

# *Algebra & Number Theory*

Volume 7

2013

No. 9

**Normal coverings of linear groups**

John R. Britnell and Attila Maróti





# Normal coverings of linear groups

John R. Britnell and Attila Maróti

For a noncyclic finite group  $G$ , let  $\gamma(G)$  denote the smallest number of conjugacy classes of proper subgroups of  $G$  needed to cover  $G$ . In this paper, we show that if  $G$  is in the range  $SL_n(q) \leq G \leq GL_n(q)$  for  $n > 2$ , then  $n/\pi^2 < \gamma(G) \leq (n+1)/2$ . This result complements recent work of Bubboloni, Praeger and Spiga on symmetric and alternating groups. We give various alternative bounds and derive explicit formulas for  $\gamma(G)$  in some cases.

## 1. Introduction

**Normal coverings.** Let  $G$  be a noncyclic finite group. We write  $\gamma(G)$  for the smallest number of conjugacy classes of proper subgroups of  $G$  needed to cover it. In other words,  $\gamma(G)$  is the least  $k$  for which there exist subgroups  $H_1, \dots, H_k < G$  such that

$$G = \bigcup_{i=1}^k \bigcup_{g \in G} H_i^g.$$

We say that the set of conjugacy classes  $\{H_i^G \mid i = 1, \dots, k\}$  is a *normal covering* for  $G$ .

Bubboloni and Praeger [2011] have recently investigated  $\gamma(G)$  in the case that  $G$  is a finite symmetric or alternating group. They show, for example, that if  $n$  is an odd composite number then

$$\frac{\phi(n)}{2} + 1 \leq \gamma(S_n) \leq \frac{n-1}{2},$$

where  $\phi$  is Euler's totient function. Similar results are established for all values of  $n$  and for both  $S_n$  and  $A_n$ . Part of the motivation for their work comes from an application in number theory.

---

Britnell was supported by a Research Fellowship at the Heilbronn Institute for Mathematical Research. The research of Maróti was supported by a Marie Curie International Reintegration Grant within the seventh European Community Framework Programme, by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences and by OTKA K84233.

*MSC2010:* primary 20D60; secondary 20G40.

*Keywords:* covering, normal covering, linear group, finite group.

It is a well-known theorem of Jordan that no finite group is covered by the conjugates of any proper subgroup. To paraphrase,  $\gamma(G) \neq 1$  for any finite group  $G$ . It is known that there exists a finite solvable group  $G$  with  $\gamma(G) = k$  for every  $k > 1$  [Crestani and Lucchini 2012]. It has been shown in [Bubboloni and Lucido 2002] that if  $G$  is one of the groups  $\text{GL}_n(q)$ ,  $\text{SL}_n(q)$ ,  $\text{PGL}_n(q)$  or  $\text{PSL}_n(q)$ , then  $\gamma(G) = 2$  if and only if  $n \in \{2, 3, 4\}$ . (Notice that  $\gamma$  is undefined for  $n = 1$  since the groups are cyclic in this case.) Other groups of Lie type possessing a normal covering of size 2 have been studied in [Bubboloni et al. 2006; 2011].

In this paper, we give bounds on  $\gamma(G)$ , where  $\text{SL}_n(q) \leq G \leq \text{GL}_n(q)$ , for all values of  $n$ . In some cases, we are able to give an exact value. Our bounds extend without change to  $G/Z(G)$ .

We introduce some notation. We write  $\lfloor x \rfloor$  for the integer part of a real number  $x$ . As already noted above,  $\phi$  denotes Euler's function. We shall also use Lehmer's *partial totient function*, which we define here.

**Definition.** Let  $k$  and  $t$  be such that  $0 \leq t < k < n$ . We define the partial totient  $\phi(k, t, n)$  to be the number of integers  $x$ , coprime with  $n$ , such that

$$\frac{nt}{k} < x < \frac{n(t+1)}{k}.$$

We give two separate upper bounds on  $\gamma(G)$ .

**Theorem 1.1.** *Let  $n \in \mathbb{N}$ , and let  $v = v(n)$  be the number of prime factors of  $n$ . Let  $p_1, \dots, p_v$  be the distinct prime factors of  $n$  with  $p_1 < p_2 < \dots < p_v$ . Let  $G$  be a group such that  $\text{SL}_n(q) \leq G \leq \text{GL}_n(q)$ .*

(1) *If  $v \geq 2$ , then*

$$\gamma(G) \leq \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \frac{n}{2} + 2.$$

(2) *If  $n > 6$ , then*

$$\gamma(G) \leq \left\lfloor \frac{n}{3} \right\rfloor + \phi(6, 2, n) + v.$$

A great deal of information is given in [Lehmer 1955, §6] about the function  $\phi(6, t, n)$ , from which the following statement can be derived:

$$\frac{\phi(n)}{6} - \phi(6, 2, n) = \begin{cases} 0 & \text{if } n \text{ is divisible either by 9 or by a prime} \\ & \text{of the form } 3k + 1 \text{ for } k \in \mathbb{N}, \\ \frac{1}{12}\lambda(n)2^v & \text{otherwise, if } n \text{ is divisible by 3,} \\ \frac{1}{6}\lambda(n)2^v & \text{otherwise, if } n \text{ is not divisible by 3,} \end{cases}$$

in which  $\lambda(n) = (-1)^\ell$ , where  $\ell$  is the number of prime divisors of  $n$  counted with multiplicity.

**Independent sets of conjugacy classes.** Let  $\kappa(G)$  be the size of the largest set of conjugacy classes of  $G$  such that any pair of elements from distinct classes generates  $G$ . We call such a set an *independent set of classes*. Guralnick and Malle [2012] have shown that  $\kappa(G) \geq 2$  for any finite simple group  $G$ . It is clear that whenever  $\gamma(G)$  is defined, we have the inequality

$$\kappa(G) \leq \gamma(G)$$

since if  $\mathcal{C}$  is a normal covering of  $G$ , and if  $\mathcal{F}$  is an independent set of classes, then each element of  $\mathcal{C}$  covers at most one element of  $\mathcal{F}$ .

We establish two lower bounds for  $\kappa(G)$ . By the observation of the previous paragraph, these also operate as lower bounds for  $\gamma(G)$ .

**Theorem 1.2.** *Let  $n \in \mathbb{N}$ , and let  $\nu = \nu(n)$  be the number of prime factors of  $n$ . Let  $p_1, \dots, p_\nu$  be the distinct prime factors of  $n$  with  $p_1 < p_2 < \dots < p_\nu$ . Let  $G$  be a group such that  $\text{SL}_n(q) \leq G \leq \text{GL}_n(q)$ .*

(1) *If  $\nu \geq 2$ , then*

$$\frac{\phi(n)}{2} + \nu(n) \leq \kappa(G).$$

(2) *If  $\nu \geq 3$ , and if  $n$  is not equal to  $6p$  or  $10p$  for any prime  $p$ , then*

$$\left\lfloor \frac{n+6}{12} \right\rfloor + \phi(12, 1, 3n) + \nu \leq \kappa(G).$$

*Furthermore, if  $\text{hcf}(n, 6) = 1$ , then*

$$\left\lfloor \frac{n+6}{12} \right\rfloor + \phi(12, 1, 3n) + \phi(12, 0, n) + \nu \leq \kappa(G).$$

The values  $t = 0, 1$  are not amongst those for which the function  $\phi(12, t, n)$  is evaluated explicitly in [Lehmer 1955]. However, Theorem 10 of the same work gives the general estimate

$$|\phi(n) - k\phi(k, t, n)| \leq (k - 1)2^\nu,$$

where  $\nu$  is the number of prime divisors of  $n$ . This yields the lower bound

$$\phi(12, t, n) \geq \frac{\phi(n)}{12} - \frac{11}{12}2^\nu.$$

There are certain cases in which an upper bound for  $\gamma(G)$  coincides with a lower bound for  $\kappa(G)$ . In these cases, we must have  $\gamma(G) = \kappa(G)$ , and we obtain a precise formula.

