



Mathematisches
Forschungsinstitut
Oberwolfach



Oberwolfach Preprints

OWP 2018 - 22

ALLA DETINKO, DANE FLANNERY AND ALEXANDER HULPKE

Computing Congruence Quotients of Zariski
Dense Subgroups

Mathematisches Forschungsinstitut Oberwolfach gGmbH
Oberwolfach Preprints (OWP) ISSN 1864-7596

Oberwolfach Preprints (OWP)

The MFO publishes a preprint series **Oberwolfach Preprints (OWP)**, ISSN 1864-7596, which mainly contains research results related to a longer stay in Oberwolfach, as a documentation of the research work done at the MFO. In particular, this concerns the Research in Pairs-Programme (RiP) and the Oberwolfach-Leibniz-Fellows (OWLF), but this can also include an Oberwolfach Lecture, for example.

A preprint can have a size from 1 - 200 pages, and the MFO will publish it on its website as well as by hard copy. Every RiP group or Oberwolfach-Leibniz-Fellow may receive on request 30 free hard copies (DIN A4, black and white copy) by surface mail.

The full copyright is left to the authors. With the submission of a manuscript, the authors warrant that they are the creators of the work, including all graphics. The authors grant the MFO a perpetual, non-exclusive right to publish it on the MFO's institutional repository.

In case of interest, please send a **pdf file** of your preprint by email to rip@mfo.de or owlf@mfo.de, respectively. The file should be sent to the MFO within 12 months after your stay as RiP or OWLF at the MFO.

There are no requirements for the format of the preprint, except that the introduction should contain a short appreciation and that the paper size (respectively format) should be DIN A4, "letter" or "article".

On the front page of the hard copies, which contains the logo of the MFO, title and authors, we shall add a running number (20XX - XX). Additionally, each preprint will get a Digital Object Identifier (DOI).

We cordially invite the researchers within the RiP or OWLF programme to make use of this offer and would like to thank you in advance for your cooperation.

Imprint:

Mathematisches Forschungsinstitut Oberwolfach gGmbH (MFO)
Schwarzwaldstrasse 9-11
77709 Oberwolfach-Walke
Germany

Tel +49 7834 979 50
Fax +49 7834 979 55
Email admin@mfo.de
URL www.mfo.de

The Oberwolfach Preprints (OWP, ISSN 1864-7596) are published by the MFO.
Copyright of the content is held by the authors.

DOI 10.14760/OWP-2018-22

COMPUTING CONGRUENCE QUOTIENTS OF ZARISKI DENSE SUBGROUPS

A. S. DETINKO, D. L. FLANNERY, AND A. HULPKE

ABSTRACT. We obtain a computational realization of the strong approximation theorem. That is, we develop algorithms to compute all congruence quotients modulo rational primes of a finitely generated Zariski dense group $H \leq \mathrm{SL}(n, \mathbb{Z})$ for $n \geq 2$. More generally, we are able to compute all congruence quotients of a finitely generated Zariski dense subgroup of $\mathrm{SL}(n, \mathbb{Q})$, $n > 2$.

1. INTRODUCTION

The *strong approximation theorem* (SAT) is a milestone result of linear group theory and its applications [18, Window 9]. It has come to play a similarly important role in computing with linear groups [4].

If H is a finitely generated Zariski dense subgroup of $\mathrm{SL}(n, \mathbb{Z})$, then SAT asserts that H is congruent to $\mathrm{SL}(n, p)$ for all but a finite number of primes $p \in \mathbb{Z}$. Therefore SAT enables us to describe the congruence quotients of H modulo all primes. Moreover, we can describe the congruence quotients of H modulo all positive integers if $n > 2$ (see [4, Section 4.1]).

Finitely generated linear groups are residually finite. So the congruence quotients of H provide important information about H ; especially when H is arithmetic, i.e., of finite index in $\mathrm{SL}(n, \mathbb{Z})$. In this case the set $\Pi(H)$ of all primes p such that $H \not\cong \mathrm{SL}(n, p) \pmod{p}$ is (apart from some exceptions for $p = 2$ and $n \leq 4$) the set of primes dividing the *level* of H , defined to be the level of the unique maximal principal congruence subgroup in H [5, Section 2]. If H is *thin*, i.e., dense but of infinite index in $\mathrm{SL}(n, \mathbb{Z})$, then we consider the *arithmetic closure* $\mathrm{cl}(H)$ of H : the intersection of all arithmetic groups in $\mathrm{SL}(n, \mathbb{Z})$ containing H [5, Section 3]. Note that $\Pi(H) = \Pi(\mathrm{cl}(H))$ determines the level of $\mathrm{cl}(H)$ just as it does when H is arithmetic. The level is a key component of subsequent algorithms for computing with arithmetic subgroups, such as membership testing and orbit-stabilizer algorithms [7].

In [5, Section 3.2] and [4], we developed algorithms to compute $\Pi(H)$ when n is prime or H has a known transvection. This paper presents a complete solution: practical algorithms to compute $\Pi(H)$ for arbitrary finitely generated dense $H \leq \mathrm{SL}(n, \mathbb{Z})$, $n \geq 2$. We also give a characterization of density that allows us to compute $\Pi(H)$ without preliminary testing of density (although this can certainly be done, as in [5, Section 5] and [6]). Without much extra work, we extend our methods to cover finitely generated subgroups of $\mathrm{SL}(n, \mathbb{Q})$.

As in [4], we rely on the classification of maximal subgroups of $\mathrm{SL}(n, p)$. In fact, we follow B. Weisfeiler's proof of the strong approximation theorem [18, Window 9]. In Section 2 we prove results about maximal subgroups of $\mathrm{SL}(n, p)$ that are needed for our main algorithms. In Section 3 we give methods to compute $\Pi(H)$ for dense $H \leq \mathrm{SL}(n, \mathbb{Q})$, and in Section 4 we outline the algorithms. Section 5 demonstrates the practicality of our algorithms.

