Mathematisches
Forschungsinstitut
Oberwolfach

Mitglied der Leibniz Gemeinschaft

Oberwolfach Preprints

OWP 2017 - 31

ALLA DETINKO, DANE FLANNERY AND ALEXANDER HULPKE

Experimenting with Zariski Dense Subgroups

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

Oberwolfach Preprints (OWP)

Starting in 2007, the MFO publishes a preprint series which mainly contains research results related to a longer stay in Oberwolfach. 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.

Of course, the full copy right is left to the authors. The MFO only needs the right to publish it on its website *www.mfo.de* as a documentation of the research work done at the MFO, which you are accepting by sending us your file.

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).

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.

DOI 10.14760/OWP-2017-31

EXPERIMENTING WITH ZARISKI DENSE SUBGROUPS

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

ABSTRACT. We give a method to describe all congruence images of a finitely generated Zariski dense group $H \leq \mathrm{SL}(n, \mathbb{Z})$. The method is applied to obtain efficient algorithms for solving this problem in odd prime degree n; if $n = 2$ then we compute all congruence images only modulo primes. We propose a separate method that works for all n as long as H contains a known transvection. The algorithms have been implemented in GAP, enabling computer experiments with important classes of linear groups that have recently emerged.

1. INTRODUCTION

This research is the next stage in our development of a novel domain of computational group theory, dealing with methods and algorithms for computing with linear groups over infinite domains. Practical software for this class of groups is in high demand.

In previous work (e.g., [9]), we obtained a method for computing with finitely generated linear groups H over an infinite field $\mathbb{F}$ based on the residual finiteness of H (an algorithmic realization of 'finite approximation'). Our method implements congruence homomorphism techniques, which reduce groups modulo ideals $\rho \subseteq R$ where R is a subring of $\mathbb{F}$ generated by the entries in elements of H. One maximal ideal is enough to solve fundamental problems such as: testing whether H is finite [9]; deciding whether H is virtually solvable or it contains a free non-abelian subgroup [10] (realizing the Tits alternative computationally); recognizing the group type; and carrying out further investigation of virtually solvable finitely generated linear groups [10].

However, most finitely generated linear groups are not virtually solvable [1], and we cannot expect that one maximal ideal (even if properly selected) would be enough to cover the full range of computational problems that we might wish to solve. Consequently we proposed to avail of the theory of linear algebraic groups; i.e., groups with the Zariski topology (see [32, Chapter 1, § 6]). Each linear group H is a subgroup of an algebraic group $\mathrm{GL}(n, \mathbb{F})$, and the Zariski closure $\mathcal{H}$ of H is the 'smallest' algebraic group containing H. To deal with groups that are not virtually solvable, we restrict attention to (semi)-simple $\mathcal{H}$; and give priority to the most interesting case of algebraic $\mathbb{Q}$-groups with $R = \mathbb{Z}$. Our initial efforts in this direction are discussed in [6], where we consider finitely generated subgroups of $\mathrm{SL}(n, \mathbb{Z})$ that are dense in $\mathrm{SL}(n, \mathbb{R})$. Computing all congruence images of dense groups is possible, affording us valuable insights into the nature of H.

2010 Mathematics Subject Classification: 20-04, 20G15, 20H25, 68W30.

We elucidate. Let H be a finitely generated subgroup of $\mathrm{SL}(n,\mathbb{Z})$, $n \geq 2$. If H is dense then it has the strong approximation property: H surjects onto $\mathrm{SL}(n,p)$ for almost all primes p [22, p. 391]. This fact makes computing all congruence images feasible. Another computational benefit comes from the congruence subgroup property, which implies that each *arithmetic* (i.e., finite index) subgroup of $\mathrm{SL}(n,\mathbb{Z})$ ($n > 2$) contains a *principal congruence subgroup of level* m, i.e., the kernel $\Gamma_{n,m}$ of the homomorphism $\varphi_m : \mathrm{SL}(n,\mathbb{Z}) \to \mathrm{SL}(n,\mathbb{Z}_m)$, $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$. In that event H contains a unique maximal principal congruence subgroup $\Gamma_{n,M}$, and we call its level $M := M(H)$ the *level* of H.

Arithmetic subgroups are dense, but a dense group $H \leq \mathrm{SL}(n,\mathbb{Z})$ can have infinite index in $\mathrm{SL}(n,\mathbb{Z})$ (be a so-called *thin* matrix group, pace [27]). A thin group H is contained in a unique 'minimal' arithmetic subgroup $\mathrm{cl}(H)$ of $\mathrm{SL}(n,\mathbb{Z})$: the *arithmetic closure* of H, which (for $n > 2$) is the intersection of all arithmetic subgroups of $\mathrm{SL}(n,\mathbb{Z})$ containing H [6, Section 3]. The level of H is defined to be the level of $\mathrm{cl}(H)$, and is again denoted $M(H)$. Our computational machinery for arithmetic subgroups can then be deployed on thin groups. For once we know the level M of $H \leq \mathrm{SL}(n,\mathbb{Z})$, we can reduce computing to the context of $\mathrm{GL}(n,\mathbb{Z}_m)$. We have used this strategy to great effect, solving problems for arithmetic subgroups such as membership testing and the orbit-stabilizer problem (see [5]). As shown in [6, Section 2], if H is dense then the set of prime divisors of $M(H)$ is exactly the set $\Pi(H)$ of primes p for which H does not surject onto $\mathrm{SL}(n,p)$ modulo p (leaving aside a tiny number of exceptions for $n \leq 4$). Furthermore, knowing the prime divisors of M we can apply algorithms for matrix groups over $\mathbb{Z}_m$ to compute the largest powers of p^a of p dividing M and thereafter find M exactly.

Clearly, our entire computational apparatus for dense subgroups is based on the ability to compute $\Pi(H)$—our computational realization of the strong approximation theorem. An early version of this appears in [6, Section 3], where we devised an effective method to compute $\Pi(H)$ if n is odd and a transvection (a unipotent element t such that $t - 1_n$ has matrix rank 1) in H is known.

The aim of the present work is twofold. First, in Section 2 we establish an approach to computing $\Pi(H)$ for dense $H \leq \mathrm{SL}(n,\mathbb{Z})$, based on the classification of maximal subgroups of $\mathrm{SL}(n,p)$ as in [2] (see also [22, p. 397]). This is then applied in Section 3 to obtain efficient algorithms to compute $\Pi(H)$ for prime degree n (in which case the types of maximal subgroups of $\mathrm{SL}(n,p)$ are quite restricted). Moreover, for odd prime n, we build on this knowledge describe the congruence images of H modulo all positive integers; for $n = 2$, the congruence images are described modulo all primes. Arbitrary degrees n are treated in [8] (albeit with algorithms that are less efficient for prime n than those herein).

We also give an algorithm to compute $\Pi(H)$ for dense subgroups H of $\mathrm{SL}(2n,\mathbb{Z})$ that contain a known transvection. This completes the task begun in [6, Section 3.2].

Another goal is to perform computer experiments successfully with low-dimensional dense representations of finitely presented groups that have recently been the focus of much attention. We compute Π and M for each group, thus enabling us to describe all of its congruence quotients. Experimental results are presented in Section 4.

We adhere to the following conventions and notation. Congruence images are sometimes indicated by overlining. Pre-images in $H = \langle g_1, \ldots, g_r \rangle \leq \mathrm{SL}(n, \mathbb{Z})$ of elements of $\bar{H}$ written as words in the $\bar{g}_i$ are found by 'lifting': $\bar{g}_{k_i}^{m_i} \cdots \bar{g}_{k_s}^{m_s}$ has pre-image $g_{k_i}^{m_i} \cdots g_{k_s}^{m_s}$. The set of prime divisors of $a \in \mathbb{N}$ is denoted $\pi(a)$. Throughout, $\mathbb{F}$ is a field.