**Theorem 1.3.** *Let  $G$  be a group such that  $\text{SL}_n(q) \leq G \leq \text{GL}_n(q)$ .*

(1) *If  $n = p^a$ , where  $p$  is a prime and  $a \in \mathbb{N}$ , and if  $n > 2$ , then*

$$\gamma(G) = \kappa(G) = \left(1 - \frac{1}{p}\right)\frac{n}{2} + 1.$$

(2) If  $n = p^a q^b$ , where  $p$  and  $q$  are distinct primes and  $a, b \in \mathbb{N}$ , then

$$\gamma(G) = \kappa(G) = \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{q}\right) \frac{n}{2} + 2.$$

(3) If  $n = 6p$ , where  $p$  is a prime, then  $\gamma(G) = \kappa(G) = p + 2$ .

(4) If  $n = 10p$ , where  $p$  is a prime, then  $\gamma(G) = \kappa(G) = 2p + 2$ .

Certain cases of Theorem 1.3 will require independent treatment as they arise as exceptional cases in the proof of Theorem 1.2.

**Linear bounds.** Theorems 1.1(1), 1.2(2) and 1.3, taken together, imply that

$$\frac{n}{12} < \kappa(G) \leq \gamma(G) \leq \frac{n+1}{2} \quad (1)$$

for all  $n > 2$ . The upper bound is exact when  $n$  is an odd prime. (When  $n = 2$ , it is known that  $\gamma(G) = 2$ ; see [Bubboloni and Lucido 2002] or the remark after Proposition 4.1 below. It is also easy to show that  $\kappa(G) = 2$  in this case.) It follows immediately that

$$\limsup \frac{\gamma(G)}{n} = \frac{1}{2}. \quad (2)$$

The lower bound for  $\gamma$  can be improved as the following theorem indicates:

**Theorem 1.4.** *If  $G$  is a group such that  $\mathrm{SL}_n(q) \leq G \leq \mathrm{GL}_n(q)$ , then  $n/\pi^2 < \gamma(G)$ .*

From the first part of Theorem 1.1 and from Theorem 1.4, it is easy to show that

$$\frac{1}{\pi^2} \leq \liminf \frac{\gamma(G)}{n} \leq \frac{1}{6}. \quad (3)$$

It follows from the theorems that we have stated that  $\gamma(G)$  and  $\kappa(G)$  are bounded above and below by monotonic functions that grow linearly with  $n$ . It appears that the situation for symmetric groups is similar. It was announced in [Bubboloni et al. 2012, §1.1] and demonstrated in [Bubboloni et al. 2013] that  $\gamma(S_n)$  and  $\gamma(A_n)$  are bounded above and below by linear functions of  $n$ . In fact, the numbers  $\gamma(S_n)$  and  $\gamma(\mathrm{GL}_n(q))$  seem to be closely related; in all cases where both are known exactly, they differ by at most 1. It is not hard to show, and it is worth remarking in this connection, that the upper bounds stated for  $\gamma(G)$  in Theorem 1.1 are also upper bounds for  $\gamma(S_n)$  improving marginally on those of [Bubboloni and Praeger 2011, Theorem A]. It should also be noted that all of our bounds are independent of the field size  $q$ .

We establish the upper bounds of Theorem 1.1 in Section 2 by exhibiting explicit normal coverings of the necessary sizes. This builds on work described in [Britnell et al. 2008], in which coverings of  $\mathrm{GL}_n(q)$  by proper subgroups are constructed. The two lower bounds of Theorem 1.2 are proved in Section 3. Both are proved by exhibiting an independent set of classes. This requires an account of overgroups of

certain special elements in  $GL_n(q)$ . For such an account, we rely on [Guralnick et al. 1999], which provides a classification of subgroups whose orders are divisible by primitive prime divisors of  $q^d - 1$  for all  $d > n/2$ . The remaining cases of Theorem 1.3 are brought together in Section 4. Finally, Theorem 1.4 is established in Section 5. Its proof relies on work from the doctoral thesis of Joseph DiMuro [2007], which extends the classification of [Guralnick et al. 1999] to cover all  $d \geq n/3$ .

The classes of subgroups in our normal covering remain distinct, proper and nontrivial in the quotient of  $G$  by  $Z(G)$ . This is true also of the classes of maximal overgroups that cover the conjugacy classes in our independent sets. It follows that the bounds that we have stated for  $\gamma(G)$  and for  $\kappa(G)$  hold equally for  $\gamma(G/Z(G))$  and for  $\kappa(G/Z(G))$ .

## 2. Normal coverings of $G$

We shall write  $V$  for the space  $\mathbb{F}_q^n$ . We assume that  $SL(V) \leq G \leq GL(V)$  throughout the paper.

We begin by introducing the classes of subgroups that we shall need for our coverings. Proposition 2.1 below contains standard information about certain subgroups of  $GL_n(q)$ , and we shall not prove it here.

**Proposition 2.1.** (1) *Let  $d$  be a divisor of  $n$ . There exist embeddings of  $GL_{n/d}(q^d)$  into  $GL_n(q)$ . All such embeddings are conjugate by elements of  $SL_n(q)$ , and each has index  $d$  in its normalizer in  $GL_n(q)$ . If  $d$  is prime, then the normalizer is a maximal subgroup of  $GL_n(q)$ .*

(2) *Suppose that  $1 \leq k < n$ , and let  $U$  be a  $k$ -dimensional subspace of  $V$ . Then the set stabilizer  $G_U$  of  $U$  in  $G$  is a maximal subgroup of  $G$ . If  $W$  is another  $k$ -dimensional subspace, then  $G_U$  and  $G_W$  are conjugate in  $G$ .*

It will be convenient to have concise notation for these subgroups.

**Definition.** (1) We refer to the maximal subgroups of Proposition 2.1(1) as *extension field subgroups* of degree  $d$ , and we write  $\text{efs}(d)$  for the conjugacy class consisting of the intersections of all such subgroups with the group  $G$ .

(2) We refer to the subgroups of Proposition 2.1(2) as *subspace stabilizers* of dimension  $k$ , and we write  $\text{ss}(k)$  for the conjugacy class consisting of all such subgroups.

The following technical lemma will be useful:

**Lemma 2.2.** (1) *Suppose that  $X \in GL(V)$  and that  $X$  stabilizes a  $k$ -dimensional subspace of  $V$ . Then  $X$  stabilizes a subspace whose dimension is  $n - k$ .*

(2) *Let  $X \in GL(V)$ , and let  $p$  be a prime dividing  $n$ . If  $X$  lies in no extension field subgroup of degree  $p$ , then it stabilizes a subspace of  $V$  whose dimension is coprime with  $p$ .*

*Proof.* (1) Suppose  $X$  stabilizes a space  $U$  of dimension  $k$ . Then the transpose  $X^t$  acts on the dual space  $V^*$  and stabilizes the annihilator of  $U$ , which has dimension  $n - k$ .

(2) If  $X$  stabilizes no subspace whose dimension is coprime with  $p$ , then every irreducible divisor of its characteristic polynomial has degree divisible by  $p$  and must therefore split into  $p$  factors over  $\mathbb{F}_{q^p}$ . Suppose that the elementary divisors of  $X$  are  $f_1^{a_1}, \dots, f_t^{a_t}$ . For each  $i$ , let  $g_i$  be an irreducible factor of  $f_i$  over  $\mathbb{F}_{q^p}$ , and let  $Y \in \text{GL}_{n/p}(q^p)$  have elementary divisors  $g_1^{a_1}, \dots, g_t^{a_t}$ . Then it is not hard to see that any embedding of  $\text{GL}_{n/p}(q^p)$  into  $\text{GL}_n(q)$  must map  $Y$  to a conjugate of  $X$ .  $\square$

We are now in a position to exhibit some normal coverings of  $G$ .