We fix some basic terms and notation. Let $S = \{g_1, \dots, g_r\}$ be a generating set of $H \leq \mathrm{SL}(n, \mathbb{Q})$. Then R is the ring (localization) $\frac{1}{\mu}\mathbb{Z}$ generated by the entries of the g_i and g_i^{-1} ; here μ is a positive integer. Note that R does not depend on the choice of S . For m coprime to μ , the congruence homomorphism φ_m induced by natural surjection $\mathbb{Z} \rightarrow \mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ maps $\mathrm{SL}(n, R)$ onto $\mathrm{SL}(n, \mathbb{Z}_m)$. Let $\Pi(H)$ be the set of all primes p (not dividing μ) such that $\varphi_p(H) \neq \mathrm{SL}(n, p)$. Overlining will denote the image modulo a specified prime p of an element of R or a matrix or set of matrices over R . In particular, $\bar{H} = \langle \bar{S} \rangle = \varphi_p(H)$. If $\bar{h} \in \bar{H}$ is given as a word $\Pi_i \bar{g}_{j_i}^{e_i}$ in \bar{S} , then the ‘lift’ of \bar{h} is its preimage $h = \Pi_i g_{j_i}^{e_i}$.

Throughout, \mathbb{F} is a field, \mathbb{F}_p is the field of size p , $\mathrm{Mat}(n, \mathbb{F})$ is the \mathbb{F} -algebra of $n \times n$ matrices over \mathbb{F} , and $1_n \in \mathrm{Mat}(n, \mathbb{F})$ is the identity matrix. We write $\langle G \rangle_D$ for the enveloping algebra of $G \leq \mathrm{GL}(n, \mathbb{F})$ over a subring $D \subseteq \mathbb{F}$.

2. MAXIMALITY OF SUBGROUPS IN $\mathrm{SL}(n, p)$

Let $G \leq \mathrm{SL}(n, p)$. We establish conditions to recognize when G is not in any maximal subgroup of $\mathrm{SL}(n, p)$, i.e., when $G = \mathrm{SL}(n, p)$. Our approach, which characterizes maximal subgroups by means of the adjoint representation, is motivated by [18, Window 9, Section 2].

We identify the adjoint module for $\mathrm{SL}(n, \mathbb{F})$ with the \mathbb{F} -space

$$\mathfrak{sl}(n, \mathbb{F}) = \{x \in \mathrm{Mat}(n, \mathbb{F}) \mid \mathrm{trace}(x) = 0\}$$

of dimension $n^2 - 1$ on which $\mathrm{SL}(n, \mathbb{F})$ acts by conjugation. Let $\mathrm{ad} : \mathrm{SL}(n, \mathbb{F}) \rightarrow \mathrm{GL}(n^2 - 1, \mathbb{F})$ be the corresponding linear representation.

The set of maximal subgroups of $\mathrm{SL}(n, p)$ is the union of Aschbacher classes $\mathcal{C}_1, \dots, \mathcal{C}_8, \mathcal{S}$ (see [1] and [18, p. 397]). The classes \mathcal{C}_4 and \mathcal{C}_7 involve tensor products, for which we adopt the following convention. If $H_1 \leq \mathrm{GL}(a, \mathbb{F})$ and $H_2 \leq \mathrm{GL}(b, \mathbb{F})$ then $H_1 \times H_2$ acts on $\mathbb{F}^a \otimes \mathbb{F}^b$. The associated matrix representation of degree ab has $(h_1, h_2) \in H_1 \times H_2$ acting as the matrix Kronecker product $h_1 \dot{\times} h_2$. The group generated by these Kronecker products is denoted $H_1 \otimes H_2$.

Proposition 2.1. *Let G be a proper absolutely irreducible subgroup of $\mathrm{SL}(n, p)$ such that $\mathrm{ad}(G)$ is irreducible. Then G lies in a maximal subgroup in $\mathcal{C}_6 \cup \mathcal{S}$.*

Proof. Since G is absolutely irreducible, it cannot be in a subgroup in \mathcal{C}_1 . Class \mathcal{C}_5 is irrelevant, as we are over a field of prime size. For each of the remaining Aschbacher classes other than \mathcal{C}_6 or \mathcal{S} , we identify a proper submodule T of the adjoint module A for $\mathrm{SL}(n, p)$.

- \mathcal{C}_2 . A maximal subgroup lies in $W = \mathrm{GL}(a, p) \wr S_b$ with $n = ab$. Let $T \leq A$ be the subspace spanned by block matrices with b blocks from $\{1_a, 0_a, -1_a\}$ and zero trace. Clearly T is preserved under conjugation by W and has dimension $b - 1$.
- \mathcal{C}_3 . A maximal subgroup here has a normal subgroup $N \cong \mathrm{SL}(a, p^b)$ with $n = ab$, $1 < a, b < n$. Each ‘entry’ of N is a $b \times b$ submatrix. The set of matrices in the center of N with trace 0 is a proper submodule of A .
- \mathcal{C}_4 . A maximal subgroup L is $\mathrm{SL}(a, p) \otimes \mathrm{SL}(b, p)$ for some $a, b < n$ such that $n = ab$. If $x \in \mathfrak{sl}(a, p)$ and $y = x \dot{\times} 1_b$ then $\mathrm{trace}(y) = 0$ and thus $y \in A$. Let T be the space spanned by all such products. Then L acts on T by the adjoint action of the $\mathrm{SL}(a, p)$ -part of elements on the x -components of such products. Thus $T \leq A$ is invariant under L , so is a proper submodule of A .
- \mathcal{C}_7 . We use an argument similar to the preceding one. Here a maximal subgroup is generated by $\mathrm{Sym}(b)$ and $\mathrm{SL}(a, p) \otimes \dots \otimes \mathrm{SL}(a, p)$ with b factors, where $n = a^b$ and $1 < a, b < n$.

Let T be the subspace of A spanned by all Kronecker products of length b with every factor 1_a except for one, taken from the adjoint module of $\mathrm{SL}(a, p)$. Then T is invariant under action by the maximal subgroup.