2. Strong approximation and recognition of congruence images

The core idea of our approach to computing $\Pi(H)$ is to find all primes p such that $\varphi_p(H)$ lies in a maximal subgroup of $\mathrm{SL}(n, p)$. Here we provide some general methods for this purpose.

2.1. **Large congruence images.** Let H be infinite. Given a positive integer k, we find all primes p such that $\varphi_p(H)$ has elements of order greater than k (cf. [30, Chapter 4] and [9, Section 3.5]).

Since a periodic linear group is locally finite, the finitely generated group H has an element h of infinite order. We can find h quickly by random selection (see [9, Section 4.2, p. 107], and the discussion in Section 3.3 on randomly selecting elements with specified properties). For $1 \leq i \leq k$, let m_i be the greatest common divisor of the non-zero entries of $h^i - 1_n$, and let $l = \mathrm{lcm}(m_1, \ldots, m_k)$. If $p \notin \pi(l)$ then $|\varphi_p(H)| > k$. For each $p \in \pi(l)$ we check whether $|\varphi_p(H)| < k$. The preceding steps define a procedure `PrimesForOrder` that accepts k and infinite $H \leq \mathrm{SL}(n, \mathbb{Z})$, and returns the (finite) set of primes p such that $|\varphi_p(H)| < k$.

We will also need the following related fact.

Lemma 2.1. *Suppose that $\varphi_p(H) = \mathrm{SL}(n, p)$ for some prime p.*

(i) *If $n \geq 3$ then H is infinite.*
(ii) *If $n = 2$ and $p \geq 3$ then H is infinite.*

Proof. Theorem A of [11] states the largest order of a finite subgroup of $\mathrm{GL}(n, \mathbb{Z})$. In both cases (i) and (ii), this maximal order is less than $|\mathrm{SL}(n, p)|$. □

2.2. **Irreducibility.** This subsection recaps an argument from [6, Section 3.2].

We test whether $H \leq \mathrm{SL}(n, \mathbb{Z})$ is absolutely irreducible by computing a $\mathbb{Q}$-basis $\mathcal{A} = \{A_1, \ldots, A_m\}$ of the enveloping algebra $\langle H \rangle_{\mathbb{Q}}$, where the A_i are words over a generating set of H. If $m = n^2$ then H is absolutely irreducible, and $\varphi_p(H)$ is absolutely irreducible for any prime p not dividing $\Delta := \det[\mathrm{tr}(A_i A_j)]$; here $\mathrm{tr}(x)$ is the trace of a matrix x. Hence we have the following.

Lemma 2.2. *If H is absolutely irreducible then $\varphi_p(H)$ is absolutely irreducible for almost all primes p.*

If $p \mid \Delta$ then $\varphi_p(H)$ might be absolutely irreducible. Testing for this as before is the last step in `PrimesForAbsIrreducible`(H), which returns the set of all primes p such that $\varphi_p(H)$ is not absolutely irreducible.

Note that if $\bar{H}$ is absolutely irreducible (e.g., $\bar{H} = \mathrm{SL}(n, p)$), and $\bar{\mathcal{A}}$ is a basis of $\langle \bar{H} \rangle_{\mathbb{Z}_p}$, then $\mathcal{A}$ is a basis of $\langle H \rangle_{\mathbb{Q}}$.

2.3. **Primitivity.** Next, we give conditions for the congruence image of an (irreducible) primitive subgroup of $\mathrm{SL}(n,\mathbb{Z})$ to be imprimitive. The main concern is prime n; in such degrees an irreducible linear group is either primitive or monomial.

Lemma 2.3. *If $H \leq \mathrm{SL}(n,\mathbb{Z})$ is not solvable-by-finite then $\varphi_p(H)$ is not monomial for almost all primes p.*

Proof. Since H has a free non-abelian subgroup by the Tits alternative, given $k \geq 1$ there exist $g, h \in H$ such that $c := [g^k, h^k] \neq 1_n$. Then $[\bar{g}^k, \bar{h}^k] = \bar{c} \neq 1_n$ for almost all primes p. The lemma follows by taking k to be the exponent of $\mathrm{Sym}(n)$. □

Lemma 2.4. *For prime n, an infinite solvable-by-finite primitive (irreducible) subgroup H of $\mathrm{SL}(n,\mathbb{Z})$ is solvable.*

Proof. Let $K \trianglelefteq H$ be solvable of finite index. Since n is prime, K is scalar or irreducible. If K were scalar then H would be finite. Thus K is irreducible. If K were monomial over $\mathbb{Q}$ then it would be finite once more; so K is primitive. Let A be a maximal abelian normal subgroup of K. Then A is irreducible, and $K = \langle A, g\rangle$ because the field $\langle A\rangle_{\mathbb{Q}}$ is a cyclic extension of $\mathbb{Q}1_n$ of degree n. Let $h \in H$ and $a \in A$; then $hah^{-1} = bg^k$ for some $b \in A$. If $n \mid k$ for all h then H normalizes A and is therefore solvable. Suppose that n and k are coprime for some h. Since $a \mapsto (bg^k)a(bg^k)^{-1}$ is a $\mathbb{Q}$-automorphism of the field $\langle A\rangle_{\mathbb{Q}}$, and $(bg^k)^n$ is fixed by this automorphism, $(bg^k)^n$ is scalar. Hence bg^k has finite order. Suppose that $a \in A$ has infinite order. Of course $hah^{-1} \neq bg^k$, implying that h normalizes $\langle a\rangle$. Since a is irreducible (i.e., $\langle a\rangle$ is irreducible), H normalizes $\langle A\rangle_{\mathbb{Q}}$, and again we conclude that H is solvable. □

Corollary 2.5. *Let n be prime. If $H \leq \mathrm{SL}(n,\mathbb{Z})$ is infinite, non-solvable, and primitive, then $\varphi_p(H)$ is primitive for almost all primes p.*

Given an input group H that is not solvable-by-finite, `PrimesForMonomial` returns the set of primes p such that $\varphi_p(H)$ is monomial. The proof of Lemma 2.3 furnishes a method to compute this finite set. First we find $g, h \in H$ such that $[g^k, h^k] \neq 1_n$, where k is the exponent of $\mathrm{Sym}(n)$. (In our experiments g, h are found by random selection; cf. [1] and see Section 3.3.) Let d be the gcd of the non-zero entries of $[g^k, h^k] - 1_n$. Then $\varphi_p(H)$ is non-monomial if $p \notin \pi(d)$. Finally, we test whether $\varphi_p(H)$ is monomial for each $p \in \pi(d)$, using, e.g., [25].

2.4. **Solvability.** Zassenhaus's theorem [29, p. 136] implies existence of a bound $\delta = \delta(n)$ on the derived length of solvable subgroups of $\mathrm{SL}(n,\mathbb{F})$ that depends only on n, not on $\mathbb{F}$. See, e.g., [29, p. 136] for an estimate of δ due to Dixon.

Let $H \leq \mathrm{SL}(n,\mathbb{Z})$ be non-solvable. We sketch a procedure `PrimesForSolvable`(H,δ) that returns the set of primes p such that $\varphi_p(H)$ is solvable and $\varphi_p(H) \neq \mathrm{SL}(n,p)$. Take a non-trivial iterated commutator in H. As usual, we do this by random selection in H, or by lifting to H from a (non-solvable) congruence image: pick $[\bar{h}_1, \ldots, \bar{h}_{\delta+1}] \neq 1_n$ in $\bar{H}$; then $g = [h_1, \ldots, h_{\delta+1}] \in H$ is as required. Let d be the gcd of the non-zero entries of $g - 1_n$.