**Lemma 2.3.** (1) *Let  $p$  be a prime dividing  $n$ . Then there is a normal covering  $\mathcal{C}_p$  for  $G$  given by*

$$\mathcal{C}_p = \{\text{efs}(p)\} \cup \{\text{ss}(k) \mid 1 \leq k \leq n/2, p \nmid k\}.$$

The size of  $\mathcal{C}_p$  is

$$|\mathcal{C}_p| = \left\lfloor \left(1 - \frac{1}{p}\right) \frac{n}{2} \right\rfloor + 1 + \epsilon,$$

where

$$\epsilon = \begin{cases} 1 & \text{if } p = 2 \text{ and } n/2 \text{ is odd,} \\ 0 & \text{otherwise.} \end{cases}$$

This is minimized when  $p$  is the smallest prime divisor of  $n$ .

(2) *Let  $p_1$  and  $p_2$  be distinct prime divisors of  $n$ . Then there is a normal covering  $\mathcal{C}_{p_1, p_2}$  for  $G$  given by*

$$\mathcal{C}_{p_1, p_2} = \{\text{efs}(p_1), \text{efs}(p_2)\} \cup \{\text{ss}(k) \mid 1 \leq k < n/2, p_1, p_2 \nmid k\}.$$

The size of  $\mathcal{C}_{p_1, p_2}$  is

$$|\mathcal{C}_{p_1, p_2}| = \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \frac{n}{2} + 2.$$

This is minimized when  $p_1$  and  $p_2$  are the two smallest prime divisors of  $n$ .

*Proof.* The sizes of the sets  $\mathcal{C}_p$  and  $\mathcal{C}_{p_1, p_2}$  are easily seen to be as stated. That  $\mathcal{C}_p$  is a normal covering follows immediately from Lemma 2.2. So it remains only to prove that  $\mathcal{C}_{p_1, p_2}$  is a normal covering.

Let  $X \in G$ , let  $f_X$  be the characteristic polynomial of  $X$ , and let  $g_1, \dots, g_s$  be the irreducible factors of  $f_X$  over  $\mathbb{F}_q$  with degrees  $d_1, \dots, d_s$ , respectively. Then clearly there exist  $X$ -invariant subspaces  $U_1, \dots, U_s$  such that  $\dim U_i = d_i$  for all  $i$  and such that  $U_i \cap U_j = \{0\}$  whenever  $i \neq j$ . If any  $d_i$  is divisible by neither of the primes  $p_1$  and  $p_2$ , then  $X$  is contained in a subspace stabilizer from one of



the classes in  $\mathcal{C}_{p_1, p_2}$ . So we assume that each  $d_i$  is divisible by at least one of  $p_1$  or  $p_2$ . Suppose that  $d_a$  is divisible by  $p_1$  but not by  $p_2$  and that  $d_b$  is divisible by  $p_2$  but not by  $p_1$ . Then  $U_a \oplus U_b$  is an  $X$ -invariant subspace, and its dimension is coprime with  $p_1$  and  $p_2$ ; so again,  $X$  is in a subspace stabilizer from  $\mathcal{C}_{p_1, p_2}$ . But if no such  $d_a$  and  $d_b$  can be found, then either all of the  $d_i$  are divisible by  $p_1$  or they are all divisible by  $p_2$ . In this case,  $X$  lies in an extension field subgroup either of degree  $p_1$  or of degree  $p_2$ .  $\square$

We note that the argument of the last paragraph of this proof does not extend to the case of three primes,  $p_1, p_2$  and  $p_3$ . It is possible to find matrices whose invariant subspaces all have dimensions divisible by one of those primes but which lie in no extension field subgroup. In the case that the primes are 2, 3 and 5, for instance, there are 30-dimensional matrices whose irreducible invariant spaces have dimensions 2, 3 and 25. (Another example is used in the proof of Proposition 4.4 below.) This is the explanation for the appearance of the two smallest prime divisors of  $n$  in the first upper bound of Theorem 1.1, which may at first seem a little curious.

The second upper bound of Theorem 1.1 is proved in a somewhat similar fashion.

**Lemma 2.4.** *Let  $p_1, \dots, p_\nu$  be the distinct primes dividing  $n$ . Then there is a normal covering  $\mathcal{D}$  of  $G$  given by*

$$\begin{aligned} \mathcal{D} = & \{ss(k) \mid 1 \leq k \leq n/3\} \\ & \cup \{ss(k) \mid n/3 < k \leq n/2, \text{hcf}(k, n) = 1\} \\ & \cup \{efs(p_i) \mid 1 \leq i \leq \nu\}. \end{aligned}$$

For  $n > 6$ , the size of  $\mathcal{D}$  is

$$\left\lfloor \frac{n}{3} \right\rfloor + \phi(6, 2, n) + \nu.$$

*Proof.* Let  $X \in G$ . Suppose that  $X$  is reducible and that its smallest nontrivial invariant subspace has dimension  $k$ . If  $k > n/3$ , then it is not hard to see (for instance, by considering the irreducible factors of the characteristic polynomial) that  $X$  stabilizes at most one other proper nontrivial subspace of dimension  $n - k$ . It follows that if  $p$  is a prime dividing both  $n$  and  $k$ , then  $X$  is contained in an element of  $efs(p)$ . It is now a straightforward matter to show that  $\mathcal{D}$  is a normal covering, and we omit further details. The size of  $\mathcal{D}$  follows immediately from its definition.  $\square$

### 3. Lower bounds for $\kappa(G)$

Recall that  $GL_n(q)$  contains elements of order  $q^n - 1$ , known as Singer elements. Such elements stabilize no nontrivial proper subspace of  $V$ . The determinant of a Singer element generates the multiplicative group of  $\mathbb{F}_q$ .

In order to handle all groups  $G$  in the range  $SL_n(q) \leq G \leq GL_n(q)$  together, we define a parameter  $\alpha \in \mathbb{N}$  by

$$\alpha = \begin{cases} 0 & \text{if } G = SL_n(q), \\ -|GL_n(q) : G| & \text{otherwise.} \end{cases}$$

Let  $\zeta$  be a generator of the multiplicative group of  $\mathbb{F}_q$ . Then we have

$$\frac{G}{SL_d(q)} \cong \langle \zeta^\alpha \rangle.$$

**Definition.** (1) For  $d = 1, \dots, n$ , let  $\Gamma_d$  be a Singer element with determinant  $\zeta$  in  $GL_d(q)$ .

(2) For  $k < n/2$ , define

$$\Sigma_k = \text{diag}(\Gamma_k^{\alpha-1}, \Gamma_{n-k}).$$

(3) For  $j < (n - 2)/4$ , define

$$T_j = \text{diag}(\Gamma_j^{\alpha-2}, \Gamma_{j+1}, \Gamma_{n-2j-1}).$$

The reasons for defining  $\alpha$  as above will be clear from the following remark:

**Remark.** (1) Since  $\det \Sigma_k = \det T_j = \zeta^\alpha$ , we have  $\Sigma_k, T_j \in G$ .

(2) It is clear from the definition of  $\alpha$  that  $(1 - q) < \alpha \leq 0$  and hence that  $|\alpha - 2| < q + 1$ . It follows easily that the actions of the matrices  $\Gamma_k^{\alpha-1}$  and  $\Gamma_j^{\alpha-2}$  are irreducible for all  $k$  and  $j$ . Therefore, the module  $\mathbb{F}_q \langle \Sigma_k \rangle$  decomposes into precisely two irreducible summands, and  $\mathbb{F}_q \langle T_j \rangle$  decomposes into precisely three irreducible summands.