\mathcal{C}_8 . A maximal subgroup that stabilizes a form preserves its own adjoint module (see, e.g., [18, p. 398] or [12, Section 1.4.3]), which cannot be A . \square

Remark 2.2. (Cf. [18, p. 392].) Even if $\mathrm{ad}(G)$ is absolutely irreducible, G could still be in a maximal subgroup in \mathcal{C}_6 . For example, $\mathrm{SL}(8, 5)$ contains the maximal subgroup $4 \circ 2^{1+6} \cdot \mathrm{Sp}_6(2) \in \mathcal{C}_6$ which acts absolutely irreducibly on A ; see [3, p. 399].

Theorem 2.3. *There exists a function f , depending only on the degree n , such that $|G| \leq f(n)$ for any proper absolutely irreducible subgroup G of $\mathrm{SL}(n, p)$ such that $\mathrm{ad}(G)$ is irreducible.*

Proof. (Cf. [18, p. 398]). By [3, Section 2.2.6], $L \leq \mathrm{SL}(n, p)$ in \mathcal{C}_6 has order bounded by a function of n only. By Proposition 2.1, then, let $L \in \mathcal{S}$. That is, $L = N_{\mathrm{SL}(n, p)}(K)$ with $K \leq \mathrm{SL}(n, p)$ simple non-abelian and $C_L(K) = \langle 1_n \rangle$. As L is embedded in $\mathrm{Aut}(K)$, a bound on $|K|$ implies a bound on $|L|$.

By the classification of finite simple groups, K can be alternating, or of Lie type, or sporadic. Sporadic groups are of course bounded in order.

If $K \cong \mathrm{Alt}(k)$ then [10, Theorem 5.7A, corrected] shows that $n \geq \frac{2k-6}{3}$; i.e., for fixed n , the permutation degree k and hence $|K|$ is bounded.

Now let $K = Y_l(r^e)$ for a Lie class Y , Lie rank l , and r prime. If $r \neq p$ then [24, Table 1] gives lower bounds for the smallest coprime degree n in which K has a faithful projective representation. These bounds are functions $a(l, r^e)$, independent of p , such that $a(l, r^e) \rightarrow \infty$ as $l \rightarrow \infty$ or $r^e \rightarrow \infty$. Thus, in bounded degree n , only a finite number (up to isomorphism) of groups $Y_l(r^e)$ are candidates for K .

If $r = p$ then [18, p. 398] shows that K and L must be in a proper connected algebraic subgroup, and thus does not act irreducibly on A . \square

Corollary 2.4. *Let $G \leq \mathrm{SL}(n, p)$, and let $f(n)$ be as in Theorem 2.3. If $\mathrm{ad}(G)$ is absolutely irreducible and $|G| > f(n)$ then $G = \mathrm{SL}(n, p)$.*

Proof. Suppose that G is block upper triangular with main diagonal (G_1, G_2) where G_i has degree $n_i > 1$. Then $\mathrm{ad}(G)$ leaves invariant the subspace of the adjoint module consisting of all block upper triangular matrices with main diagonal $(x, 0_{n_2})$, where x has trace 0. \square

Remark 2.5. Theorem 2.3 and Corollary 2.4 remain valid if we let $f(n)$ be a bound on $\exp(G)$, or a bound on the largest order of an element of G .

Using the formulae for the smallest representation degree of alternating groups, and of Lie-type groups in cross-characteristic, it would be possible to give a rough upper estimate of $f(n)$. We do not attempt this. In Section 5.1, we instead use the tables of [3, Chapter 8] to give tight values for $f(n)$ in degrees $n \leq 12$, extending the values in [4, Remark 3.3].

3. REALIZING STRONG APPROXIMATION COMPUTATIONALLY

Let H be a dense subgroup of $\mathrm{SL}(n, R)$, $R = \frac{1}{\mu}\mathbb{Z}$. By Corollary 2.4 and Remark 2.5, if $\mathrm{ad}(\varphi_p(H))$ is absolutely irreducible and $f(n)$ is exceeded by $\varphi_p(H)$, then $\varphi_p(H) = \mathrm{SL}(n, p)$. This result, and a well-known criterion of density, comprise the background for our main algorithm.

Input groups for all the algorithms are finitely generated. Sometimes we will write input as a finite generating set, or as the group itself.

3.1. Preliminaries. We start by giving two auxiliary procedures.

3.1.1. *Bounded order test.* The first auxiliary procedure is a slight generalization of one in our previous work [8, Section 3.5] and [4, Section 2.1].

Lemma 3.1. *If k is a positive integer and $H \leq \mathrm{GL}(n, R)$ is infinite, then $\varphi_p(H)$ has an element of order greater than k for almost all primes p .*

Proof. The proof is the same as in [4, Section 2.1]. \square

Lemma 3.2. *Suppose that $H \leq \mathrm{SL}(n, R)$ and $\varphi_p(H) = \mathrm{SL}(n, p)$ for some prime p . If $n \geq 3$ or $p > 2$ then H is infinite.*

Proof. See [4, Lemma 2.1]; a finite subgroup of $\mathrm{SL}(n, R)$ can be conjugated into $\mathrm{SL}(n, \mathbb{Z})$. \square

The procedure `PrimesForOrder(H, k)` accepts an infinite subgroup $H \leq \mathrm{GL}(n, R)$ and a positive integer k , and returns the finite set of all primes p such that $\varphi_p(H)$ has maximal element order at most k . This output obviously contains all primes p such that $|\varphi_p(H)| \leq k$.

3.1.2. *Testing absolute irreducibility.* For this subsection, we refer to [9, p. 401] and [5, Section 3.2].

Let N be the normal closure $\langle X \rangle^H$ where X is a finite subset of a finitely generated group $H \leq \mathrm{GL}(n, \mathbb{F})$. The procedure `BasisAlgebraClosure(X, S)` computes a basis $\{A_1, \dots, A_m\}$ of $\langle N \rangle_{\mathbb{F}}$, thereby deciding whether N is absolutely irreducible, i.e., whether $m = n^2$.