Then $\varphi_p(H)$ is non-solvable if $p \notin \pi(d)$. Solvability of $\varphi_p(H)$ for $p \in \pi(d)$ can be tested using [25]. We have proved the following.

Lemma 2.6. *If H is non-solvable then $\varphi_p(H)$ is non-solvable for almost all primes p.*

We get better bounds on derived length for irreducible groups in prime degree.

Lemma 2.7. *Let n be prime. An irreducible solvable subgroup G of $\mathrm{GL}(n,\mathbb{F})$ has derived length $d \leq 6$.*

Proof. A monomial group G is an extension of its subgroup of diagonal matrices by a solvable transitive permutation group of prime degree. Such permutation groups are metacyclic, so $d \leq 3$. Suppose that G is primitive. By [30, Theorem 3.3, p. 42], there exists $E \trianglelefteq G$ of derived length at most 2, such that G/E is isomorphic to a subgroup of $\mathrm{SL}(2,n)$. Since $\delta(\mathrm{SL}(2,n)) \leq 4$ (see, e.g., [29, §21.3]), we get $d \leq 6$ as required. □

Remark 2.8. If $n = 2, 3$ and $G \leq \mathrm{SL}(n,\mathbb{F})$ then $d \leq 4$, $d \leq 5$, respectively.

2.5. **Isometry.** We say that $G \leq \mathrm{GL}(n,\mathbb{F})$ is an *isometry group* if it preserves a non-degenerate bilinear (symmetric or alternating) form. On the other hand, since $\mathrm{SL}(2,\mathbb{F}) = \mathrm{Sp}(2,\mathbb{F})$, we say that G is not an isometry group if G does not preserve a non-degenerate bilinear form for $n > 2$.

Lemma 2.9. *Let $G \leq \mathrm{GL}(n,\mathbb{F})$ be absolutely irreducible. Then G is an isometry group if and only if $\mathrm{tr}(g) = \mathrm{tr}(g^{-1})$ for all $g \in G$.*

Proof. Suppose that $\mathrm{tr}(g) = \mathrm{tr}(g^{-1})$ for all $g \in G$. As their characters are equal, the identity and contragredient representations of G are therefore equivalent; i.e., $g = \Phi(g^{\top})^{-1}\Phi^{-1}$ for some $\Phi \in \mathrm{GL}(n,\mathbb{F})$. Rearranging this equality, we see that G preserves the form with matrix Φ. □

The procedure `PrimesForIsometry` accepts an absolutely irreducible subgroup H of $\mathrm{SL}(n,\mathbb{Z})$ that is not an isometry group. It selects $h \in H$ such that $a := \mathrm{tr}(h) - \mathrm{tr}(h^{-1}) \neq 0$, and (using [25]) returns those $p \in \pi(a)$ such that $\varphi_p(H)$ is an isometry group.

We will need to check not only whether a congruence image of H preserves a form, but whether it lies in the similarity group generated by a full isometry group and all scalars. This is achieved with `PrimesForSimilarity`(H), which selects $h = [h_1, h_2] \in H$ such that $a := \mathrm{tr}(h) - \mathrm{tr}(h^{-1}) \neq 0$. Clearly $\varphi_p(H)$ is in a similarity group only if $p \in \pi(a)$. Hence we have the following.

Lemma 2.10. *Suppose that $H \leq \mathrm{SL}(n,\mathbb{Z})$ is absolutely irreducible and not an isometry group. Then for almost all primes p, $\varphi_p(H)$ does not lie in a similarity group over $\mathbb{Z}_p$.*

3. Algorithms for strong approximation

We proceed to formulate an algorithm that realizes strong approximation in prime degree n. That is, the algorithm computes $\Pi(H)$ for any dense input $H \leq \mathrm{SL}(n,\mathbb{Z})$. We also compute Π for dense subgroups of $\mathrm{SL}(2n,\mathbb{Z})$ containing a transvection.

3.1. **Density in prime degree.** For the entirety of this subsection, n is prime.

By [2] (cf [22, p. 397]), the set $\mathcal{C}$ of maximal subgroups of $\mathrm{SL}(n,p)$ is a union of certain subsets $\mathcal{C}_1,\ldots,\mathcal{C}_9$. For each i, we determine all primes p such that $\varphi_p(H)$ could be in a group in $\mathcal{C}_i$. Hence, we provide criteria for H to surject onto $\mathrm{SL}(n,p)$ for almost all primes p. These conditions turn out to be equivalent to density. They constitute the background of our main algorithm and obviate any need to test density of the input (as in, say, [6, Section 5]).

We start with an auxiliary statement for $\mathcal{C}_9$ (called class $\mathcal{S}$ in [3, Chapter 8]).

Lemma 3.1. *There is a bound in terms of n on the order of subgroups of $\mathrm{SL}(n,p)$ that are contained solely in groups in $\mathcal{C}_9$.*

Proof. Suppose that $U \leq \mathrm{SL}(n,p)$ lies only in $\mathcal{C}_9$ and not in $\mathcal{C}_i$ for $i \neq 9$. The perfect residuum U^∞ (i.e., the last term of the derived series of U) is therefore a simple absolutely irreducible subgroup of $\mathrm{SL}(n,p)$. If we show that the order of U^∞ is bounded, then $U \leq \mathrm{Aut}(U^\infty)$ also has bounded order. Thus, without loss of generality, $U = U^\infty$ from now on.

Prime degree faithful representations of quasisimple groups are classified in [24, Theorem 1.1]. The orders of the groups in classes (10)–(27) of this classification are bounded absolutely (i.e., by a bound not depending on n or p). The orders of groups in classes (2)–(9) are bounded by a function of n.

Class (1) groups are of Lie type in characteristic p in the Steinberg representation [15], whose degree n is the p-part of the group order. For each class of groups of Lie type $\mathcal{G}_m(p)$, this p-part is p^a with $a \leq 1$ for only finitely many values of m. So class (1) is finite for prime n.

Finally we come to the case excluded by [24, Theorem 1.1], namely $U/Z(U) \cong \mathrm{Alt}(m)$ for $m > 18$. As a consequence of [16, 18], there are only finitely many degrees l such that $\mathrm{Sym}(l)$ and thus $\mathrm{Alt}(l)$ has a faithful (projective) representation of degree m. □

The main procedure, `PrimesForDense`(H), combines the subsidiary procedures of Section 2. Its output is the union of

- `PrimesForAbsIrreducible`(H)
- `PrimesForMonomial`(H)
- `PrimesForSolvable`(H,δ), where δ is a bound on the derived length of a solvable linear group of degree n
- `PrimesForSimilarity`(H)
- `PrimesForOrder`(H,k) where k is a bound on element orders for groups of degree n in $\mathcal{C}_6 \cup \mathcal{C}_9$.

Theorem 3.2. *Assuming termination for input H,* `PrimesForDense`(H) *returns* $\Pi(H)$.

Proof. Each prime returned must lie in $\Pi(H)$. Conversely, let p be a prime such that $\varphi_p(H) \neq \mathrm{SL}(n,p)$. Then $\varphi_p(H)$ is in a group in some $\mathcal{C}_i$, $1 \leq i \leq 9$. For each i, we show that (at least) one of the subsidiary procedures returns p.

$\mathcal{C}_1$: here $\varphi_p(H)$ is reducible, so p is returned by `PrimesForAbsIrreducible`(H).

$\mathcal{C}_2$: p is returned by `PrimesForMonomial`(H).

$\mathcal{C}_3$: for prime n, the stabilizers of extension fields are solvable, so p is returned by `PrimesForSolvable`(H, δ).

$\mathcal{C}_4$, $\mathcal{C}_7$: since the degree of a tensor product is the product of the factor degrees, and n is prime, these classes are empty.