**Lemma 3.1.** *Suppose that  $n > 4$ . Let  $k < n/2$ , and if  $q = 2$ , then suppose that  $n - k \neq 6$ . Let  $j < (n - 2)/4$ , and if  $q = 2$ , then suppose that  $n - 2j - 1 \neq 6$ .*

- (1) *If  $M$  is a maximal subgroup of  $G$  containing  $\Gamma_n$ , then  $M$  is an extension field subgroup of prime degree.*
- (2) *If  $M$  is a maximal subgroup of  $G$  containing  $\Sigma_k$ , then  $M$  is either an extension field subgroup whose degree is a prime divisor of  $\text{gcd}(k, n)$  or else the stabilizer of a subspace of dimension  $k$  or  $n - k$ .*
- (3) *Let  $n$  have at least three distinct prime divisors. If  $M$  is a maximal subgroup of  $G$  containing  $T_j$ , then  $M$  is the stabilizer of a subspace whose dimension is one of  $j, j + 1, 2j + 1, n - 2j - 1, n - j - 1$  or  $n - j$ .*

*Proof.* Part (1) of the lemma is a result of Kantor [1980].

For  $(n, q) \neq (11, 2)$ , part (2) of the lemma follows from [Britnell et al. 2008, Theorem 4.1(2)]. However, a few comments are to be made about this assertion. The matrix that we have called  $\Sigma_k$  is referred to as GLk in [Britnell et al. 2008]. The result in [Britnell et al. 2008] is stated only for the groups  $GL_n(q)$  and  $SL_n(q)$ , but the proof given there applies equally to intermediate subgroups. Finally, the proof in [Britnell et al. 2008] relies on the existence of primitive prime divisors of  $q^{n-k} - 1$  (where  $n - k > 2$ ), which is given by the theorem of Zsigmondy [1892] for all pairs  $(q, n - k)$  except  $(2, 4)$  and  $(2, 6)$ ; the second of these exceptions accounts for the excluded case in the statement of the present lemma. The argument uses the classification in [Guralnick et al. 1999] of subgroups of  $GL_n(q)$  whose order is divisible by a prime divisor of  $q^e - 1$ , where  $e > n/2$ .

To finish the proof of part (2) of the present lemma, we must consider the exceptional case of the group  $GL_{11}(2)$ . In this case, we require a reference directly to the lists of [Guralnick et al. 1999]. We find that there are several irreducible subgroups whose order is divisible by a primitive prime divisor 11 of  $2^{10} - 1$ ; we must show that none of these contains  $\Sigma_1$ . All of these subgroups are almost simple and have a socle that is isomorphic either to one of the Mathieu groups  $M_{23}$  or  $M_{24}$  or to the unitary group  $PSU_5(2)$  or to a linear group  $SL_2(11)$  or  $SL_2(23)$ . (These subgroups may be found in Table 5 (lines 12 and 14) and Table 8 (lines 2, 7 and 9) of [Guralnick et al. 1999].) Information about these groups may be found in [Conway et al. 1985]. None of these groups themselves, nor any of their outer automorphism groups, have order divisible by 31. Therefore, an almost simple group of one of these types can contain no element of order  $2^{10} - 1 = 3 \cdot 11 \cdot 31$ , which is the order of the element  $\Sigma_1$ .

For the proof of part (3) of the lemma, we refer once again to the classification of [Guralnick et al. 1999], this time for matrix groups whose order is divisible by a primitive prime divisor of  $q^{n-2j-1} - 1$ . It is not hard to see that  $T_j$  has no overgroups of classical type. The condition that  $n$  has three distinct prime divisors rules out the small dimensional sporadic examples contained in Tables 1–7. Other examples are ruled out because their order is less than  $q^{n-2j-1} - 1$ , which is the order of the summand  $\Gamma_{n-2j-1}$  of  $T_j$ . □

We define a set of classes that will help us to establish the first of our lower bounds for  $\kappa(G)$ .

**Definition.** Define a set  $\Phi$  of classes of  $G$  by

$$\Phi = \{[\Sigma_p] \mid p \mid n, p \text{ prime}, p < n/2\} \cup \{[\Sigma_k] \mid k < n/2, \text{hcf}(n, k) = 1\},$$

where  $[g]$  denotes the conjugacy class of  $g$ .

**Lemma 3.2.** *Let  $n > 2$ , and let  $v(n)$  be the number of prime factors of  $n$ . Then*

$$|\Phi| = \phi(n)/2 + v(n) - \epsilon,$$

where

$$\epsilon = \begin{cases} 1 & \text{if } n = 2p \text{ for some odd prime } p, \\ 0 & \text{otherwise.} \end{cases}$$

*Proof.* This is immediate from the definition of  $\Phi$ . □

Lemma 3.2, together with the following two lemmas, will imply the first part of Theorem 1.2:

**Lemma 3.3.**  *$\Phi$  is an independent set of classes.*

*Proof.* Suppose that  $q \neq 2$  or that  $[\Sigma_{n-6}] \notin \Phi$ . Then Lemma 3.1 provides full information about the maximal subgroups of  $G$  that contain elements of  $\Phi$ , and it is easy to check that the result holds in this case.

Next suppose that  $q = 2$  and  $[\Sigma_{n-6}] \in \Phi$ . (This implies that  $n \in \{7, 8, 9, 11\}$ .) Lemma 3.1 gives full information about the maximal subgroups of  $G$  covering elements of the classes in  $\Phi$  other than  $[\Sigma_{n-6}]$ . No class of subgroups contains elements of more than one such class, and it is easy to check that none covers the element  $\Sigma_{n-6}$  itself. □

**Lemma 3.4.** *Let  $n = 2p$ , where  $p > 2$  is a prime. Then  $\kappa(G) \geq |\Phi| + 1$ .*

*Proof.* The proof of Lemma 3.3 shows that in any normal covering of  $G$ , the distinct classes in  $\Phi$  are covered by distinct classes of subgroups. We add an extra conjugacy class to  $\Phi$ , namely the class represented by  $\Sigma_p = \text{diag}(\Gamma_p^{\alpha-1}, \Gamma_p)$ , where  $\Gamma_p$  is a Singer element in  $\text{GL}_p(q)$ . This element stabilizes no subspace of dimension  $k$  for any  $k$  coprime with  $n$  nor does it stabilize a subspace of dimension 2 or  $n - 2$ . Therefore, by part (2) of Lemma 3.1, if  $\Phi \cup \{[\Sigma_p]\}$  is not an independent set of classes, then  $\Sigma_p$  must lie in a subgroup in  $\text{efs}(2)$ .

Note that since 2 and  $p$  are coprime,  $\Sigma_p^2$  has two irreducible summands of dimension  $p$ . It is not hard to show that these submatrices are not conjugate, and neither of them is reducible over  $\mathbb{F}_{q^2}$ ; it follows that  $\Sigma_p^2$  is not contained in any embedding of  $\text{GL}_p(q^2)$  into  $G$ . Hence,  $\Sigma_p$  itself is not contained in an embedding of  $\text{GL}_p(q^2) \cdot 2$ . □

Lemmas 3.2, 3.3 and 3.4 complete the proof of part (1) of Theorem 1.2.

We define a second independent set of classes that yields the second lower bound of Theorem 1.2. We shall require the following lemma:

**Lemma 3.5.** *Let  $p$  be a prime divisor of  $n$ . Suppose that  $n$  has at least three distinct prime divisors and that  $n$  is not equal to  $6q$  or  $10q$  for any prime  $q$ . Then there exists an integer  $w_p$  such that  $(n - 2)/4 \leq w_p < n/2$  and such that  $w_p$  is divisible*

by  $p$  and by no other prime divisor of  $n$ . If  $p \neq 3$ , then  $w_p$  may be chosen so that it is not divisible by 3.