The procedure `PrimesForAbsIrreducible` from [4, Section 2.2] will operate in the same way for absolutely irreducible $H \leq \mathrm{GL}(n, R)$: it accepts a generating set S of H , and returns the (finite) set of primes p such that $\varphi_p(H)$ is not absolutely irreducible. The first step is to compute a basis of $\langle H \rangle_{\mathbb{Q}}$. By making a small adjustment, we get `PrimesForAbsIrreducible(X, S)`; for absolutely irreducible $N = \langle X \rangle^H$, it returns the primes p such that $\varphi_p(N)$ is not absolutely irreducible.

If $\bar{H} = \varphi_p(H)$ is absolutely irreducible (e.g., $\bar{H} = \mathrm{SL}(n, p)$) and $\{\bar{A}_1, \dots, \bar{A}_{n^2}\}$ is a basis of $\langle \bar{H} \rangle_{\mathbb{F}_p}$, then H is absolutely irreducible and $\{A_1, \dots, A_{n^2}\}$ is a basis of $\langle H \rangle_{\mathbb{Q}}$. Thus, we can simplify `PrimesForAbsIrreducible` by computing a basis of the enveloping algebra over a finite field and then lifting it to a basis of $\langle H \rangle_{\mathbb{Q}}$ (cf. [4, Section 2.2]).

3.2. Density and strong approximation. We now give elementary proofs of some properties of dense groups, including strong approximation (cf. [17], [18, Theorem 9, p. 396], and [4, Corollary 3.10]). Recall the following density criterion.

Proposition 3.3 ([22, p. 22]). *A subgroup H of $\mathrm{SL}(n, \mathbb{C})$ is dense if and only if H is infinite and $\mathrm{ad}(H)$ is absolutely irreducible.*

Now let H be a finitely generated subgroup of $\mathrm{SL}(n, R)$.

Lemma 3.4. *$\varphi_p(\mathrm{ad}(H)) = \mathrm{ad}(\varphi_p(H))$ for all primes p (coprime to μ).*

Corollary 3.5. *If $\mathrm{ad}(H)$ is absolutely irreducible then $\mathrm{ad}(\varphi_p(H))$ is absolutely irreducible for almost all primes p .*

Lemma 3.6. *If $\varphi_p(H) = \mathrm{SL}(n, p)$ then $\mathrm{ad}(H)$ is absolutely irreducible.*

Proof. By Lemma 3.4, $\varphi_p(\mathrm{ad}(H)) = \mathrm{ad}(\mathrm{SL}(n, p))$. Since the latter is absolutely irreducible, its preimage $\mathrm{ad}(H)$ is too. \square

Proposition 3.7. *The following are equivalent.*

- (i) H is dense.
- (ii) H surjects onto $\mathrm{SL}(n, p)$ for almost all primes p .
- (iii) H surjects onto $\mathrm{SL}(n, p)$ for some prime $p > 2$.

Proof. Suppose that (i) holds. Then by Lemma 3.1, Proposition 3.3, and Corollary 3.5, $\mathrm{ad}(\varphi_p(H))$ is absolutely irreducible and $|\varphi_p(H)| > f(n)$ for almost all primes p . By Corollary 2.4, $\varphi_p(H) = \mathrm{SL}(n, p)$ for such p .

Suppose that (iii) holds. By Lemma 3.6, $\mathrm{ad}(H)$ is absolutely irreducible, and by Lemma 3.2, H is infinite. Thus H is dense by Proposition 3.3. \square

4. THE MAIN ALGORITHMS

In this section we combine Sections 2 and 3 to obtain the promised algorithms to compute $\Pi(H)$ for dense groups H . These consist of the main procedure, a variation aimed at improved performance, and an alternative that could be preferable in certain degrees.

Our main procedure, based on Corollary 2.4, follows.

`PrimesNonSurjectiveSL`

Input: a finite generating set of a dense group $H \leq \mathrm{SL}(n, R)$.

Output: $\Pi(H)$.

1. $\mathcal{P} := \text{PrimesForOrder}(H, f(n)) \cup \text{PrimesForAbsIrreducible}(\mathrm{ad}(H))$.
2. Return $\{p \in \mathcal{P} \mid \varphi_p(H) \neq \mathrm{SL}(n, p)\}$.

Step 2 is performed via standard methods for matrix groups over finite fields (available in, e.g., [19]).

Proposition 4.1. `PrimesNonSurjectiveSL` returns $\Pi(H)$ for dense input H .

Proof. Proposition 3.3 implies that both procedures in Step 1 terminate. Then $\varphi_p(H) = \mathrm{SL}(n, p)$ for any $p \notin \mathcal{P}$ by Corollary 2.4 and Lemma 3.4. \square

4.1. Testing irreducibility. Testing absolute irreducibility of $\mathrm{ad}(H)$ for H of degree n entails computation in degree about n^4 , which is comparatively expensive. However, we can avoid this test by Theorem 2.3. That is, we adapt Meataxe ideas [14, 21] to determine all primes modulo which the adjoint representation is merely reducible. For simplicity, the discussion will be restricted to $R = \mathbb{Z}$.

Recall the following special case of Norton's criterion for the natural module V of a matrix algebra \mathcal{A} .

Suppose that $B \in \mathcal{A}$ has rank $\mathrm{rk}(B) = n - 1$. Assume that $v\mathcal{A} = V$ for some nonzero v in the nullspace of B , and $\mathcal{A}w = V^\perp$ and for some nonzero w^\top in the nullspace of B^\top . Then V is irreducible.

Now let $\mathcal{A} \subseteq \mathrm{Mat}(n, \mathbb{Q})$ be a \mathbb{Z} -algebra, and suppose that the following hold.

- (1) We have found $B \in \mathcal{A}$ such that $\mathrm{rk}(B) = n - 1$.
- (2) For a nonzero v in the nullspace of B , the \mathbb{Z} -span $v\mathcal{A}$ contains n linearly independent vectors v_1, \dots, v_n .
- (3) For a nonzero w^\top in the nullspace of B^\top , there are n linearly independent vectors $w_1, \dots, w_n \in \mathcal{A}w$.

