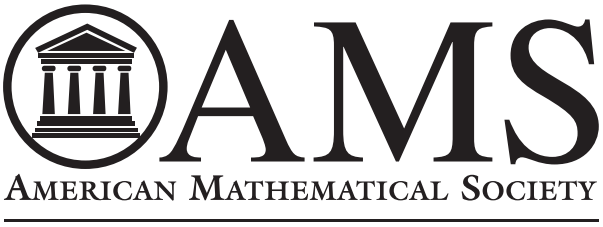

www.ams.org

Alla Detinko, Dane L. Flannery, Alexander Hulpke

Zariski density and computing in arithmetic groups

Mathematics of Computation

DOI: 10.1090/mcom/3236

Accepted Manuscript

ZARISKI DENSITY AND COMPUTING IN ARITHMETIC GROUPS

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

ABSTRACT. For $n > 2$, let Γ_n denote either $\mathrm{SL}(n, \mathbb{Z})$ or $\mathrm{Sp}(n, \mathbb{Z})$. We give a practical algorithm to compute the level of the maximal principal congruence subgroup in an arithmetic group $H \leq \Gamma_n$. This forms the main component of our methods for computing with such arithmetic groups H. More generally, we provide algorithms for computing with Zariski dense groups in Γ_n. We use our GAP implementation of the algorithms to solve problems that have emerged recently for important classes of linear groups.

1. INTRODUCTION

This paper is the next phase in our ongoing project to build up a new area of computational group theory: computing with linear groups given by a finite set of generating matrices over an infinite field. Previously we established a uniform approach for handling such groups in a computer. This is based on the use of congruence homomorphisms, taking advantage of the residual finiteness of finitely generated linear groups: a realisation of the 'method of finite approximation' [13]. We verified decidability, and then obtained efficient algorithms for solving problems such as testing finiteness and virtual solvability. We also implemented a suite of algorithms to perform extensive structural investigation of solvable-by-finite linear groups.

Most finitely generated linear groups, however, are not virtually solvable, and computing with those groups is largely unexplored territory. Obstacles include undecidability of certain algorithmic problems, complexity issues (e.g., growth of matrix entries), and a dearth of methods. In [11], we initiated the development of practical algorithms for arithmetic subgroups of semisimple algebraic groups $\mathcal{G}$ defined over the rational field $\mathbb{Q}$. We were motivated by the pivotal role that these groups play throughout algebra and its applications, and the concomitant demand for practical techniques and software to work with them.

At this stage we restrict attention to $\mathcal{G}$ possessing the *congruence subgroup property*: each arithmetic group $H \leq \mathcal{G}(\mathbb{Z})$ contains the kernel of the congruence homomorphism on $\mathcal{G}(\mathbb{Z})$ modulo some positive integer m, the so-called *principal congruence subgroup (PCS) of level* m. Prominent examples are $\mathcal{G}(\mathbb{Z}) = \mathrm{SL}(n, \mathbb{Z})$

Date: October 26, 2016.

and $\mathrm{Sp}(n,\mathbb{Z})$ for $n > 2$ (see [2]). The congruence subgroup property allows us to reduce much of the computing to the environment of matrix groups over finite rings; but we first need to know (the level of) a PCS in H. In [11] we showed that construction of a PCS in an arithmetic group $H \leq \mathrm{SL}(n,\mathbb{Z})$ is decidable. As a consequence, this proves that other algorithmic questions (e.g., membership testing, orbit-stabilizer problems, analyzing subnormal structure) are decidable, and yields algorithms for their solution.

The current paper gives a practical algorithm to compute a PCS in an arithmetic subgroup $H \leq \Gamma_n = \mathrm{SL}(n,\mathbb{Z})$ or $\mathrm{Sp}(n,\mathbb{Z})$ for degrees $n > 2$. More precisely, we compute the *level* $M = M(H)$ of H, i.e., the level of the unique maximal PCS in H. Knowing M, we can undertake further computation with H (this subsumes all algorithms from [11]).