*Proof.* Bertrand's postulate states that for every  $k > 3$  there is a prime  $r$  such that  $k < r < 2k - 2$ . The conditions on  $n$  imply that  $n \geq 12p$ . So there is a prime  $r > 3$  such that

$$\frac{n}{4p} < r < \frac{n}{2p}.$$

If  $r$  is not itself a prime divisor of  $n$  or if it is equal to  $p$ , then we may take  $w_p = pr$ . On the other hand, if  $r$  is a prime divisor of  $n$  other than  $p$ , then clearly  $n = 3pr$ , and since we have assumed that  $n \geq 12p$ , we have  $r \geq 5$ . Now we see that there exists  $m$  equal either to  $r + 1$  or to  $r + 2$  such that  $m$  is not divisible by 3, and we may take  $w_p = pm$ . □

**Definition.** Let  $n$  be a number with at least three distinct prime divisors and not equal to  $6p$  or  $10p$  for any prime  $p$ . We define a set  $\Psi$  of classes of  $G$  by

$$\begin{aligned} \Psi = & \{[T_j] \mid j < (n - 2)/4, j \equiv 1 \pmod 3\} \\ & \cup \{[\Sigma_k] \mid n/4 < k < n/2, \text{hcf}(3n, k) = 1\} \\ & \cup \{[\Sigma_{6b}] \mid b < n/12, \text{hcf}(n, 6b) = 1\} \\ & \cup \{[\Sigma_{w_p}] \mid p \mid n, p \text{ prime}\}, \end{aligned}$$

where  $w_p$  is as constructed in Lemma 3.5 and where  $[g]$  denotes the conjugacy class of  $g$ .

To describe the size of the set  $\Psi$ , we use Lehmer's partial totient function  $\phi(k, t, n)$ , which was defined before the statement of Theorem 1.1 above.

**Lemma 3.6.** *Let  $n$  have  $v$  distinct prime divisors, where  $v \geq 3$ , and suppose that  $n$  is not equal to  $6p$  or  $10p$  for any prime  $p$ .*

(1) *If 2 or 3 divides  $n$ , then*

$$|\Psi| = \left\lfloor \frac{n+6}{12} \right\rfloor + \phi(12, 1, 3n) + v.$$

(2) *If  $\text{hcf}(n, 6) = 1$ , then*

$$|\Psi| = \left\lfloor \frac{n+6}{12} \right\rfloor + \phi(12, 1, 3n) + \phi(12, 0, n) + v.$$

*Proof.* We write  $\lceil x \rceil$  for the least integer not less than  $x$ . The size  $X$  of the set  $\{[T_j] \mid j < (n - 2)/4, j \equiv 1 \pmod 3\}$  is  $\lceil N/3 \rceil$ , where  $N = \lfloor (n - 2)/4 \rfloor$ . By examining residues modulo 12, it is not hard to show that  $X = \lfloor (n + 6)/12 \rfloor$ , the first term in our sum.

It is immediate from the definition of the function  $\phi(k, t, n)$  that the size of the set  $\{[\Sigma_k] \mid n/4 < k < n/2, \text{hcf}(3n, k) = 1\}$  is  $\phi(12, 1, 3n)$ . We observe that the set

$\{[\Sigma_{6b}] \mid b < n/12, \text{hcf}(n, 6b) = 1\}$  is empty if  $\text{hcf}(n, 6) \neq 1$ ; otherwise, it has size  $\phi(12, 0, n)$ . And clearly the set  $\{[\Sigma_{w_p}] \mid p \mid n, p \text{ prime}\}$  has size  $\nu$  as required.  $\square$

To establish the second lower bound in Theorem 1.2, it will suffice to show that any normal covering for  $G$  has size at least  $|\Psi|$ . This is done in the following lemma:

**Lemma 3.7.** *Let  $n$  have at least three distinct prime divisors and not be equal to  $6p$  or  $10p$  for any prime  $p$ . Then  $\Psi$  is an independent set of classes.*

*Proof.* Lemma 3.1 describes the maximal subgroups of  $G$  that contain elements of the classes in  $\Psi$ . The elements  $T_j$  lie only in members of  $\text{ss}(\ell)$  or  $\text{ss}(n - \ell)$ , where  $\ell \in \{j, j + 1, 2j + 1\}$ . Notice that if  $\ell > n/4$ , then  $\ell = 2j + 1$ , and hence,  $\ell \equiv 3 \pmod{6}$ . The elements  $\Sigma_k$ , where  $k$  is coprime with  $n$ , lie only in members of  $\text{ss}(k)$  or  $\text{ss}(n - k)$ . And the elements  $\Sigma_{w_p}$  lie in subspace stabilizers and also in elements of  $\text{efs}(p)$ . It is easy to check that the values permitted for  $j, k, b$  and  $w_p$  ensure that no two elements of distinct classes in  $\Psi$  stabilize subspaces of the same dimension. Therefore, no two classes in  $\Psi$  can be covered by a single class of subgroups.  $\square$

#### 4. Several equalities

In this section, we establish the various claims of Theorem 1.3. We do this simply by comparing upper and lower bounds from earlier parts of the paper.

**Proposition 4.1.** *If  $n = p^a$ , where  $p$  is a prime and  $a \in \mathbb{N}$ , and if  $n > 2$ , then*

$$\gamma(G) = \kappa(G) = \left(1 - \frac{1}{p}\right)\frac{n}{2} + 1.$$

*Proof.* Lemmas 2.3 and 3.3 together tell us that

$$|\Phi| \leq \kappa(G) \leq \gamma(G) \leq |\mathcal{C}_p|.$$

But it is easy to check, using Lemma 3.2, that  $|\Phi| = |\mathcal{C}_p|$  and that this number is as claimed in the proposition.  $\square$

**Remark.** If  $n = 2$ , then the covering  $\mathcal{C}_2$  has size 2. Since no finite group is covered by a single class of proper subgroups, it follows that  $\gamma(G) = 2$  in this case.

**Proposition 4.2.** *If  $n = p^a q^b$ , where  $p$  and  $q$  are distinct primes and  $a, b \in \mathbb{N}$ , then*

$$\gamma(G) = \kappa(G) = \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)\frac{n}{2} + 2.$$

*Proof.* As in the proof above, Lemma 2.3 with Lemmas 3.3 and 3.4 yields that

$$|\Phi| + \epsilon \leq \kappa(G) \leq \gamma(G) \leq |\mathcal{C}_{p,q}|,$$

where  $\epsilon = 1$  if  $n = 2p$  (or  $n = 2q$ ) and  $\epsilon = 0$  otherwise. But we see that  $|\Phi| + \epsilon = |\mathcal{C}_{p,q}|$  and that this number is as claimed in the proposition.  $\square$

**Proposition 4.3.** *If  $n = 6p$ , where  $p$  is a prime, then*

$$\gamma(G) = \kappa(G) = p + 2.$$

*Proof.* In this case, we have

$$|\Phi| \leq \kappa(G) \leq \gamma(G) \leq |\mathcal{C}_{2,3}|,$$

and it is easy to calculate that  $|\Phi| = |\mathcal{C}_{2,3}| = p + 2$ . □

**Proposition 4.4.** *If  $n = 10p$ , where  $p$  is a prime, then*

$$\gamma(G) = \kappa(G) = 2p + 2.$$

*Proof.* If  $p$  is 2 or 5, then the result follows from Proposition 4.2; if  $p = 3$ , then it follows from Proposition 4.3. So we may assume that  $p > 5$ . Then we have

$$|\Phi| \leq \kappa(G) \leq \gamma(G) \leq |\mathcal{C}_{2,5}|,$$

but in this case, we see that  $|\Phi| = 2p + 1$  whereas  $|\mathcal{C}_{2,5}| = 2p + 2$ . To prove that the upper bound is sharp for  $\kappa(G)$ , it will be sufficient to exhibit an element  $Y$  of  $G$  that cannot be covered by any class of subgroups containing an element of any conjugacy class in  $\Phi$ . We define

$$Y = \text{diag}(\Gamma_p^{\alpha-2}, \Gamma_5, \Gamma_{n-p-5}).$$

Notice that  $n - p - 5$  is even and coprime with 5 and with  $p$ . It follows that  $Y$  does not stabilize a subspace of dimension coprime with  $n$ . But certainly  $Y$  lies in no extension field subgroup, and so it satisfies the required condition. □

