathrm{Aut}(\Gamma(G))$ to $\mathrm{Aut}(\overline{\Gamma}_{\mathrm{w}}(G))$ is $\mathrm{S}_4 \times (\mathrm{S}_2)^5$.

It remains to perform the analysis for the groups of type (4).

Theorem 5.9. *Let T be a finite simple group and let $N = T^r \leq G \leq \mathrm{Aut}(T) \wr \langle \sigma \rangle$, where σ acts as an r-cycle. Assume that there exists $g = (y_1, \ldots, y_r)\sigma$, with $y_1, \ldots, y_r \in \mathrm{Aut}(T)$, such that $G = N\langle g \rangle$. By substituting g by a conjugate in $\mathrm{Aut}(T) \wr \langle \sigma \rangle$, if necessary, we may assume that $g = (y, 1, \ldots, 1)\sigma$. If there exist $s, t \in T$ such that $T \leq \langle ys, (ys)^t \rangle$, then $\mathrm{Aut}(G) = \mathrm{Aut}^*(G)$.*

Proof. Since N is the unique minimal normal subgroup of $\mathrm{Aut}(G)$, if the conclusion is false, then N must act trivially on $\overline{\Gamma}(G)$. But this is impossible, for the following reason.

Let $\bar{y} = ys$ and $\bar{g} = (\bar{y}, 1, \ldots, 1)\sigma \in G$. Notice that G contains $\bar{g}^r = (\bar{y}, \ldots, \bar{y})$, $z = (t, 1, \ldots, 1)$ and $(\bar{g}^r)^z = (\bar{y}^t, \bar{y}, \ldots, \bar{y})$. Consider the subgroup X of G generated by $\bar{g}$ and $(\bar{g}^r)^z$. Since X contains $(\bar{y}, \ldots, \bar{y})$ and $(\bar{y}^t, \bar{y}, \ldots, \bar{y})$, we easily conclude that $X = G = \langle \bar{g}, (\bar{g}^r)^z \rangle$. Now if N acts trivially, then conjugacy classes under N are contained in $\equiv_\Gamma$-equivalence classes. Hence, in particular, $\bar{g}^r \equiv_\Gamma (\bar{g}^r)^z$, so $G = \langle \bar{g}, (\bar{g}^r)^z \rangle = \langle \bar{g}, \bar{g}^r \rangle = \langle \bar{g} \rangle$, a contradiction. □

Theorem 5.10. *Let G be a group of nonzero spread. Then $\mathrm{Aut}^*(G) = \mathrm{Aut}(G)$ if and only if G is nonabelian.*

Proof. The abelian groups of nonzero spread were considered in Propositions 5.4 and 5.5, where we showed that $\mathrm{Aut}^*(G) \neq \mathrm{Aut}(G)$.

The soluble nonabelian groups of nonzero spread were considered in Proposition 5.7, where we showed that $\mathrm{Aut}^*(G) = \mathrm{Aut}(G)$.

The only remaining case is the insoluble groups of nonzero spread (that is type (4)), so let G be such a group, and let $N \cong T^r = \mathrm{Soc}(G)$. We can identify G with a subgroup of $\mathrm{Aut}(T) \wr \langle \sigma \rangle$, where σ is the r-cycle $(1, 2, \ldots, r)$. Let t be an involution in T and let $n = (t, 1, \ldots, 1)$. Since G is of nonzero spread, there exists $g \in G$ with $G = \langle n, g \rangle$. Up to conjugation by an element of $(\mathrm{Aut}\, T)^r$, we may assume $g = (y, 1, \ldots, 1)\sigma$ for some $y \in \mathrm{Aut}(T)$. But now $G = \langle n, g \rangle$ implies that $H = \langle y, t \rangle$ is almost simple with socle T. Since $|t| = 2$, the subgroup $\langle y, y^t \rangle$ is normal in H. From this we see that $T \leq \langle y, y^t \rangle$, and so by Theorem 5.9, we conclude that $\mathrm{Aut}(G) = \mathrm{Aut}^*(G)$. □

We finish this discussion with an open problem:

Question 5.11. Let G be an insoluble group of nonzero spread. Is $\mathrm{Aut}(G) = \mathrm{Aut}(\overline{\Gamma}_{\mathrm{w}}(G))$?

We know of no examples where this is not the case.

5.1. **Calculations with $\overline{\Gamma}_{\mathrm{w}}(G)$.** In this subsection we describe some experiments that we have carried out on insoluble groups with nonzero spread.

Recall the definition of the m-universal action from Subsection 2.4, and that we showed in Theorem 2.26 that if G is almost simple, with socle of order less than 10000 and all proper quotients cyclic then $\psi(G) = 2$. It is immediate from Lemma 2.23(2) that two group elements x, y are incident in

$\Gamma(G)$ if and only if the fixed-point sets of x and y in the m-universal action are disjoint.