In contrast to computing with a virtually solvable linear group, computing with an arithmetic group $H \leq \Gamma_n$ entails reduction modulo ideals that may not be maximal. Moreover, we must consider images of H modulo all primes. Fortunately, H and Γ_n are congruent modulo p for almost all primes p. This property holds in a wider class, namely subgroups of Γ_n that are dense in the Zariski topology on $\mathrm{SL}(n,\mathbb{C})$, respectively $\mathrm{Sp}(n,\mathbb{C})$. Density is weaker than arithmeticity, easier to test, and indeed furnishes a preliminary step in arithmeticity testing (see [36] for justification of the significance of this problem). Dense non-arithmetic subgroups are called *thin* matrix groups. If H is dense (either arithmetic or thin), then by the strong approximation theorem H surjects onto $\mathrm{SL}(n,p)$, respectively $\mathrm{Sp}(n,p)$, modulo all but a finite number of primes p [30, p. 391]. We design effective algorithms to compute the set $\Pi(H)$ of these primes for finitely generated $H \leq \Gamma_n$ containing a transvection. As a by-product, we get a simple algorithm to test density of such groups (albeit for odd n only if $\Gamma_n = \mathrm{SL}(n,\mathbb{Z})$). Computing $\Pi(H)$ when H does not have a known transvection will be dealt with in a subsequent paper [12]. Our next major result shows that the algorithm to compute the level of the maximal PCS of an arithmetic subgroup also finds the minimal arithmetic overgroup L of a finitely generated dense subgroup H of Γ_n. Algorithms for the arithmetic group L (e.g., as in [11]) can thereby be used to study H.

When computing with arithmetic groups, the relevant congruence images are over finite rings $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$ (for virtually solvable groups, the images are over finite fields). We prove some essential results about subgroups of $\mathrm{GL}(n,\mathbb{Z}_m)$ in Section 2.3. These underlie Subsection 2.4, wherein we present our algorithm to compute the level M of an arithmetic group in Γ_n. Section 3 is dedicated to density testing and computing $\Pi(H)$ for a finitely generated dense group $H \leq \Gamma_n$. In Section 4, we use our algorithms to solve computational problems that have recently emerged for important classes of groups. The experimental results

demonstrate the efficiency of our algorithms. Finally, in Section 5 we discuss our GAP [15] implementation of density testing algorithms, including those from [34].

2. The level of an arithmetic subgroup

In this section we develop techniques for computing the level of an arithmetic group in Γ_n.

2.1. **Setup.** We adhere to the following notation. Let R be a commutative unital ring. The symplectic group of degree $n = 2s$ over R is

$$\mathrm{Sp}(n, R) = \{x \in \mathrm{GL}(n, R) \mid xJx^\top = J\}$$

where

$$J = \begin{pmatrix} 0_s & 1_s \\ -1_s & 0_s \end{pmatrix}.$$

Notice that $\mathrm{Sp}(2, R) = \mathrm{SL}(2, R)$. Let $t_{ij}(m) = 1_n + me_{ij} \in \mathrm{SL}(n, R)$, where e_{ij} has 1 in position (i, j) and zeros elsewhere. Define

$$E_{n,m} = \langle t_{ij}(m) \,:\, i \neq j,\, 1 \leq i, j \leq n \rangle$$

if $\Gamma_n = \mathrm{SL}(n, R)$, and

$$\begin{aligned} E_{n,m} = \; & \{t_{i,s+j}(m)t_{j,s+i}(m), t_{s+i,j}(m)t_{s+j,i}(m) \mid 1 \leq i < j \leq s\} \\ & \cup \{t_{i,s+i}(m), t_{s+i,i}(m) \mid 1 \leq i \leq s\} \end{aligned}$$

if $\Gamma_n = \mathrm{Sp}(2s, R)$. The $E_{n,m}$ are *elementary subgroups of* Γ_n *of level* m ([11, Section 1.1], [17, pp. 223–224]). For $R = \mathbb{Z}$ or $\mathbb{Z}_r$ we have $E_{n,1} = \mathrm{SL}(n, R)$ if $\Gamma_n = \mathrm{SL}(n, R)$ and $E_{n,1} = \mathrm{Sp}(n, R)$ if $\Gamma_n = \mathrm{Sp}(n, R)$.