### 5. Proof of Theorem 1.4

For a positive integer  $n$ , let  $f(n)$  be the number of partitions of  $n$  with exactly three parts. By an elementary counting argument, the following formula can be found for  $f(n)$ :

**Lemma 5.1.** 
$$f(n) = \begin{cases} \frac{1}{12}(n-1)(n-2) + \frac{1}{2}\lfloor (n-1)/2 \rfloor & \text{if } 3 \nmid n, \\ \frac{1}{12}(n-1)(n-2) + \frac{1}{2}\lfloor (n-1)/2 \rfloor + \frac{1}{3} & \text{if } 3 \mid n. \end{cases}$$

It follows from Lemma 5.1 that

$$\left| f(n) - \frac{n^2}{12} \right| \leq \frac{1}{3}.$$

We define  $\epsilon_n = f(n) - n^2/12$ .

Let  $P(n)$  be the set of partitions of  $n$  into three parts having no common divisor greater than 1. Let  $g(n) = |P(n)|$ . Then we have  $f(n) = \sum_{d|n} g(d)$ . By the Möbius

inversion formula, we obtain

$$\begin{aligned} g(n) &= \sum_{d|n} \mu(d) f(n/d) = \sum_{d|n} \mu(d) \frac{1}{12} (n/d)^2 + \sum_{d|n} \mu(d) \epsilon_{n/d} \\ &> \frac{n^2}{12} \sum_{d|n} \frac{\mu(d)}{d^2} + \sum_{d|n} \mu(d) \epsilon_{n/d} \\ &> \frac{n^2}{12} \prod_{p \text{ prime}} \left(1 - \frac{1}{p^2}\right) + \sum_{d|n} \mu(d) \epsilon_{n/d}. \end{aligned}$$

Since

$$\prod_{p \text{ prime}} \left(1 - \frac{1}{p^2}\right) = \frac{6}{\pi^2},$$

we have

$$g(n) > \frac{n^2}{2\pi^2} + \sum_{d|n} \mu(d) \epsilon_{n/d}.$$

Now since the number of divisors of  $n$  is less than  $2\sqrt{n}$ , we obtain the following lemma:

**Lemma 5.2.** *We have*

$$\frac{n^2}{2\pi^2} - \frac{2}{3}\sqrt{n} < g(n).$$

The next lemma is the principal step in our proof. It gives information about the maximal overgroups in  $G$  of an element of the form  $\text{diag}(\Gamma_a^{\alpha-2}, \Gamma_b, \Gamma_c)$ , where the degrees  $a$ ,  $b$  and  $c$  are coprime. The proof relies on knowledge of the subgroups of  $\text{GL}_n(q)$  whose order is divisible by a primitive prime divisor of  $q^d - 1$ , where  $d > n/3$ . An account of such subgroups has been given in the doctoral dissertation of Joseph DiMuro [2007]; this work extends the classification of [Guralnick et al. 1999], which deals with the case  $d > n/2$ .<sup>1</sup>

**Lemma 5.3.** *Let  $v(n) \geq 3$ , and let  $n \geq 98$ . For  $\lambda = (a, b, c) \in P(n)$  with  $a \leq b \leq c$  and with  $a$ ,  $b$  and  $c$  coprime, let*

$$g = g_\lambda = \text{diag}(\Gamma_a^{\alpha-2}, \Gamma_b, \Gamma_c).$$

*Then every maximal overgroup  $M$  of  $g$  in  $G$  is a subspace stabilizer except possibly in the following cases:*

- (i)  $2 \mid n$ ,  $c = n/2$  and  $M \cong G \cap (\text{GL}_{n/2}(q) \wr C_2)$ .

<sup>1</sup>DiMuro's dissertation aims to classify elements of  $\text{GL}_n(q)$  of prime power order that act faithfully and irreducibly on a subspace of dimension  $n/3$  or greater. However, we have been informed by its author that there is at present a gap in the argument concerning those elements whose orders are prime powers but not prime. For our purposes, only the results concerning elements of prime order are required.



- (ii)  $4 \mid n$ ,  $(a, b, c) = (2, (n-2)/2, (n-2)/2)$  and either  $M \cong G \cap (\text{GL}_{n/2}(q) \wr C_2)$  or  $M \cong G \cap (\text{GL}_{n/2}(q) \circ \text{GL}_2(q))$ .

(Here  $\circ$  is used to denote a central product.)

*Proof.* We observe that  $V$  may be decomposed as  $V_a \oplus V_b \oplus V_c$ , where  $V_a, V_b$  and  $V_c$  are  $g$ -invariant subspaces of dimensions  $a, b$  and  $c$ , respectively. The action of  $g$  on each of these summands is irreducible. It follows that  $g$  lies in the stabilizers of proper subspaces of at least four different dimensions, and so  $g$  is covered by the class  $\text{ss}(k)$  for at least four values of  $k$ .

Note that  $c > n/3$  and that  $q^c - 1$  divides the order of  $g$ . Hence, a maximal overgroup  $M$  of  $g$  must belong to one of the classes of groups mentioned in [DiMuro 2007, §1.2]. We observe firstly that owing to our assumption that  $v \geq 3$  and  $n \geq 98$ , the subgroup  $M$  cannot be any of those in [DiMuro 2007, Tables 1.1–1.9]; this immediately rules out several of the Examples listed there. We shall go through the remaining Examples.

*Example 1. Classical examples.* The determinant of  $g$  is a generator of the quotient  $G/\text{SL}_n(q)$ , and so  $M$  cannot contain  $\text{SL}_n(q)$ .

Any element of a symplectic or orthogonal group is similar to its own inverse; an element  $g$  of a unitary group is similar to its conjugate inverse  $g^{-\tau}$ , where  $\tau$  is induced by an involutory field automorphism. (See [Wall 1963, §2.6 or (3.7.2)] for groups in characteristic 2.)

If  $M$  normalizes a symplectic or orthogonal group  $H$ , then  $g^{q-1}$  lies in  $H$  itself, and so  $g^{q-1}$  is similar to its own inverse. Then it is clear that  $\Gamma_c^{q-1}$  is similar to its own inverse (it does not matter here whether  $b = c$ ). But this cannot be the case since  $c > 2$ .

Similarly, if  $M$  normalizes a unitary group  $U$ , then  $g^{q+1}$  lies in  $U$ , and it follows that  $g^{q+1}$  is similar to its conjugate inverse. But then it follows that  $\Gamma_c^{q+1}$  is similar to its conjugate inverse, and it is easy to show that this is not the case.

*Example 3. Imprimitve examples.* Here  $M$  preserves a decomposition  $V = U_1 \oplus \dots \oplus U_t$  for  $t \geq 2$ . Let  $\dim U_i = m$  so that  $n = mt$ . Recall that the  $\langle g \rangle$ -module  $V$  is the direct sum of three irreducible submodules  $V_a, V_b$  and  $V_c$  of dimensions  $a, b$  and  $c$ , respectively. So  $\langle g \rangle$  has at most three orbits on the set of spaces  $U_i$ .