Norton's criterion, applied to the above configuration modulo p , shows that $\varphi_p(\mathcal{A})$ is irreducible unless

$$\begin{aligned} & \text{rk}(\varphi_p(B)) < n - 1, \text{ or} \\ & \varphi_p(v_1), \dots, \varphi_p(v_n) \text{ are linearly dependent, or} \\ & \varphi_p(w_1), \dots, \varphi_p(w_n) \text{ are linearly dependent.} \end{aligned}$$

To find (a finite superset of) the set of primes p for which $\varphi_p(\mathcal{A})$ is reducible, we take the union of three sets, namely the prime divisors of $\det(M_1)$, $\det(M_2)$, and $\det(M_3)$, where

$$\begin{aligned} M_1 & \text{ is a full rank } (n-1) \times (n-1) \text{ minor of } B \text{ (modulo other primes, } B \text{ has rank } n-1), \\ M_2 & \text{ is the matrix with rows } v_1, \dots, v_n \text{ (modulo other primes, } v \text{ spans the whole module),} \\ M_3 & \text{ is the matrix with rows } w_1, \dots, w_n. \end{aligned}$$

To make this into a concrete test `PrimesForIrreducible`, let $\mathcal{A} = \langle \text{ad}(H) \rangle_{\mathbb{Z}}$. Take a small number (say, 100) of random \mathbb{Z} -linear combinations $B \in \mathcal{A}$ until a B of rank $n-1$ is detected. Although we do not have a justification that such elements occur with sufficient frequency, they seem to (as observed in [20]); in every experiment so far we found such a B . (Also note that there are irreducible H such that $\langle H \rangle_{\mathbb{Q}}$ does not have an element of rank $n-1$; but if H is absolutely irreducible then such elements always exist.)

We now state a version of `PrimesNonSurjectiveSL` that may have improved performance in many situations (see Section 5).

`PrimesNonSurjectiveSL`, modified.

1. If `PrimesForIrreducible` confirms that $\text{ad}(H)$ is irreducible then

$$\begin{aligned} \mathcal{P} & := \text{PrimesForOrder}(H, f(n)) \cup \text{PrimesForAbsIrreducible}(H) \\ & \quad \cup \text{PrimesForIrreducible}(\text{ad}(H)); \end{aligned}$$

else

$$\mathcal{P} := \text{PrimesForOrder}(H, f(n)) \cup \text{PrimesForAbsIrreducible}(\text{ad}(H)).$$

2. Return $\{p \in \mathcal{P} \mid \varphi_p(H) \neq \text{SL}(n, p)\}$.

Proposition 4.2. *The above modification of `PrimesNonSurjectiveSL` terminates, returning $\Pi(H)$ for input dense H .*

Proof. This follows from Theorem 2.3 and Proposition 4.1. □

Remark 4.3. Suppose that `PrimesForIrreducible` completes, i.e., $\text{ad}(H)$ is confirmed to be irreducible. Then H is dense if it is infinite and absolutely irreducible (cf. the density testing algorithm `IsDenseIR2` of [6]).

4.2. Individual Aschbacher classes. Some Aschbacher classes may not occur in a given degree. For example, the tensor product classes \mathcal{C}_4 and \mathcal{C}_7 are empty in degree 4. Consonant with the approach of [4], we show how to determine the primes p such that $\varphi_p(H)$ lies in a group in $\mathcal{C}_i \notin \{\mathcal{C}_4, \mathcal{C}_7, \mathcal{S}\}$, using tests that do not involve $\text{ad}(H)$. The following is vital.

Lemma 4.4. *Let $H \leq \text{SL}(n, \mathbb{Q})$ be dense. If $N \trianglelefteq H$ is non-scalar then N is dense, thus absolutely irreducible.*

Proof. This follows from Proposition 3.7: since N is non-scalar, $\varphi_p(N)$ is a normal non-scalar subgroup of $\text{SL}(n, p)$ for almost all primes p . □

4.2.1. *Testing imprimitivity.* Suppose that $H \leq \mathrm{GL}(n, \mathbb{F})$ is imprimitive, so $H \leq \mathrm{GL}(a, \mathbb{F}) \wr \mathrm{Sym}(b)$ for some $a, b > 1$ such that $n = ab$. If $\mathrm{Sym}(b)$ has exponent k then $\langle h^k : h \in H \rangle \leq \mathrm{GL}(a, \mathbb{F})^b$ is reducible. Hence we have the following procedure.

`PrimesForPrimitive`

Input: dense $H = \langle S \rangle \leq \mathrm{SL}(n, \mathbb{Q})$.

Output: the set of primes p for which $\varphi_p(H)$ is imprimitive.

1. Select $h \in H$ such that h^e is non-scalar, where $e = \exp(\mathrm{Sym}(n))$.
2. $\mathcal{P} := \text{PrimesForAbsIrreducible}(h^e, S)$.
3. Return all $p \in \mathcal{P}$ such that $\varphi_p(H)$ is imprimitive.

Once more [19] is used in implementing the last step. Lemma 4.4 guarantees termination, with the stated output.

If we happen to know a prime p such that $\varphi_p(H) = \mathrm{SL}(n, p)$, then `PrimesForPrimitive` simplifies in the familiar way (i.e., by computing in a congruence image and then lifting).

`PrimesForPrimitive, modified.`

1. Let p be a prime for which $\varphi_p(H) = \mathrm{SL}(n, p)$.
2. Find n^2 elements $h_i \in H$ such that the $\varphi_p(h_i^k)$ span $\mathrm{Mat}(n, \mathbb{F}_p)$, where $k := \exp(\mathrm{Sym}(n))$.
3. Return all $p \in \text{PrimesForAbsIrreducible}(h_1^k, \dots, h_{n^2}^k)$ such that $\varphi_p(H)$ is imprimitive.

The h_i as required in Step 2 exist by Step 1 and Lemma 4.4.

4.2.2. *Testing for field extensions.* If $G \in \mathcal{C}_3$ then the second derived group $G^{(2)}$ is quasisimple and reducible (see [3, p. 66] and [15, §4.3]). Accordingly, `PrimesForReducibleSecondDerived` selects a non-scalar double commutator g in the dense group H then returns `PrimesForAbsIrreducible(g, S)`. By Lemma 4.4, we get all primes modulo which H is in a group in \mathcal{C}_3 .