We denote by φ_m the reduction modulo m homomorphism on $R = \mathbb{Z}$ or $R = \mathbb{Z}_r$, and its entrywise extension to $\mathrm{GL}(n, R)$. This congruence homomorphism maps Γ_n onto $\mathrm{SL}(n, \mathbb{Z}_m)$ or $\mathrm{Sp}(n, \mathbb{Z}_m)$ respectively. For $\Gamma_n = \mathrm{SL}(n, \mathbb{Z})$ and $n > 2$, the normal closure $E_{n,m}^{\Gamma_n}$ is the principal congruence subgroup (PCS) of level m, i.e., the kernel of φ_m on Γ_n, denoted $\Gamma_{n,m}$ [11, Proposition 1.6]. Similarly, $E_{n,m}^{\Gamma_n}$ is the kernel $\Gamma_{n,m}$ of φ_m on $\Gamma_n = \mathrm{Sp}(n, \mathbb{Z})$ when $n > 2$ [2, Proposition 13.2]. Let $H \leq \Gamma_n$. As usual $\Pi := \Pi(H)$ is the set of primes p such that $\varphi_p(H) \neq \varphi_p(\Gamma_n)$. If $|\Gamma_n : H|$ is finite then H contains some $\Gamma_{n,m}$ [2]. Indeed, H contains a unique maximal PCS; its level is defined to be the level $M = M(H)$ of H.

2.2. **Decidability.** Let $n > 2$. Decision problems for arithmetic groups H in $\Gamma_n = \mathrm{SL}(n, \mathbb{Z})$ were discussed in [11, Section 3.1]. Here we cover $\Gamma_n = \mathrm{Sp}(n, \mathbb{Z})$ as well.

Lemma 2.1. *If* $\Gamma_{n,m} \leq H$ *then* $\varphi_k(H) = \varphi_k(\Gamma_n)$ *for* k *coprime to* m.

Proof. Cf. [11, Remark 1.18]. □

Denote the set of prime divisors of $a \in \mathbb{Z}$ by $\pi(a)$.

Corollary 2.2. *If H has level M and $\Gamma_{n,m} \leq H$ then $\Pi \subseteq \pi(M) \subseteq \pi(m)$.*

Proposition 2.3. *Let $H \leq \Gamma_n$ be arithmetic. Then computing the level of a PCS in H is decidable.*

Proof. We can compute $c = |\Gamma_n : H|$ by the Todd-Coxeter procedure. The core H_{Γ_n} is a normal subgroup of Γ_n contained in H, and $|\Gamma_n : H_{\Gamma_n}|$ divides $m := c!$. So $x^m \in H_{\Gamma_n}$ for all $x \in \Gamma_n$. Thus $E_{n,m} \leq H_{\Gamma_n}$, and $\Gamma_{n,m} \leq H$. □

Corollary 2.4. *If $H \leq \Gamma_n$ is arithmetic then testing membership of $g \in \Gamma_n$ in H is decidable.*

Knowing the level m of any PCS in H, we can determine $|G : H|$ and the level M of H. Therefore, computing M is equivalent to computing $|\Gamma_n : H|$. According to [16, pp. 531–532], an arithmetic subgroup $H \leq \mathcal{G}(\mathbb{Z})$ of an algebraic $\mathbb{Q}$-group $\mathcal{G} \leq \mathrm{GL}(n, \mathbb{C})$ is *given explicitly* if there is an effective way to test membership of elements of $\mathcal{G}(\mathbb{Z})$ in H, and we have an upper bound on $|\mathcal{G}(\mathbb{Z}) : H|$. By Proposition 2.3 and Corollary 2.4, every arithmetic subgroup of $\mathcal{G} = \mathrm{SL}(n, \mathbb{C})$ or $\mathrm{Sp}(n, \mathbb{C})$ is explicitly given. This guarantees decidability of certain algorithmic problems for these groups, as in [16] (see also [11, Section 3.1]).