$\mathcal{C}_5$ is empty over fields of prime size.

$\mathcal{C}_6$ consists of groups whose structure depends on n but not on p [3, Section 2.2.6]. The number of such groups (and thus the largest order of an element in any one of them) is bounded, and so `PrimesForOrder`(H, k) returns p.

$\mathcal{C}_8$: the groups in this class preserve a form modulo $Z(\mathrm{SL}(n, p))$. Hence the derived group of $\varphi_p(H)$ preserves a form and p is returned by `PrimesForSimilarity`(H).

$\mathcal{C}_9$: by Proposition 3.1, the number of groups in this class is finite. Thus (as with $\mathcal{C}_6$) `PrimesForOrder`(H, k) returns p. □

Remark 3.3. Using GAP and tables in [3, Chapter 8], we can calculate bounds on the order of groups in $\mathcal{C}_6 \cup \mathcal{C}_9$ (and hence bounds on their element orders) for small n. For $n = 2$, 3, 5, 7, 11, these bounds are 10, 21, 60, 84, 253, respectively.

Remark 3.4. `PrimesForDense` simplifies in small degrees. If $n \leq 3$ then the groups in $\mathcal{C}_2$ are solvable, so `PrimesForSolvable` overrides `PrimesForMonomial`. In degree 2, `PrimesForSimilarity` is also redundant.

If `PrimesForDense`(H) terminates then $\Pi(H)$ is finite, i.e., H is dense [26, p. 3650]. Next we prove the converse. This leads to a characterization of density in $\mathrm{SL}(n, \mathbb{Z})$.

Lemma 3.5. *If H is irreducible, not solvable-by-finite, and not an isometry group, then $\Pi(H)$ is finite.*

Proof. Each constituent output set is finite by Lemmas 2.2, 2.3, 2.6, 2.10, and 3.1. □

Lemma 3.6. *If H is infinite, non-solvable, primitive, and not an isometry group, then $\Pi(H)$ is finite.*

Proof. As the previous proof, but relying on Corollary 2.5 instead of Lemma 2.3. □

Lemma 3.7. *Suppose that $\varphi_p(H) = \mathrm{SL}(n, p)$ for some prime p, where $p > 3$ if $n = 2$. Then H is infinite, non-solvable, and primitive. Furthermore, H is not an isometry group.*

Proof. Since $\mathrm{SL}(n, p)$ is absolutely irreducible and non-solvable, the same is true of H. A monomial subgroup of $\mathrm{SL}(n, \mathbb{Z})$ cannot surject onto $\mathrm{SL}(n, p)$ because it has an abelian normal subgroup whose index is too small. The remaining assertion follows from Lemmas 2.1 and 2.9. □

Lemmas 3.6 and 3.7 yield

Corollary 3.8 (Cf. p. 396 of [22] and Proposition 1 of [23])**.** *If $\varphi_q(H) = \mathrm{SL}(n, q)$ for one prime $q > 3$, then $\varphi_p(H) = \mathrm{SL}(n, p)$ for almost all primes p.*

Corollary 3.9. *The following are equivalent.*

(i) H *is dense.*
(ii) H *surjects onto* $\mathrm{SL}(n,p)$ *modulo some prime* p*, where* $p>3$ *if* $n=2$*.*
(iii) H *is infinite, non-solvable, primitive, and not an isometry group.*
(iv) H *is irreducible, not solvable-by-finite, and not an isometry group.*

Remark 3.10. Let $n=2$. Then H is dense if and only if H is not solvable-by-finite; which is equivalent to H being infinite and non-solvable.

To round out the subsection, we give one more set of criteria for density in odd prime degree.

Lemma 3.11. *Let* $n>2$*. If* H *contains an irreducible element and is not solvable-by-finite then* H *is dense.*

Proof. We appeal to Lemma 3.5. Let $h\in H$ be irreducible. Suppose that H preserves a form with (symmetric or skew-symmetric) matrix Φ. Then $x\mapsto \Phi x^{\top}\Phi^{-1}$ defines a $\mathbb{Q}$-automorphism of $\langle h\rangle_{\mathbb{Q}}$ of order 2. But $\langle h\rangle_{\mathbb{Q}}$ is a field extension of odd degree n. Hence H is not an isometry group. □

Corollary 3.12. *For* $n>2$*, a finitely generated subgroup of* $\mathrm{SL}(n,\mathbb{Z})$ *is dense if and only if it contains an irreducible element and is not solvable-by-finite.*

Remark 3.13. Lemma 3.6 allows us to replace 'not solvable-by-finite' in Lemma 3.11 and Corollary 3.12 by 'infinite non-solvable primitive', or by 'infinite non-solvable' if $n=3$ (cf. [19, p. 415], [20, Theorem 2.2]).

3.2. **Algorithms for groups with a transvection.** In [6, Section 3.2] we gave a straightforward procedure `PrimesForDense` to compute $\Pi(H)$ if H is dense in $\mathrm{SL}(2n+1,\mathbb{Z})$ or $\mathrm{Sp}(2n,\mathbb{Z})$ and contains a known transvection. The case $H\leq \mathrm{SL}(2n,\mathbb{Z})$ was left open. Now we close that gap.

Lemma 3.14. *Suppose that* $H\leq \mathrm{SL}(2n,\mathbb{Z})$ *contains a transvection* t*. Then* H *is dense if and only if* $N:=\langle t\rangle^H$ *is absolutely irreducible and* $\mathrm{tr}(h)\neq\mathrm{tr}(h^{-1})$ *for some* h *in* N*.*

Proof. Suppose that H is dense. Then N is absolutely irreducible by [6, Corollary 3.5]. If $\mathrm{tr}(h)=\mathrm{tr}(h^{-1})$ for all $h\in N$, then by Lemma 2.9 there is a form with matrix Φ such that $h\Phi h^{\top}=\Phi$ for all $h\in N$. Since $N\trianglelefteq H$ and N is absolutely irreducible, $h\Phi h^{\top}=\alpha\Phi$ for all $h\in H$ and some $\alpha\in\mathbb{Q}$ (see, e.g., [3, Lemma 1.8.9, p. 41]). This contradicts density of H.

Now suppose that N is absolutely irreducible and $\mathrm{tr}(h)\neq\mathrm{tr}(h^{-1})$ for some $h\in N$. Then $\varphi_p(N)$ is absolutely irreducible and $\varphi_p(\mathrm{tr}(h))\neq\varphi_p(\mathrm{tr}(h^{-1}))$ for almost all primes p. So there are $p>3$ and $g\in\varphi_p(N)$ such that $\varphi_p(N)$ is absolutely irreducible and $\mathrm{tr}(g)\neq\mathrm{tr}(g^{-1})$. Since $\varphi_p(N)$ is generated by transvections, the theorem of [31, p. 1] implies that $\varphi_p(N)=\mathrm{SL}(2n,p)$ or $\mathrm{Sp}(2n,p)$. Since the latter possibility is ruled out by Lemma 2.9, we must have $\varphi_p(H)=\mathrm{SL}(2n,p)$ and so H is dense (see [23, Proposition 1]). □

The procedure `PrimesForDense`(H, t), based on Lemma 3.14, accepts dense $H \leq \mathrm{SL}(2n, \mathbb{Z})$ containing a transvection t, and returns $\Pi(H)$. It combines `PrimesForAbsIrreducible`(N) and `PrimesForIsometry`(N), checking whether $\varphi_p(H) = \mathrm{SL}(2n, p)$ for each p in the union of their outputs. See [6, Section 3] for an algorithm to compute a basis of $\langle N \rangle_{\mathbb{Q}}$ without computing (a full generating set of) the normal closure N. Similarly, the application of `PrimesForIsometry` does not require computing N, and just randomly selects $h \in N$ such that $tr(h) \neq tr(h^{-1})$.