Let  $r$  be the smallest integer such that  $V_c$  is contained in the direct sum of  $r$  of the spaces  $U_i$ . We observe that  $n/3 < c \leq rm$ , and so  $m > n/3r$ . Without loss of generality, we may assume that  $V_c \leq W = U_1 \oplus \dots \oplus U_r$ . It is clear that  $W$  is  $g$ -invariant. Let  $\bar{g}$  be the restriction of  $g$  to  $W$ . Then  $\langle \bar{g} \rangle$  acts transitively on  $\{U_1, \dots, U_r\}$ . Since  $\bar{g}^r$  acts in the same way on each  $U_i$  for  $i \leq r$ , an upper bound for the order of  $\bar{g}$  is  $(q^m - 1)r$ . But since  $m \leq n/r$  and since  $n \geq 98$  by assumption,

we see that  $(q^m - 1)r < q^{n/3} - 1$  if  $r \geq 4$ . Therefore, we must have  $r \leq 3$ .

It follows that  $V_c$  is a simple  $\mathbb{F}_q\langle \bar{g}^r \rangle$ -module. Now since  $\bar{g}^r$  commutes with the projections of  $W$  onto its summands  $U_i$ , we see that at least one of the spaces  $U_i$  contains an  $\bar{g}^r$ -invariant subspace of dimension  $c$ . So  $m > n/3$ , and hence,  $r \neq 3$ .

Suppose that  $r = 2$ . Since  $\bar{g}^r$  has two fixed spaces of dimension  $m$ , we see that  $b = c = m$  and that  $V_b \oplus V_c \leq W$ . If  $W < V$ , then  $W = V_b \oplus V_c$ . Now we see that  $m$  divides each of  $a$  and  $b + c = 2c$ . Since  $a, b$  and  $c$  are coprime, it follows that  $m = 2$ . But this implies that  $n < 6$ , which contradicts the assumption that  $n \geq 98$ . So we may suppose that  $W = V$ . Then it is not hard to show that  $V_a$  has two irreducible summands as a  $\langle \bar{g}^2 \rangle$ -module. But this can occur only when  $a = 2$ , and this accounts for the first of the exceptional cases of the lemma.

Finally, if  $r = 1$ , then  $m \geq c > n/3$ , and so  $t = 2$ . It is easy to see, in this case, that  $c = m = n/2$ , and this accounts for the second exceptional case of the lemma.

*Example 4. Extension field examples.* If  $g$  stabilizes an  $\mathbb{F}_{q^r}$ -structure on  $V$ , then  $g^r$  lies in the image of an embedding of  $\text{GL}_{n/r}(q^r)$  into  $\text{GL}_n(q)$ . Now if this is the case, then it is not hard, by considering the degrees of the eigenvalues of  $g$  over the fields  $\mathbb{F}_q$  and  $\mathbb{F}_{q^r}$ , to show that  $r$  must divide each of  $a, b$  and  $c$ . But this implies that  $r = 1$  since  $a, b$  and  $c$  are coprime.

*Example 5. Tensor product decomposition examples.* Here  $M$  stabilizes a nontrivial tensor product decomposition  $V = V_1 \otimes V_2$ . There is an embedding of the central product  $\text{GL}(V_1) \circ \text{GL}(V_2)$  into  $\text{GL}_n(q)$ , and  $M$  is the intersection of this group with  $G$ . For  $x_1 \in \text{GL}(V_1)$  and  $x_2 \in \text{GL}(V_2)$ , we write  $(x_1, x_2)$  for the corresponding element of  $\text{GL}(V_1) \circ \text{GL}(V_2)$ .

We shall suppose that  $V_1$  and  $V_2$  have dimensions  $n_1$  and  $n_2$ , respectively, with  $n_1 \leq n_2$ . Then since  $c > n/3$ , it is not hard to see that we have  $n_1 = 2$ .

Suppose  $g \in M$ , and let  $g_1 \in \text{GL}(V_1)$  and  $g_2 \in \text{GL}(V_2)$  be such that  $g = (g_1, g_2)$ . Let  $h = g^{q^2-1}$ . Since the order of  $g$  is coprime with  $q$ , we see that the element  $g_1^{q^2-1}$  is the identity on  $V_1$ , and so  $h = (1, h_2)$  for some  $h_2 \in \text{GL}(V_2)$ .

The largest dimension of an irreducible  $\langle h \rangle$ -subspace of  $V$  is  $c$ , and there are at most two such subspaces. We obtain the  $\langle h \rangle$ -subspace decomposition of  $V$  up to isomorphism by taking two copies of each summand of the  $\langle h_2 \rangle$ -subspace decomposition of  $V_2$ . It follows that there must be at least two summands of dimension  $c$  and hence that  $b = c$  and that  $a < b$ . It follows also that the  $a$ -dimensional summand of  $g$  splits into two summands as an  $\mathbb{F}_q\langle h \rangle$ -module. But it is not hard to see that this can occur only if  $a = 2$ , and so we have  $a = 2$  and  $b = c = (n - 2)/2$ . This is the second exceptional case of the lemma.

*Example 6. Subfield examples.* These cannot occur since  $g$  is built up using Singer cycles, which do not preserve any proper subfield structure.

Example 7. *Symplectic type examples.* This class of groups exists only in prime-power dimension and cannot occur in the cases we are considering since we have assumed that  $\nu \geq 3$ .

Example 8(a). *Permutation module examples.* In this case,  $S$  is an alternating group  $A_m$  for some  $m \geq 5$ . Then it is known that the order of an element in  $M$  is at most  $(q - 1) \cdot e^{\vartheta \sqrt{m \log m}}$ , where  $\vartheta = 1.05314$ , by a result of Massias [1984]. Here  $n = m - 1$  or  $m - 2$ . But a routine calculation shows that the inequality  $e^{\vartheta \sqrt{(n+2) \log(n+2)}} < (q^{n/3} - 1)/(q - 1)$  holds for all  $q \geq 2$  and for all  $n \geq 98$ . (This inequality fails when  $q = 2$  and  $n = 97$ .)

Example 11. *Cross-characteristic groups of Lie type.* The examples not yet ruled out are contained in [DiMuro 2007, Table 1.10]. But the order of an element of  $M$  is less than  $n^3$ , which is less than  $q^{n/3} - 1$  for  $n \geq 98$ . □

*Proof of Theorem 1.4.* Define a set  $\Omega$  of classes of  $G$  by

$$\Omega = \{[\Gamma_n^{\alpha+q-1}]\} \cup \{[g_\lambda] \mid \lambda \in P(n)\}.$$

Let  $\mathcal{C}$  be a set of conjugacy classes of subgroups of  $G$  that covers  $\Omega$  of the smallest size such that this is possible. Then clearly  $|\mathcal{C}| \leq \gamma(G)$ . By the theorem of Kantor [1980] mentioned in the proof of Lemma 3.1 above and by Lemma 5.3, we see that  $\mathcal{C}$  must contain a single class of extension field subgroups. If  $n \geq 98$  and  $\nu \geq 3$ , then each remaining element of  $\mathcal{C}$  is either a class of subspace stabilizers or else one of the classes of subgroups mentioned in the exceptional cases of Lemma 3.1. Each subspace stabilizer contains at most  $n/2$  of the elements  $g_\lambda$ , and each of the exceptional classes contains at most  $n/4$ . Now, using Lemma 5.2, we see that

$$\gamma(G) \geq |\mathcal{C}| \geq 1 + \frac{2g(n)}{n} > \frac{n}{\pi^2}$$

as required for the theorem.