If we know a prime p such that $\varphi_p(H) = \mathrm{SL}(n, p)$ then `PrimesForReducibleSecondDerived` can be modified along the lines that we modified `PrimesForPrimitive`. Now we search for double commutators (instead of k th powers) in $\varphi_p(H)$ that span $\mathrm{Mat}(n, \mathbb{F}_p)$; they exist because $\varphi_p(H) = \mathrm{SL}(n, p)$ is perfect (if $n > 2$ or $p > 3$).

4.2.3. *Excluding classes.* For prime n or $n = 4$, the results of Sections 4.2.1 and 4.2.2, together with those of [4], enable us to compute $\Pi(H)$ without recourse to $\mathrm{ad}(H)$. This is done by using the procedures indicated below to rule out individual Aschbacher classes.

\mathcal{C}_1 : `PrimesForAbsIrreducible.`

\mathcal{C}_2 : `PrimesForPrimitive.`

\mathcal{C}_3 : `PrimesForReducibleSecondDerived.`

$\mathcal{C}_6, \mathcal{S}$: `PrimesForOrder.`

\mathcal{C}_8 : `PrimesForSimilarity`, as in [4, Section 2.5].

5. EXPERIMENTS

Our algorithms have been implemented in `GAP`, enhancing previous functionality for computing with dense groups [6]. Below we report on experiments undertaken with our new implementation. One major application is computing all congruence quotients of a finitely generated dense group $H \leq \mathrm{SL}(n, \mathbb{Z})$ from $\Pi(H)$, as explained in [4, Section 4.1].

5.1. Explicit order bounds. As order bound $f(n)$ we take a bound on the largest element order for the absolutely irreducible groups of degree n in $\mathcal{C}_6 \cup \mathcal{S}$ that are irreducible in their adjoint representation. The tables in [3, Section 8] furnish bounds for $n \leq 12$. We construct an example of each such group in $\mathcal{C}_6 \cup \mathcal{S}$, using the MAGMA [2] implementation that accompanies [3]. Then we use GAP [11] to calculate conjugacy class representatives and their orders.

This data is compiled in Table 1. For completeness, we give maximal subgroup order, maximal element order, and the least common multiple of exponents. The column ‘Geometric’ lists the number i of each Aschbacher class \mathcal{C}_i that can occur.

We also include, for degrees $n \in \{3, 4, 5, 7, 11\}$, the element order bounds from [4] for *all* groups in $\mathcal{C}_6 \cup \mathcal{S}$. The rows with these bounds have $n\mathcal{S}$ in the Degree column. For $n = 3, 4, 5$ we have omitted the row beginning with n , because the bounds agree.

Degree	Geometric	Group Order	Element order	Exponent lcm
3 \mathcal{S}	1, 2, 3, 6, 8	1080	21	1260
4 \mathcal{S}	1, 2, 3, 6, 8	103680	36	2520
5 \mathcal{S}	1, 2, 3, 6, 8	129600	60	3960
6	1, 2, 3, 4, 8	39191040	60	2520
7	1, 2, 3, 6, 8	115248	56	168
7 \mathcal{S}		115248	84	168
8	1, 2, 3, 4, 6, 8	743178240	120	5040
9	1, 2, 3, 6, 7, 8	37791360	90	360
10	1, 2, 3, 4, 8	4435200	120	9240
11	1, 2, 3, 6, 8	244823040	198	637560
11 \mathcal{S}		244823040	253	637560
12	1, 2, 3, 4, 8	5380145971200	156	360360

TABLE 1. Order bounds in small degrees

5.2. Implementation and experimental results.

5.2.1. Triangle groups. Let $\Delta(3, 3, 4)$ be the triangle group $\langle a, b \mid a^3 = b^3 = (ab)^4 = 1 \rangle$. In [16, Theorem 1.1], a four-dimensional real representation of $\Delta(3, 3, 4)$ is defined by

$$\rho_k(a) = \begin{pmatrix} k(3 - 4k + 4k^2) & -1 - 4k - 8k^2 + 16k^3 - 16k^4 & 0 & 0 \\ 1 - k + k^2 & -1 - 3k + 4k^2 - 4k^3 & 0 & 0 \\ k(1 - 2k + 2k^2) & -3 - 4k - 2k^2 + 8k^3 - 8k^4 & 1 & 0 \\ 2(1 - k + k^2) & -2(1 + 2k - 4k^2 + 4k^3) & 0 & 1 \end{pmatrix},$$

$$\rho_k(b) = \begin{pmatrix} 1 & 0 & -4 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & -1 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Let $H(k) = \langle \rho_k(a), \rho_k(b) \rangle$. If $k \in \mathbb{Z}$ then $H(k) \leq \mathrm{SL}(4, \mathbb{Z})$.

Let $F(k)$ be the image under ρ_k of $\langle [a, b], [a, b^{-1}] \rangle$. Calculations by D. F. Holt (personal communication) using `kbmag` [13] show that the latter is a free subgroup of $\Delta(3, 3, 4)$. All groups $H(k)$ (resp. $F(k)$) are 2-generated, and of the same structure; as k varies we are just changing the size

of matrix entries. Note that the entries of the generators of $F(k)$ have roughly twice the number of digits as those of $H(k)$. Our experiments justify that $H(k)$, $F(k)$ are dense (for $H(k)$ this follows independently from [16]), and non-arithmetic, i.e., thin. As \mathcal{C}_4 and \mathcal{C}_7 do not figure in degree 4, the algorithm from Section 4.2 can be utilized here. This will illustrate the benefit of the improvements in Sections 4.1 and 4.2.