3.3. **General considerations.** We make further comments on the operation of our algorithms.

When selecting (pseudo-)random elements of $\mathrm{SL}(n, \mathbb{Z})$ for some subprocedures, we seek just one element with a nominated property. These will be plentiful in dense subgroups. Hence we do not aim for any semblance of a random distribution, but randomly take words of length 5 in the given generators. If these repeatedly fail to have the desired property then we gradually increment the word length.

At the start of the calculation we also select (e.g., by computing the orders, or invoking composition tree on images of H modulo different primes [25]) a prime $p_0 > 3$ such that $\varphi_{p_0}(H) = \mathrm{SL}(n, p_0)$. The properties of elements that we are seeking may then be maintained modulo p_0. That is, instead of searching in H, we search for an element $\bar{h}$ in $\varphi_{p_0}(H)$ that has the desired properties (over $\mathbb{Z}_{p_0}$) and lift to the pre-image $h \in H$.

Each of the subsidiary procedures for `PrimesForDense`(H) returns a positive integer d divisible by every prime p such that $\varphi_p(H)$ is in the respective class of maximal subgroups of $\mathrm{SL}(n, p)$. However, d can have prime factors not in $\Pi(H)$. Furthermore, these factors might be so large as to make factorization of d impractical, or make the test of the congruence image overly expensive. Thus we do not factor d fully, but only attempt a cheap partial factorization (e.g., by trial division and a Pollard-ρ algorithm). If d does not factorize, or has large prime factors (magnitudes larger than the entries of the input matrices), then we compute another positive integer d' using the same algorithm but with different choices of random elements, and replace d by $\gcd(d, d')$.

4. Experimenting with low-dimensional dense subgroups

In this section we present experimental results obtained from our GAP implementation of the algorithms. We demonstrate the practicality of our software and how it can be used to obtain important information about groups. In particular we describe all congruence images of H, as explained in the next subsection.

4.1. **Computing all congruence images.** Let $H \leq \mathrm{SL}(n, \mathbb{Z})$ be dense. As in [6, Section 2.4.1], define $\tilde{\Pi}(H) = \Pi(H) \cup \{2\}$ if $\varphi_2(H) = \mathrm{SL}(n, 2)$ and $\varphi_4(H) \neq \mathrm{SL}(n, 4)$; whereas $\tilde{\Pi}(H) = \Pi(H)$ otherwise. Note that the disparity between $\tilde{\Pi}(H)$ and $\Pi(H)$ can arise only when $n \leq 4$, and $M(H)$ is even but $2 \notin \Pi(H)$. By [6, Theorem 2.18], $\tilde{\Pi}(H) = \pi(M(H))$. If $n > 2$ then $\varphi_k(H) = \varphi_k(\mathrm{cl}(H))$ for all k; so $\tilde{\Pi}(H) = \tilde{\Pi}(\mathrm{cl}(H))$. We may therefore assume that H is arithmetic, of level M. Let $a = \gcd(k, M)$, so $k = abc$, $\pi(b) \subseteq \pi(a)$, and $\gcd(c, a) = 1$. Then $\varphi_k(H) \cong H/(H \cap \Gamma_k) \cong H\Gamma_k/\Gamma_k$ is a subgroup of

$\Gamma_{ab}/\Gamma_k \times \Gamma_c/\Gamma_k$. It is not difficult to show that $\varphi_k(H)$ splits as a direct product of Γ_{ab}/Γ_k with $Q := ((H\Gamma_k) \cap \Gamma_c)/\Gamma_k$. Since $\Gamma_{ab}/\Gamma_k \cong \mathrm{SL}(n,\mathbb{Z})/\Gamma_c$, this expresses $\varphi_k(H)$ as a direct product of Q with a subgroup isomorphic to $\mathrm{SL}(n,\mathbb{Z}_c)$. Hence the task in describing all congruence images of H boils down to computing with the quotient Q of $\varphi_k(H)$ in $\mathrm{SL}(n,\mathbb{Z}_k)$; in effect, ranging over all divisors of M. If $n = 2$ then the congruence subgroup property does not hold, and we can only handle $k = p$ prime. Note that our actual implementation (see [7]) computes $\tilde{\Pi} = \pi(M)$ rather than $\Pi(H)$ for input dense H.

In some of the examples below we describe the congruence quotient modulo the level M, exhibiting which parts of its structure arise for various prime powers. We give this as an ATLAS-style composition structure [4] (separating composition factors by dots; cf. [3]), marked up to show the prime powers for which each factor first arises. We emphasize that these have been generated 'semiautomatically' using *some* composition series that refines the congruence structure, not necessarily the nicest or best possible. One example from Table 1 is a group of level $3^4 5{\cdot}19$ with quotient structure

$$\underset{3^4}{3^4}.\underset{3^3}{3^3}.\underset{3^2}{3^3}.\underset{5}{5^2}.\underset{}{2.2.2.}\underset{3,5}{3.3.}\underset{19}{L_2(19)}$$

In the standard notation $L_m(q) := \mathrm{PSL}(m,q)$, this has congruence image $L_2(19)$ modulo 19, which is a simple direct factor not interacting with the other primes. The quotient modulo 3 has structure 3.3 (and is almost certainly the group 3^2). The quotient modulo 5 is $5^2.2.2.2.3.3$, forming a subdirect product with the quotient of order 3 in which the full factor 3.3 is glued together. Modulo 9 the group possesses a factor 3^3 (of the possible $3^{3\cdot 3-1} = 3^8$), modulo 27 another factor 3^3, and modulo 81 a factor 3^4. (Since 3^4 is the prime power dividing the level, the quotient modulo 243 would contain a full 3^8.) The structural analysis in [6, Section 2] proves that the exponent for p^{i+1} cannot be smaller than the exponent for p^i. The name indicates all proper prime powers dividing the level. Thus 'empty' factors $\underset{p^a}{\_}$ are possible if the group has no elements on that level.

Experimental results are displayed in Tables 1 and 2 (writing A_m for $\mathrm{Alt}(m)$ and S_m for $\mathrm{Sym}(m)$). We do not state $\Pi(H)$ as this set almost always coincides with $\pi(M)$.

Experiments were performed on a 2013 MacPro with a 3.7 GHz Intel Xeon E5 utilizing up to 8GB of memory. The software can be accessed at `http://www.math.colostate.edu/~hulpke/arithmetic.g`. Some documentation [7] is also available.

4.2. **Low-dimensional dense subgroups.** Our examples in this subsection come from a family of low-dimensional representations of finitely presented groups, as defined in [19, 20, 21]. For each test group H we compute $\Pi(H)$, incidentally justifying density of H. Thereafter we compute $M(H)$, $|\mathrm{SL}(n,\mathbb{Z}) : H|$, and the congruence quotients of H.

4.2.1. Adopting the notation of [19, p. 414], let

$$\Gamma := \langle x, y, z \mid zxz^{-1} = xy, zyz^{-1} = yxy \rangle;$$

this is the fundamental group of the figure-eight knot complement. Let $F = \langle x, y \rangle$. In [19] two families of representations β_T, ρ_k of Γ in $\mathrm{SL}(3,\mathbb{Z})$ were constructed. Section 4 of [6]

reports on experiments with β_T for a range of T and ρ_k for $k = 0, 2, 3, 4, 5$. The groups $\rho_k(\Gamma)$, $\rho_k(F)$ for $k \neq 0, 2, 3, 4, 5$ are of special interest (see [19, Section 5]). However, neither the methods of [19] nor those of [6] facilitate proper study of ρ_k for such k.