To remove the conditions that  $n \geq 98$  and that  $\nu \geq 3$ , it is enough to observe that the lower bound for  $\kappa(G)$  given by Theorem 1.2 is larger than  $n/\pi^2$  in any case where either of these conditions fails. □

### References

[Britnell et al. 2008] 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**:3 (2008), 442–465. MR 2009b:20089 Zbl 1140.05033

[Bubboloni and Lucido 2002] D. Bubboloni and M. S. Lucido, “Coverings of linear groups”, *Comm. Algebra* **30**:5 (2002), 2143–2159. MR 2003h:20088 Zbl 1007.20030

[Bubboloni and Praeger 2011] D. Bubboloni and C. E. Praeger, “Normal coverings of finite symmetric and alternating groups”, *J. Combin. Theory Ser. A* **118**:7 (2011), 2000–2024. MR 2012e:20006 Zbl 1248.20005

- [Bubboloni et al. 2006] D. Bubboloni, M. S. Lucido, and T. Weigel, “Generic 2-coverings of finite groups of Lie type”, *Rend. Sem. Mat. Univ. Padova* **115** (2006), 209–252. MR 2007f:20087 Zbl 1156.20039
- [Bubboloni et al. 2011] D. Bubboloni, M. S. Lucido, and T. Weigel, “2-Coverings of classical groups”, preprint, 2011. arXiv 1102.0660v1
- [Bubboloni et al. 2012] D. Bubboloni, F. Luca, and P. Spiga, “Compositions of  $n$  satisfying some coprimality conditions”, *J. Number Theory* **132**:12 (2012), 2922–2946. MR 2965200 Zbl 1251.05011
- [Bubboloni et al. 2013] D. Bubboloni, C. E. Praeger, and P. Spiga, “Normal coverings and pairwise generation of finite alternating and symmetric groups”, *J. Algebra* **390** (2013), 199–215. MR 3072118
- [Conway et al. 1985] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of finite groups*, Oxford University Press, Eynsham, 1985. MR 88g:20025 Zbl 0568.20001
- [Crestani and Lucchini 2012] E. Crestani and A. Lucchini, “Normal coverings of solvable groups”, *Arch. Math. (Basel)* **98**:1 (2012), 13–18. MR 2012m:20043 Zbl 1255.20027
- [DiMuro 2007] J. DiMuro, *On prime power elements of  $GL_d(q)$  acting irreducibly on large subspaces*, Ph.D. thesis, University of Southern California, 2007, Available at <http://digitalibrary.usc.edu/assetserver/controller/item/etd-DiMuro-20071119.pdf>.
- [Guralnick and Malle 2012] R. Guralnick and G. Malle, “Simple groups admit Beauville structures”, *J. Lond. Math. Soc. (2)* **85**:3 (2012), 694–721. MR 2927804 Zbl 1255.20009
- [Guralnick et al. 1999] R. Guralnick, T. Penttila, C. E. Praeger, and J. Saxl, “Linear groups with orders having certain large prime divisors”, *Proc. London Math. Soc. (3)* **78**:1 (1999), 167–214. MR 99m:20113 Zbl 1041.20035
- [Kantor 1980] W. M. Kantor, “Linear groups containing a Singer cycle”, *J. Algebra* **62**:1 (1980), 232–234. MR 81g:20089 Zbl 0429.20004
- [Lehmer 1955] D. H. Lehmer, “The distribution of totatives”, *Canad. J. Math.* **7** (1955), 347–357. MR 16,998i Zbl 0064.27902
- [Massias 1984] J.-P. Massias, “Majoration explicite de l’ordre maximum d’un élément du groupe symétrique”, *Ann. Fac. Sci. Toulouse Math. (5)* **6**:3-4 (1984), 269–281. MR 87a:11093 Zbl 0574.10043
- [Wall 1963] G. E. Wall, “On the conjugacy classes in the unitary, symplectic and orthogonal groups”, *J. Austral. Math. Soc.* **3** (1963), 1–62. MR 27 #212 Zbl 0122.28102
- [Zsigmondy 1892] K. Zsigmondy, “Zur Theorie der Potenzreste”, *Monatsh. Math. Phys.* **3**:1 (1892), 265–284. MR 1546236 Zbl 24.0176.02

Communicated by David Benson

Received 2012-07-28

Revised 2012-11-01

Accepted 2013-01-14

j.britnell@imperial.ac.uk

*Department of Mathematics, Imperial College London, South Kensington Campus, London SW7 2AZ, United Kingdom*

maroti.attila@renyi.mta.hu

*Hungarian Academy of Sciences,  
Alfréd Rényi Institute of Mathematics,  
Reáltanoda utca 13–15, H-1053, Budapest, Hungary*

# Algebra & Number Theory

msp.org/ant

## EDITORS

### MANAGING EDITOR

Bjorn Poonen  
Massachusetts Institute of Technology  
Cambridge, USA

### EDITORIAL BOARD CHAIR

David Eisenbud  
University of California  
Berkeley, USA

## BOARD OF EDITORS

Georgia Benkart	University of Wisconsin, Madison, USA	Susan Montgomery	University of Southern California, USA
Dave Benson	University of Aberdeen, Scotland	Shigefumi Mori	RIMS, Kyoto University, Japan
Richard E. Borcherds	University of California, Berkeley, USA	Raman Parimala	Emory University, USA
John H. Coates	University of Cambridge, UK	Jonathan Pila	University of Oxford, UK
J-L. Colliot-Thélène	CNRS, Université Paris-Sud, France	Victor Reiner	University of Minnesota, USA
Brian D. Conrad	University of Michigan, USA	Karl Rubin	University of California, Irvine, USA
Hélène Esnault	Freie Universität Berlin, Germany	Peter Sarnak	Princeton University, USA
Hubert Flenner	Ruhr-Universität, Germany	Joseph H. Silverman	Brown University, USA
Edward Frenkel	University of California, Berkeley, USA	Michael Singer	North Carolina State University, USA
Andrew Granville	Université de Montréal, Canada	Vasudevan Srinivas	Tata Inst. of Fund. Research, India
Joseph Gubeladze	San Francisco State University, USA	J. Toby Stafford	University of Michigan, USA
Roger Heath-Brown	Oxford University, UK	Bernd Sturmfels	University of California, Berkeley, USA
Ehud Hrushovski	Hebrew University, Israel	Richard Taylor	Harvard University, USA
Craig Huneke	University of Virginia, USA	Ravi Vakil	Stanford University, USA
Mikhail Kapranov	Yale University, USA	Michel van den Bergh	Hasselt University, Belgium
Yujiro Kawamata	University of Tokyo, Japan	Marie-France Vignéras	Université Paris VII, France
János Kollár	Princeton University, USA	Kei-Ichi Watanabe	Nihon University, Japan
Yuri Manin	Northwestern University, USA	Efim Zelmanov	University of California, San Diego, USA
Barry Mazur	Harvard University, USA	Shou-Wu Zhang	Princeton University, USA
Philippe Michel	École Polytechnique Fédérale de Lausanne		

## PRODUCTION

production@msp.org

Silvio Levy, Scientific Editor

---

See inside back cover or [msp.org/ant](http://msp.org/ant) for submission instructions.


The subscription price for 2013 is US \$200/year for the electronic version, and \$350/year (+\$40, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

---

ANT peer review and production are managed by EditFlow<sup>®</sup> from Mathematical Sciences Publishers.

PUBLISHED BY

 **mathematical sciences publishers**  
nonprofit scientific publishing

<http://msp.org/>

© 2013 Mathematical Sciences Publishers

# Algebra & Number Theory

Volume 7    No. 9    2013

---

Multiplicities associated to graded families of ideals STEVEN DALE CUTKOSKY	2059
Normal coverings of linear groups JOHN R. BRITNELL and ATTILA MARÓTI	2085
Modularity of the concave composition generating function GEORGE E. ANDREWS, ROBERT C. RHOADES and SANDER P. ZWEGERS	2103
Moduli of elliptic curves via twisted stable maps ANDREW NILES	2141
Regular permutation groups of order $mp$ and Hopf Galois structures TIMOTHY KOHL	2203
Further evidence for conjectures in block theory BENJAMIN SAMBALE	2241
Network parametrizations for the Grassmannian KELLI TALASKA and LAUREN WILLIAMS	2275
Chow quotients of toric varieties as moduli of stable log maps QILE CHEN and MATTHEW SATRIANO	2313
Vinberg's representations and arithmetic invariant theory JACK A. THORNE	2331



1937-0652(2013)7:9;1-4