In Table 2, M is the level of $\text{cl}(H)$ and ‘Index’ is $|\text{SL}(4, \mathbb{Z}) : H|$. We remark that computing $\Pi(H)$, M , and indices is not possible with our previous methods [4, 5]. Other columns give runtimes in seconds on a 3.7GHz Xeon E5 (2013 MacPro). Column t_A gives the runtime of PrimesNonSurjectiveSL. Column t_I gives the time of the Meataxe-based algorithm from Section 4.1. Due to the randomized nature of the Meataxe calculations, these timings turned out to be variable. We thus give a timing of ten experiments and list minimum, maximum, and average runtime in the format min–max; average. Column t_B gives runtimes of the algorithm in Section 4.2 (computing $\Pi(H)$ without $\text{ad}(H)$), and the final column t_M is runtime to compute M and Index from $\Pi(H)$.

H	M	Index	t_A	t_I	t_B	t_M
$H(1)$	$2^5 7^2$	$2^{41} 3^3 5^3 7^6 19$	63	7–69; 27	4	31
$H(2)$	$2^3 3 13$	$2^{17} 3^2 5^2 13 \cdot 97 \cdot 101 \cdot 181^2$	54	10–104; 30	7	3331
$H(3)$	$2^5 7 \cdot 199$	$2^{43} 3^6 5^3 7 \cdot 11 \cdot 19 \cdot 13267 \cdot 19801$	62	9–90; 43	7	1314
$H(4)$	$2^3 7 \cdot 607$	$2^{21} 3^5 5^5 7 \cdot 13 \cdot 19 \cdot 101 \cdot 7369 \cdot 9463$	90	22–65; 37	19	9650
$H(5)$	$2^5 5^2 409$	$2^{44} 3^3 5^6 17 \cdot 31 \cdot 55897 \cdot 83641$	73	13–107; 48	11	7256
$H(6)$	$2^3 7 \cdot 31 \cdot 97$	$2^{27} 3^7 5^5 7 \cdot 13 \cdot 19 \cdot 37$ $\cdot 331 \cdot 941 \cdot 3169$	85	14–144; 63	7	1679
$H(10)$	$2^3 5^2 7 \cdot 919$	$2^{26} 3^8 5^8 7^2 13 \cdot 17 \cdot 19^2 31$ $\cdot 37 \cdot 101 \cdot 113 \cdot 163$	93	67–390; 235	14	43468
$F(1)$	$2^5 3^2 7^2$	$2^{53} 3^8 5^4 7^6 19$	77	595–707; 645	3	73
$F(2)$	$2^4 3^2 7 \cdot 13 \cdot 313$	$2^{38} 3^9 5^6 7 \cdot 13 \cdot 17 \cdot 97 \cdot 101 \cdot 181^2$	78	689–831; 750	11	24133
$F(3)$	$2^5 3^2 7 \cdot 29$ $\cdot 37 \cdot 199$	$2^{62} 3^{15} 5^6 7^3 11 \cdot 19 \cdot 67 \cdot 137$ $\cdot 421 \cdot 13267 \cdot 19801$	106	718–851; 769	10	76606
$F(4)$	$2^4 3^3 7 \cdot 59 \cdot 607$	$2^{37} 3^{15} 5^7 7 \cdot 13 \cdot 19 \cdot 29 \cdot 101$ $\cdot 1741 \cdot 7369 \cdot 9463$	102	719–899; 798	19	193796
$F(5)$	$2^5 3^3 5^2 7$ $\cdot 71 \cdot 409$	$2^{66} 3^{15} 5^{10} 7 \cdot 17 \cdot 31 \cdot 2521$ $\cdot 55897 \cdot 83641$	139	700–1010; 881	27	345039

TABLE 2.

After computing M , we can find all congruence quotients of $H(k)$, and hence a set of finite quotients of $\Delta(3, 3, 4)$. We see from the results for $k = 1, 2$ that $\Delta(3, 3, 4)$ has quotients $\text{PSL}(4, p)$ for $p > 2$. On the other hand, a calculation with the GAP operation `GQuotients` shows that $\Delta(3, 3, 4)$ has no quotient isomorphic to $\text{PSL}(4, 2)$. Furthermore, since $\Delta(3, 3, 4)$ has quotients isomorphic to $\text{Alt}(10)$, which cannot be a section of a matrix group of degree 4 over a finite field, $H(k) \leq \text{SL}(n, \mathbb{Z})$ for $k \in \mathbb{Z}$ is thin. The $F(k)$ are thin because they are free.

5.2.2. Other experiments. We used the following constructions of dense groups, including examples that permit tensor decomposition modulo some primes.

- (i) Let $K(a, b, m)$ be the subgroup of $\mathrm{SL}(ab, \mathbb{Z})$ generated by $\mathrm{SL}(a, \mathbb{Z}) \otimes \mathrm{SL}(b, \mathbb{Z})$ and the elementary matrix $mt_{1, a+1}$ (two generators per factor of the Kronecker product).
- (ii) For distinct monic polynomials $p(x), q(x) \in \mathbb{Z}[x]$ of equal degree n , let $C(p, q)$ be the subgroup of $\mathrm{SL}(n, \mathbb{Z})$ generated by the companion matrices C_p and C_q for $p(x)$ and $q(x)$.

Regarding density of the $K(a, b, m)$, cf. [4, Lemma 3.15]. By [22, Theorem 1.5], $C(p, q)$ is dense if it is nonabelian, C_q has infinite order, and $p(x)$ is irreducible with Galois group $\mathrm{Sym}(n)$.

The runtimes in Table 3 have the same interpretation as in Table 2. For some of the larger groups, the direct test for absolute irreducibility of the adjoint module did not complete for several hours. In that event, the column entry is blank. Similarly, we did not try to compute the level (of the arithmetic closure) for some of the larger groups, as the calculation would have taken too long. Indices are not listed for space reasons.

Group	Degree	Primes	M	t_A	t_I	t_M
$K(2, 2, 275)$	4	5, 11	$5^2 11$	101	1–3; 1	43
$K(2, 3, 441)$	6	3, 7	$3^3 7^2$	37951	4–47; 17	1488
$K(3, 2, 8959)$	6	17, 31	$17^2 31$	39873	8–43; 28	49342
$K(2, 4, 100)$	8	2, 5			17–96; 53	
$K(3, 3, 11979)$	9	3, 11			81–246; 180	
$C(x^4 - x + 1, x^4 + 5x^3 - x^2 + 1)$	4	11, 61	11·61	58	3–26; 8	19999
$C(x^6 + 2x^4 + x + 1, x^6 - x^2 + 1)$	6	7, 23			12–305; 73	
$C(x^8 + x + 1, x^8 - x + 1)$	8	2	2^2		52–368; 150	158

TABLE 3.