For each such almost simple group G, we constructed $\overline{\Gamma}(G)$ and hence $\mathrm{Aut}(\overline{\Gamma}(G))$. For all such groups except for $\mathrm{PSL}_2(16)$ and $\mathrm{PSL}_2(25)$ we found that $\mathrm{Aut}(\overline{\Gamma}(G)) \cong \mathrm{Aut}(G)$. In these remaining two cases, $\mathrm{Aut}(\overline{\Gamma}(G)) \cong C_2 \times \mathrm{Aut}(G)$, but the elements in the centre of $\mathrm{Aut}(\overline{\Gamma}(G))$ do not preserve the graph weightings. From this we can conclude:

Theorem 5.12. *Let G be an almost simple group with socle of order less than 10000 such that all proper quotients of G are cyclic. Then $\mathrm{Aut}(\overline{\Gamma}_{\mathrm{w}}(G)) = \mathrm{Aut}(G)$.*

In addition, we carried out the same calculation with the subgroups of $\mathrm{S}_5 \wr \mathrm{S}_2$ of nonzero spread (there are two of them), and for both such groups G we found that $\psi(G) = 2$ and there are no additional automorphisms of $\overline{\Gamma}_{\mathrm{w}}(G)$. That is, both such groups satisfied $\mathrm{Aut}(\overline{\Gamma}_{\mathrm{w}}(G)) = \mathrm{Aut}(G)$.

References

[1] A. Ballester-Bolinches and L.M. Ezquerro, *Classes of Finite Groups* Springer, 2006.

[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. R. Britnell, A. Evseev, R. M. Guralnick, P. E. Holmes and A. Maróti, Sets of elements that pairwise generate a linear group, *J. Combin. Theory Ser. A* **115** (2008), no. 3, 442–465.

[4] T. Burness, M. Liebeck and A. Shalev, Generation and random generation: from simple groups to maximal subgroups, *Adv. Math.* **248** (2013), 59–95.

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

[6] E. Crestani and A. Lucchini, The generating graph of finite soluble groups, *Israel J. Math.* **198** (2013), no. 1, 63–74.

[7] E. Crestani and A. Lucchini, Bias of group generators in the solvable case, *Israel J. Math.* **207** (2015), no. 2, 739–761.

[8] F. Dalla Volta and A. Lucchini, Finite groups that need more generators than any proper quotient, *J. Austral. Math. Soc.* Ser. A **64** (1998), no. 1, 82–91.

[9] P. Diaconis and L. Saloff-Coste, Walks on generating sets of groups, *Invent. Math.* **134** (1998), 251–299.

[10] W. Gaschütz, Zu einem von B. H. und H. Neumann gestellten Problem, *Math. Nachr.* **14** (1955), 249-252.

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

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

[13] J. I. Hall, Classifying copolar spaces and graphs, *Quart. J. Math. Oxford* **33** (1982), 421–449.

[14] S. Jambor, The minimal generating sets of $\mathrm{PSL}(2, p)$ of size four, *Lond. Math. Soc. J. Comput. Math.* **16** (2013), 419–423.

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

[16] M.W. Liebeck and A. Shalev, Simple Groups, Probabilistic Methods, and a Conjecture of Kantor and Lubotzky. *J. Algebra* **184** (1996), 31–57.

[17] A. Lucchini, The largest size of a minimal generating set of a finite group, *Arch. Math.* **101** (2013), no. 1, 1-8.
[18] A. Lucchini and A. Maróti, On the clique number of the generating graph of a finite group, *Proc. Amer. Math. Soc.* **137** (2009), no. 10, 3207–3217.
[19] A. Lucchini and A. Maróti, Some results and questions related to the generating graph of a finite group, in *Ischia group theory 2008*, 183–208, World Sci. Publ., Hackensack, NJ, 2009.
[20] A. Lucchini, A. Maróti, and C.M. Roney-Dougal, On the generating graph of a simple group, *J. Austral. Math. Soc.*, to appear.
[21] T. Łuczak and L. Pyber, On random generation of the symmetric group, *Combin., Prob. Comput.* **2** (1993), 505–512.
[22] The On-Line Encyclopedia of Integer Sequences, `https://oeis.org/`
[23] A. Maróti, Covering the symmetric groups with proper subgroups, *J. Combin. Theory Ser. A* **110** (2005), no. 1, 97–111.
[24] D. Robinson, *A course in the theory of groups,* Graduate Texts in Mathematics, **80** Springer-Verlag, New York-Berlin, 1982.
[25] A. Stein, 1 1/2-generation of finite simple groups, *Beiträge Algebra Geom.* **39** (1998), 349–358.
[26] A. Shalev, A theorem on random matrices and some applications. *J. Algebra* **199** (1998), 124–141.
[27] J. Whiston, Maximal independent generating sets of the symmetric group, *J. Algebra* **232** (2000), 255–268.

Peter J. Cameron, University of St Andrews, Mathematical Institute, St Andrews, Fife KY16 9SS, Scotland
E-mail address: `pjc20@st-andrews.ac.uk`

Andrea Lucchini, Dipartimento di Matematica, Università degli studi di Padova, Via Trieste 63, 35121 Padova, Italy
E-mail address: `lucchini@math.unipd.it`

Colva M. Roney-Dougal, University of St Andrews, Mathematical Institute, St Andrews, Fife KY16 9SS, Scotland
E-mail address: `colva.roney-dougal@st-andrews.ac.uk`