Recall that

$$\rho_k(x) = \begin{pmatrix} 1 & -2 & 3 \\ 0 & k & -1-2k \\ 0 & 1 & -2 \end{pmatrix}, \quad \rho_k(y) = \begin{pmatrix} -2-k & -1 & 1 \\ -2-k & -2 & 3 \\ -1 & -1 & 2 \end{pmatrix},$$

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

The results of experiments with $\rho_k(\Gamma)$ and $\rho_k(F)$ are collected in Table 1; here M is the level (which turns out to be the same for both Γ and F), Index_Γ is $|\mathrm{SL}(3,\mathbb{Z}) : \mathrm{cl}(\rho_k(\Gamma))|$, and $\text{Index}_{\Gamma,F}$ is $|\mathrm{cl}(\rho_k(\Gamma)) : \mathrm{cl}(\rho_k(F)|)$. The last column is the congruence image of $\rho_k(F)$ modulo M. For $k = 1$, 6, 10 the groups surject modulo 2 but not modulo 4.

Determination of the relevant primes was instantaneous. The time to calculate level and index increased roughly with the level, from a few seconds for $k = 1$ to about 15 minutes for $k = 20$.

k	M	Index_Γ	$\text{Index}_{\Gamma,F}$	StructureF
1	$2^2 3^4$	$2^{10}3^{15}13$	2^2	$\underset{3^4}{3^4}.\underset{3^3}{3^3}.\underset{2^2}{\_}.\underset{3^2}{3^3}.\underset{3}{3.3}.\underset{2}{L_3(2)}$
6	$2^2 31{\cdot}43$	$2^{10}3^3 7{\cdot}43^2 331{\cdot}631$	$2{\cdot}3{\cdot}5$	$\underset{2^2}{\_}.\underset{31}{31.31.2}.\underset{43}{L_2(43)}.\underset{31}{L_2(31)}.\underset{2}{L_3(2)}$
7	$3^4 5{\cdot}19$	$2^6 3^{17} 5{\cdot}13{\cdot}19^2 31{\cdot}127$	$2^2 3^2$	$\underset{3^4}{3^4}.\underset{3^3}{3^3}.\underset{3^2}{3^3}.\underset{5}{5^2.2.2.2}.\underset{3,5}{3.3}.\underset{19}{L_2(19)}$
10	$2^2 3^4 11{\cdot}37$	$2^{14}3^{16}7^2 13{\cdot}19{\cdot}37^2 67$	$2^2 3^2 5$	$\underset{3^4}{3^4}.\underset{3^3}{3^3}.\underset{2^2}{\_}.\underset{3^2}{3^3}.\underset{11}{11.11.2}.\underset{3}{3}.\underset{3,11}{3}$ $.\underset{37}{L_2(37)}.\underset{11}{L_2(11)}.\underset{2}{L_3(2)}$
15	$229{\cdot}241$	$2^6 3^3 5{\cdot}97{\cdot}181{\cdot}241^2 19441$	$2{\cdot}3{\cdot}19$	$\underset{229}{229.229.2}.\underset{241}{L_2(241)}.\underset{229}{L_2(229)}$
20	$409{\cdot}421$	$2^4 3^3 5{\cdot}7{\cdot}421^2 55897{\cdot}59221$	$2^2 3{\cdot}17$	$\underset{409}{409.409.2}.\underset{421}{L_2(421)}.\underset{409}{L_2(409)}$

TABLE 1.

4.2.2. Next we look at triangle groups $\Delta(p, q, r) = \langle a, b \mid a^p = b^q = (ab)^r = 1\rangle$.

In [20] representations of $\Delta(3, 3, 4)$ in $\mathrm{SL}(3,\mathbb{Z})$ are defined by

$$a \mapsto a_1 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad b \mapsto b_1(t) = \begin{pmatrix} 1 & 2-t+t^2 & 3+t^2 \\ 0 & -2+2t-t^2 & -1+t-t^2 \\ 0 & 3-3t+t^2 & (-1+t)^2 \end{pmatrix}.$$

These representations are faithful for all $t \in \mathbb{R}$, and if $t \in \mathbb{Z}$ then the images are dense and non-conjugate for different t [20, Theorem 1.1]. If $t = 1$ then the group is conjugate to the one constructed by Kac and Vinberg [19, p. 422]. Put $H_1(t) = \langle a_1, b_1(t)\rangle$.

In [20, p. 8], the following faithful dense representations $H_2(t) = \langle a_2(t), b_2 \rangle$ of $\Delta(3,4,4)$ were constructed:

$$a \mapsto a_2(t) = \begin{pmatrix} 1 & 4+3t^2/4 & 3(6-t+t^2)/2 \\ 0 & -(4+t+t^2)/2 & -3-t^2 \\ 0 & (4+2t+t^2)/4 & (2+t+t^2)/2 \end{pmatrix},$$

$$b \mapsto b_2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -1 \\ 0 & 1 & 1 \end{pmatrix}.$$

In [21, p. 13], faithful representations of $\Delta(3,3,4)$ in $\mathrm{SL}(5,\mathbb{Z})$ are defined by

$$a \mapsto a_3(k) = \begin{pmatrix} 1 & 0 & -3-2k-8k^2 & -1+10k+32k^3 & -5-16k^2 \\ 0 & 4(-1+k) & -13-4k & 3+16(1+k)^2 & -4+16k \\ 0 & 1-k+4k^2 & 3-2k+8k^2 & -2(1+3k+16k^3) & 3+16k^2 \\ 0 & k & 2k & 1-2k-8k^2 & 1+4k \\ 0 & 0 & 3k & 3(-1+k-4k^2) & -2 \end{pmatrix},$$

$$b \mapsto b_3(k) = \begin{pmatrix} 0 & 0 & -3-2k-8k^2 & -1+10k+32k^3 & -5-16k^2 \\ 0 & 1 & 3+4k & -13-8k-16k^2 & 4-16k \\ 0 & 0 & -2(1+k+4k^2) & 6k+32k^3 & -3-16k^2 \\ 1 & 0 & -2(1+k) & -1+2k+8k^2 & -1-4k \\ 2k & 0 & 1-2k & -4k & 1 \end{pmatrix}.$$

As k ranges over $\mathbb{Z}$, the $H_3(k) = \langle a_3(k), b_3(k) \rangle$ are dense and pairwise non-conjugate.

It is known that $H_1(t)$, $H_2(t)$, $H_3(k)$ are thin [20, 21]. For each of these groups we computed its level M and the index of its arithmetic closure in $\mathrm{SL}(n,\mathbb{Z})$ for several values of the parameters. See Table 2.

For $t \equiv 1 \pmod 4$, the $H_1(t)$ as far as we tested surject onto $\mathrm{SL}(3,2)$ but not onto $\mathrm{SL}(3,\mathbb{Z}_4)$.

Runtimes for degree 3 groups were consistent with the previous example. In degree 5, identification of primes was again instantaneous, while the calculation of level and index took about 6 minutes for $H_3(0)$ and 20 minutes for $H_3(3)$. So we did not try larger k.

4.2.3. *Random generators.* We constructed subgroups of $\mathrm{SL}(n,\mathbb{Z})$ for $n = 3$ and 5 generated by a pair of pseudo-random matrices (via the GAP command `RandomUnimodularMat`). More than half of the groups so generated surject onto $\mathrm{SL}(n,p)$ modulo all primes p (and also modulo 4). We attempted to verify whether each group is arithmetic by expressing its generators as words in standard generators of $\mathrm{SL}(n,\mathbb{Z})$ and running a coset enumeration with the presentation from [28]. As the enumeration never terminated, we suspect that these groups are not arithmetic (and indeed a random finitely generated subgroup of $\mathrm{SL}(n,\mathbb{Z})$ is likely to be thin [12, 26]).