5.2.3. *Performance observations.* The runtime to find $\Pi(H)$ is roughly proportional to the magnitudes of its elements. In fact, runtime is dominated by tests to ensure that no prime p returned is a false positive, i.e., that the p -congruence image really is a proper subgroup of $\mathrm{SL}(n, p)$.

The timings show that the method of Section 4.2 is clearly superior to the default, with the Meataxe-based algorithm performing better unless matrix entries become very large. This pattern becomes more pronounced in larger degrees.

Acknowledgments. We are grateful to Mathematisches Forschungsinstitut Oberwolfach for generous hospitality and facilitation of this research through the programme ‘Research in Pairs’ in 2018. A. S. Detinko was supported by Marie Skłodowska-Curie Individual Fellowship grant H2020 MSCA-IF-2015, no. 704910 (EU Framework Programme for Research and Innovation). A. Hulpke was supported by Simons Foundation Collaboration Grant no. 524518 and National Science Foundation grant DMS-1720146.

REFERENCES

1. M. Aschbacher, *On the maximal subgroups of the finite classical groups*, Invent. Math. **76** (1984), 469–514.
2. W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3–4, 235–265.
3. J. N. Bray, D. F. Holt, and C. M. Roney-Dougal, *The maximal subgroups of the low-dimensional finite classical groups*, London Math. Soc. Lecture Note Ser. **407**, Cambridge University Press, Cambridge, 2013.
4. A. S. Detinko, D. L. Flannery, and A. Hulpke, *Experimenting with Zariski dense subgroups*, Exp. Math., DOI: 10.1080/10586458.2018.1466217

5. A. S. Detinko, D. L. Flannery, and A. Hulpke, *Zariski density and computing in arithmetic groups*, Math. Comp. **87** (2018), no. 310, 967–986.
6. A. S. Detinko, D. L. Flannery, and A. Hulpke, *GAP functionality for Zariski dense groups*, Oberwolfach Preprints (OWP 2017-22); DOI: 10.14760/OWP-2017-22.
7. A. S. Detinko, D. L. Flannery, and A. Hulpke, *Algorithms for arithmetic groups with the congruence subgroup property*, J. Algebra **421** (2015), 234–259.
8. A. S. Detinko, D. L. Flannery, and E. A. O’Brien, *Recognizing finite matrix groups over infinite fields*, J. Symbolic Comput. **50** (2013), 100–109.
9. A. S. Detinko, D. L. Flannery, and E. A. O’Brien, *Algorithms for the Tits alternative and related problems*, J. Algebra **344** (2011), 397–406.
10. J. Dixon and B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics **163**, Springer, New York, 1996.
11. The GAP Group, GAP – Groups, Algorithms, and Programming, <http://www.gap-system.org>
12. R. Goodman and N. R. Wallach, *Symmetry, representations, and invariants*, Graduate Texts in Mathematics **255**, Springer, Dordrecht, 2009.
13. D. F. Holt, The GAP package kbmag, *Knuth-Bendix on Monoids and Automatic Groups*, <https://www.gap-system.org/Packages/kbmag.html>
14. D. F. Holt and S. Rees, *Testing modules for irreducibility*, J. Austral. Math. Soc. (Series A) **57** (1994), 1–16.
15. P. Kleidman and M. Liebeck, *The subgroup structure of the finite classical groups*. London Math. Soc. Lecture Note Ser. **129**, Cambridge Univ. Press, Cambridge, 1990.
16. D. D. Long and M. Thistlethwaite, *Zariski dense surface subgroups in $SL(4, \mathbb{Z})$* , Exp. Math. **27** (2018), no. 1, 82–92.
17. A. Lubotzky, *One for almost all: generation of $SL(n, p)$ by subsets of $SL(n, \mathbb{Z})$* , Contemp. Math. **243**, 125–128, 1999.
18. A. Lubotzky and D. Segal, *Subgroup growth*, Birkhäuser, Basel, 2003.
19. M. Neunhöffer, Á. Seress, et al., The GAP package recog, *A collection of group recognition methods*, <http://gap-packages.github.io/recog/>
20. R. A. Parker, *An integral meataxe*, in: The atlas of finite groups: ten years on (Birmingham, 1995), 215–228, London Math. Soc. Lecture Note Ser. **249**, Cambridge Univ. Press, Cambridge, 1998.
21. R. A. Parker, *The computer calculation of modular characters (the meat-axe)*, in: Computational group theory (Durham, 1982), 267–274, Academic Press, London, 1984.
22. I. Rivin, *Large Galois groups with applications to Zariski density*, <http://arxiv.org/abs/1312.3009v4>
23. P. Sarnak, *Notes on thin matrix groups*, in: Thin groups and superstrong approximation, 343–362, Math. Sci. Res. Inst. Publ. **61**, Cambridge Univ. Press, Cambridge, 2014.
24. G. M. Seitz and A. E. Zalesskii, *On the minimal degrees of projective representations of the finite Chevalley groups. II*, J. Algebra **158** (1993), no. 1, 233–243.

SCHOOL OF COMPUTER SCIENCE, UNIVERSITY OF ST ANDREWS, NORTH HAUGH, ST ANDREWS KY16 9SX, UK
E-mail address: ad271@st-andrews.ac.uk

SCHOOL OF MATHEMATICS, STATISTICS AND APPLIED MATHEMATICS, NATIONAL UNIVERSITY OF IRELAND
 GALWAY, UNIVERSITY ROAD, GALWAY H91TK33, IRELAND
E-mail address: dane.flannery@nuigalway.ie

DEPARTMENT OF MATHEMATICS, COLORADO STATE UNIVERSITY, FORT COLLINS, CO 80523-1874, USA
E-mail address: Alexander.Hulpke@colostate.edu