In practice, we would not compute M or $|\Gamma_n : H|$ as in the proof of Proposition 2.3: the runtime of the Todd-Coxeter procedure may be arbitrarily large. Subsection 2.4 gives a practical method for computing M. This requires extra results, to be presented in the next subsection.

2.3. **Existence of supplements of congruence subgroups over $\mathbb{Z}_m$.** Denote the kernel of the reduction modulo r homomorphism φ_r on $\varphi_m(\Gamma_n) = \mathrm{SL}(n, \mathbb{Z}_m)$ or $\mathrm{Sp}(n, \mathbb{Z}_m)$ by K_r. Let p be a prime. Our main objective in this subsection is to prove the following theorem.

Theorem 2.5. *Let a, $n \geq 2$, and $G = \mathrm{SL}(n, \mathbb{Z}_{p^a})$ or $\mathrm{Sp}(2n, \mathbb{Z}_{p^a})$. Then $K_{p^{a-1}}$ has a proper supplement in G if and only if G is one of*

$$\mathrm{SL}(2, \mathbb{Z}_4), \quad \mathrm{SL}(2, \mathbb{Z}_9), \quad \mathrm{SL}(3, \mathbb{Z}_4), \quad \mathrm{SL}(4, \mathbb{Z}_4). \tag{1}$$

Part of the symplectic group case of Theorem 2.5 is treated in [19].

We need several preparatory lemmas.

Lemma 2.6. *Let $a \geq 2$.*

(i) *The kernel $K_{p^{a-1}}$ of $\varphi_{p^{a-1}} \colon \mathrm{SL}(n, \mathbb{Z}_{p^a}) \to \mathrm{SL}(n, \mathbb{Z}_{p^{a-1}})$ is*

$$\left\{ 1_n + p^{a-1}x \;\middle|\; x \in \mathrm{Mat}(n, \{0, 1, \ldots, p-1\}),\ \mathrm{trace}(x) \equiv 0 \bmod p \right\}.$$

(ii) *Multiplication in $K_{p^{a-1}}$ translates to matrix addition in* $\mathrm{Mat}(n, \mathbb{Z}_p)$:

$$(1_n + p^{a-1}x)(1_n + p^{a-1}y) = 1_n + p^{a-1}z$$

where $z \equiv x + y$ mod p. In particular, $K_{p^{a-1}}$ is an elementary abelian p-group.

Proof. By induction on n, $\det(1_n + p^{a-1}x) = 1 + p^{a-1}\mathrm{tr}(x)$, so (i) follows. The other part is obvious. □

Lemma 2.7. *Let $a \geq 3$ and $G = \mathrm{SL}(n, \mathbb{Z}_{p^a})$ for $n \geq 2$ or $G = \mathrm{Sp}(n, \mathbb{Z}_{p^a})$ for $n \geq 4$. Then $K = K_{p^{a-1}}$ is a central subgroup of $L = K_{p^{a-2}}$ and has no proper supplement in L.*

Proof. Since $2a - 3 \geq a$,

$$\begin{aligned}(1_n + p^{a-1}x)(1_n + p^{a-2}v) &= 1_n + p^{a-1}x + p^{a-2}v \\ &= (1_n + p^{a-2}v)(1_n + p^{a-1}x)\end{aligned}$$

in $\mathrm{Mat}(n, \mathbb{Z}_{p^a})$. Thus $K \leq Z(L)$.

The subgroup K is generated by pth powers of elements of L. If $L = KU$ then $K = L^p = K^pU^p \leq U$; hence $U = L$. □

Lemma 2.8. *Let $G = \mathrm{Sp}(4, \mathbb{Z}_{p^2})$ and $H = \mathrm{Sp}(2, \mathbb{Z}_{p^2})$, p odd. Denote by C, D the kernel of φ_p on G, H, respectively. If there is a proper supplement of C in G then there is a proper supplement of D in H.*

Proof. The assignment

$$\lambda : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & 0 & b & 0 \\ 0 & 1 & 0 & 0 \\ c & 0 & d & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

defines an embedding $\lambda\colon H \to G$. Clearly $\lambda(D) \leq C$. Let N be the subgroup of C whose elements are of the form $1_4 + pr$ where

$$r = \begin{pmatrix} 0 & v_1 & 0 & w_1 \\ -w_3 & v_2 & w_1 & w_2 \\ 0 & v_3 & 0 & w_3 \\ v_3 & v_4 & -v_1 & -v_2 \end{pmatrix}. \tag{2}$$

Then N complements $\lambda(D)$ in C, and is normalized by $\lambda(H)$. Therefore N is a normal subgroup of $W = C\lambda(H) = N\lambda(H)$.