4.2.4. *Further experimentation.* Comparing congruence images with finite quotients (obtained, e.g., by the low-index algorithm of [14, Section 5.4]) may help to decide whether a dense representation of a finitely presented group is faithful, or justify that a group is thin. For example, low-index calculations with the finitely presented group Γ as in Subsection 4.2.1 expose quotients (such as $\mathrm{Sym}(23)$, $\mathrm{Sym}(29)$, $\mathrm{Alt}(11) \wr C_2$, to name just a few) that cannot be congruence images of any $\rho_k(\Gamma)$, as they do not have representations

of suitably small degree. Thus ρ_k cannot be faithful on Γ if $\rho_k(\Gamma)$ is arithmetic (cf. [19, Question 5.1]). This fact has a clear explanation: F is free and normal in Γ; hence a representation of Γ in $\mathrm{SL}(3,\mathbb{Z})$ is arithmetic precisely when its restriction on F is arithmetic [19, p. 420]; but any virtually free group cannot have a faithful arithmetic representation in $\mathrm{SL}(n,\mathbb{Z})$ for $n > 2$.

To illustrate another potential application of our algorithms, we show that faithful dense representations of the triangle groups $\Delta(3,3,4)$, $\Delta(3,4,4)$ in $\mathrm{SL}(3,\mathbb{Z})$ or $\mathrm{SL}(5,\mathbb{Z})$ are not arithmetic; this includes $H_1(t)$, $H_2(t)$, $H_3(k)$ as in Section 4.2.2 (cf. [20, 21]). Indeed, $\Delta(3,3,4)$ and $\Delta(3,4,4)$ each have a quotient isomorphic to $\mathrm{Alt}(20)$. This is not a congruence quotient of an arithmetic group in $\mathrm{SL}(3,\mathbb{Z})$ or $\mathrm{SL}(5,\mathbb{Z})$, because $\mathrm{Alt}(20)$ does not have a faithful representation in $\mathrm{SL}(3,p)$ or $\mathrm{SL}(5,p)$ for any p.

We also use this example to compare the capability of our algorithm with that of the low-index algorithm. Congruence quotients of $\rho_k(\Gamma)$ (modulo any integer $m > 1$, including m not dividing the level) produced by our algorithms expose quotients of Γ (such as $\mathrm{SL}(n,p)$ for large p) that are infeasible to find through a low-index computation, because these groups do not have a faithful permutation representation of sufficiently small degree. Using a homomorphism search [14, Section 9.1.1], we find that Γ has 34 normal subgroups N such that $\Gamma/N \cong \mathrm{SL}(3,5)$. Applying our algorithm, we identify 80 values of k in the range $1,\ldots,100$, such that $5 \notin \Pi(\rho_k(\Gamma))$. For these k, the kernels of the induced surjections $\Gamma \to \rho_k(\Gamma) \to \mathrm{SL}(3,5)$ expose just 4 of the 34 normal subgroups. This prompts us to conjecture that the ρ_k will not expose all $\mathrm{SL}(n,p)$ quotients of Γ.

Acknowledgments. We thank Mathematisches Forschungsinstitut Oberwolfach for its generous hospitality during a Research in Pairs visit. Our work was further supported by a Marie Skłodowska-Curie Individual Fellowship grant under Horizon 2020 (EU Framework Programme for Research and Innovation), and Simons Foundation Collaboration Grant 244502.

Group	Level	Index	Quotient
$H_1(1)$	$2^2 3 \cdot 5^2 19$	$2^{13}3^3 5^5 13 \cdot 19^3 31 \cdot 127$	$\underset{2^2}{\_}.\underset{5^2}{5^6}.\underset{19}{3}.\underset{5,19}{2.2.3^2}.\underset{3}{2}.\ \underset{3,5}{2^2.3}.\underset{19}{A_6}.\underset{2}{L_3(2)}$
$H_1(2)$	2^3	$2^7 7$	$\underset{2^3}{2^5}.\underset{2^2}{2^5}.\underset{2}{2^2.3}$
$H_1(5)$	$2^3 7 \cdot 19 \cdot 31$	$2^{23}3^6 5^2 7^2 19^2 31^3 127 \cdot 331$	$\underset{2^3}{\_}.\underset{2^2}{\_}.\underset{31}{3}.\underset{19}{19^2.2.2.2}.\ \underset{7,19,\ 31}{3}\ .\underset{31}{A_6}.\underset{7}{L_2(7)}.\underset{2}{L_3(2)}$
$H_1(9)$	$2^2 67$	$2^9 3^2 7^2 11^2 17 \cdot 31 \cdot 67$	$\underset{2^2}{\_}.\underset{67}{67^2.2.2^2.3}.\underset{2}{L_3(2)}$
$H_1(10)$	$2^3 3 \cdot 7$	$2^{16}3^4 7^2 13 \cdot 19$	$\underset{2^3}{2^5}.\underset{2^2}{2^4}.\underset{7}{7.7}.\underset{3,7}{3.3.2}.\underset{2,3,7}{2^2.3}$
$H_1(12)$	$2^3 7 \cdot 31$	$2^{16}3^5 5^2 7^3 19 \cdot 31 \cdot 331$	$\underset{2^3}{2^5}.\underset{2^2}{2^4}.\underset{31}{31.31.2}.\underset{2,31}{2^2}.\ \underset{2,7,31}{3}\ .\underset{7}{L_2(7)}$
$H_1(50)$	$2^3 601$	$2^{14}3^3 5^4 7^2 13 \cdot 43 \cdot 601 \cdot 9277$	$\underset{2^3}{2^5}.\underset{2^2}{2^4}.\underset{601}{601.601}.\underset{2,601}{2.2^2.3}$
$H_1(100)$	$2^3 3 \cdot 19 \cdot 43$	$2^{19}3^9 5 \cdot 7^3 11 \cdot 13 \cdot 19 \cdot 43 \cdot 127 \cdot 631$	$\underset{2^3}{2^5}.\underset{2^2}{2^4}.\underset{43}{43.43}.\underset{19,43}{19.19}.\underset{3,19,43}{3.3.2}.\ \underset{2,3,19,43}{2^2.3}$
$H_2(2)$	$2^2 13$	$2^7 3^2 7 \cdot 61$	$\underset{2^2}{2^2}.\underset{13}{13.13.2.2}.\underset{2,13}{2^2.3}.\underset{13}{L_2(13)}.\ \underset{2,13}{2}$
$H_2(10)$	$2^2 5 \cdot 109$	$2^{10}3^4 5^2 7^2 31 \cdot 571$	$\underset{2^2}{2^2}.\underset{109}{109.109.2.2}.\ \underset{2,109}{2^2}\ .\underset{2}{3}.\underset{109}{L_2(109)}.\underset{5}{A_5}.\ \underset{2,5,109}{2}$
$H_2(12)$	$2^8 3^4 17$	$2^{38}3^{15}7 \cdot 13 \cdot 307$	$\underset{2^8}{2^6}.\underset{2^7}{2^6}.\underset{2^6}{2^5}.\underset{2^5}{2^3}.\underset{2^4}{2^3}.\underset{3^4}{3^4}.\underset{2^3}{2^2}.\underset{3^3}{3^3}.\underset{2^2}{\_}.\underset{3^2}{3^3}.\underset{17}{17^2}.\underset{3,17}{2.3.3.2}.\ \underset{2,3,17}{2^2}\ .\ \underset{2,17}{3}\ .\ \underset{2,3,17}{2}\ .\underset{17}{L_2(17)}$
$H_2(50)$	$2^2 5^2 13 \cdot 193$	$2^{16}3^4 5^7 7^2 31 \cdot 61 \cdot 1783$	$\underset{2^2}{2^2}.\underset{5^2}{5^3}.\underset{193}{193.193}.\underset{13,193}{2}.\underset{2,193}{13.13.2.2}.\ \underset{2}{2^2}\ .\underset{2}{3}.\underset{193}{L_2(193)}.\underset{13}{L_2(13)}.\underset{5}{A_5}.\ \underset{2,5,13,193}{2}$
$H_3(0)$	$2^3 7^3 19^2$	$2^{52}3^{14}5^5 7^{32}19^{21}31 \cdot 127 \cdot 151 \cdot 181 \cdot 911 \cdot 2801$	$\underset{2^3}{2^8}.\underset{7^3}{7^1}\underset{2^2}{8}.\underset{7^2}{2^6}.\underset{19^2}{7^8}.\underset{19}{19^{12}}.\underset{2,19}{19^2.2.2.2.2^6}.\underset{2,7}{3}.\underset{2,7}{L_3(2)}$
$H_3(1)$	$2^6 67^2$	$2^{87}3^6 5^2 7^3 11^4 17^2 31^2 67^{20} \cdot 449 \cdot 761 \cdot 26881$	$\underset{2^6}{2^{21}}.\underset{2^5}{2^{11}}.\underset{2^4}{2^8}.\underset{2^3}{2^5}.\underset{2^2}{2^4}.\underset{67^2}{67^{12}}.\underset{67}{67.67.2}.\underset{2,67}{2^2.3}$
$H_3(2)$	$2^3 13 \cdot 211^2$	$2^{33}3^9 5^6 7^5 13^5 31^2 37 \cdot 53^2 61 \cdot 113 \cdot 197$ $\cdot 211^{20} \cdot 1361 \cdot 30941 \cdot 292661$	$\underset{2^3}{2^{16}}.\underset{2^2}{2^{14}}.\underset{211^2}{211^{12}}.\underset{211}{211^2.2.2.2}.\underset{13,211}{13.13.13.13}.\ \underset{2,13,211}{2^6.3}\ .\underset{13}{L_2(169)}.\underset{2}{L_3(2)}$
$H_3(3)$	$2^6 7 \cdot 11^2 41^2$	$2^{106}3^8 5^{13}7^8 11^{20}19^2 \ \cdot\ 29^2 31 \cdot 41^{20}61$ $\cdot 1723 \cdot 2801 \cdot 3221 \cdot 579281$	$\underset{2^6}{2^{21}}.\underset{2^5}{2^{11}}.\underset{2^4}{2^8}.\underset{2^3}{2^5}.\underset{2^2}{2^4}.\underset{11^2}{11^{12}}.\underset{41^2}{41^{12}}.\underset{41}{41.41}.\underset{11,41}{11.11.2}.$ $\underset{7,11,41}{7.7.7.7.2}.\ \underset{2,7,11,41}{2^2.3}\ .\underset{7}{L_2(7)}.\underset{7}{L_2(7)}$

TABLE 2.

REFERENCES

1. R. Aoun, *Random subgroups of linear groups are free*, Duke Math. J. **160** (2011), no. 1, 117–173.
2. M. Aschbacher, *On the maximal subgroups of the finite classical groups*, Invent. Math. **76** (1984), 469–514.
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. J. H. Conway, S. P. Norton, R. A. Wilson, R. T. Curtis, and R. A. Parker, *Atlas of Finite Groups: Maximal Subgroups and Ordinary Characters for Simple Groups*, Oxford, 1986.
5. A. S. Detinko, D. L. Flannery, and A. Hulpke, *Algorithms for arithmetic groups with the congruence subgroup property*, J. Algebra **421** (2015), 234–259.
6. A. S. Detinko, D. L. Flannery, and A. Hulpke, *Zariski density and computing in arithmetic groups*, Math. Comp., `https://doi.org/10.1090/mcom/3236`
7. A. S. Detinko, D. L. Flannery, and A. Hulpke, *GAP functionality for Zariski dense groups*, Oberwolfach Preprints OWP 2017-22.
8. A. S. Detinko, D. L. Flannery, and A. Hulpke, *Strong approximation and algorithms for computing with dense subgroups*, preprint, 2017.
9. 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.
10. 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
11. W. Feit, *The orders of finite linear groups*, preprint, 1995.
12. E. Fuchs, I. Rivin, *Generic thinness in finitely generated subgroups of* $\mathrm{SL}(n,\mathbb{Z})$, Int. Math. Res. Not. IMRN, `https://doi.org/10.1093/imrn/rnw136`
13. The GAP Group, *GAP – Groups, Algorithms, and Programming*, `http://www.gapsystem.org`
14. D. F. Holt, B. Eick, and E. A. O'Brien, *Handbook of computational group theory*, Discrete Mathematics and its Applications, Chapman & Hall/CRC, Boca Raton, FL, 2005.
15. J. E. Humphreys, *The Steinberg representation*, Bull. AMS (New Series) **16**, Number 2 (1987), 247 – 263.
16. G. D. James, *On the minimal dimensions of irreducible representations of symmetric groups*. Mathematical Proceedings of the Cambridge Philosophical Society **94** (1983), 417–424
17. P. Kleidman and M. Liebeck, *The subgroup structure of the finite classical groups*, Cambridge, 1990
18. A. S. Kleshchev and P. H. Tiep, *Small-dimensional projective representations of symmetric and alternating groups*. Algebra Number Theory **6** (2012), 1773–1816.
19. D. D. Long, A. W. Reid, *Small subgroups of* $\mathrm{SL}(3,\mathbb{Z})$, Exper. Math. **20** (2011), no. 4, 412–425.
20. D. D. Long, A. W. Reid, M. Thistlethwaite, *Zariski dense surface subgroups in* $\mathrm{SL}(3,\mathbb{Z})$, Geometry & Topology **15** (2011) 1-9.
21. D. D. Long, M. Thistlethwaite, *Zariski dense surface subgroups in* $\mathrm{SL}(4,\mathbb{Z})$, J. of Experimental Math., to appear.
22. A. Lubotzky and D. Segal, Subgroup Growth, Birkhäuser, Basel, 2003.
23. A. Lubotzky, *One for almost all: generation of* $\mathrm{SL}(n,p)$ *by subsets of* $\mathrm{SL}(n,\mathbb{Z})$, Contemp. Math. **243**, 125–128, 1999.
24. G. Malle and A. E. Zalesskii, *Prime power degree representations of quasi-simple groups*, Arch. Math. (Basel) **77** (1981), 461–468.

25. M. Neunhöffer, Á. Seress, et al., The GAP package `recog`, *a collection of group recognition methods*, `http://gap-packages.github.io/recog/`
26. I. Rivin, *Zariski density and genericity*, Int. Math. Res. Not. IMRN 2010, no. 19, 3649–3657.
27. P. Sarnak, *Notes on thin matrix groups*, Thin groups and superstrong approximation, 343–362, Math. Sci. Res. Inst. Publ. **61**, Cambridge Univ. Press, Cambridge, 2014.
28. R. Steinberg, *Some consequences of the elementary relations in* SL_n, Finite groups—coming of age (Montreal, Que., 1982), Contemp. Math., vol. 45, Amer. Math. Soc., Providence, RI, 1985, pp. 335–350.
29. D. A. Suprunenko, *Matrix groups*, Transl. Math. Monogr., vol. 45, American Mathematical Society, Providence, RI, 1976.
30. B. A. F. Wehrfritz, *Infinite linear groups*, Springer-Verlag, New York, 1973.
31. A. E. Zalesskii, V. N. Serežkin, *Linear groups generated by transvections*, Izv. Akad. Nauk SSSR Ser. Mat. **40** (1976), no. 1, 26–49 (Russian).
32. A. E. Zalesskii, *Linear groups*, Algebra, IV, Encyclopaedia Math. Sci., **37**, pp. 97–196, Springer, Berlin, 1993.

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`