The natural epimorphism $\kappa\colon W \to H$ with kernel N maps C to D. Suppose that S is a supplement of C in G. Then $\kappa(S \cap W)$ supplements D in H; if it does not do so properly then $\kappa(S \cap C) = D$. Assuming this, we prove that $C \leq S$, i.e., $S = G$.

Note that $S \cap C \trianglelefteq G$. As Lemma 2.6 indicates, we may view C as an additive subspace of $\mathrm{Mat}(4, \mathbb{Z}_p)$, replacing $1_4 + px$ by its *relic* x with entries in $\{0, 1, \ldots, p-1\}$. Since $S \cap C$ surjects onto D, it must contain a relic $a = r + e_{31}$ with r as in (2). Let $b_1 = 1_4 + e_{13} \in G$ and $a_1 = a - a^{b_1} = e_{11} + e_{13} - e_{33} + v_3(e_{12} - e_{43}) + w_3(e_{23} + e_{14})$. Then $a_2 = \frac{1}{2}(a_1^{b_1} - a_1) = e_{13} \in S \cap C$.

Since G contains a permutation matrix t for $(1,2)(3,4)$, $e_{24} = e_{13}^t \in S \cap C$. We construct more elements in $S \cap C$. Let $d_1 = 1_4 + e_{31}$, $d_2 = 1_4 + e_{14} + e_{23}$, and $d_3 = 1_4 + e_{32} + e_{41}$. Then

$\frac{1}{2}(a_2^{d_1} - a_2^{d_1^{-1}}) = e_{11} - e_{33}$; conjugating by t gives $e_{22} - e_{44}$,
$\frac{1}{2}(a_2^{d_3} - a_2^{d_3^{-1}}) = e_{12} - e_{43}$; conjugating by t gives $e_{21} - e_{34}$,
$\frac{1}{2}(-a_2^{d_1} + a_2^{d_1^{-1}} + a_2^{d_1 d_2} - a_2^{d_1^{-1} d_2}) = e_{14} + e_{23}$,
$\frac{1}{2}(2a_2 - a_2^{d_1} - a_2^{d_1^{-1}}) = e_{31}$; conjugating by t gives e_{42},
$-a_2 + a_2^{d_1} + a_2^{d_3} - a_2^{d_1 d_3} = e_{32} + e_{41}$.

Modulo p, the relics of C are exactly those matrices x such that Jx is symmetric. Thus C has $\mathbb{Z}_p$-dimension 10. It is readily checked that e_{13}, e_{24}, and the eight other elements of $S \cap C$ just listed are linearly independent. So they comprise a basis of C. Therefore $C \leq S$ as claimed. □

Everything is in place to prove Theorem 2.5.

Proof. If there were a proper supplement of $K_{p^{a-1}}$ in G then there would be a proper supplement of $K_{p^{a-1}}$ in $K_{p^{a-2}}$. So fix $a = 2$ by Lemma 2.7.

We appeal to [3], [41, Theorem 1], and [42]. If G is not one of the groups in (1), or if $G = \mathrm{Sp}(n, \mathbb{Z}_{p^2})$ for $n \geq 6$ but $G \neq \mathrm{Sp}(6, \mathbb{Z}_4)$, then these results imply that K_p lies in the Frattini subgroup of G. Therefore G does not have a proper supplement.

A standard GAP computation reveals that if G is one of the groups in (1) then K_p is properly supplemented.

Since $\mathrm{Sp}(2, R) = \mathrm{SL}(2, R)$, it remains to prove non-supplementation of K_p in $\mathrm{Sp}(6, \mathbb{Z}_4)$ and $\mathrm{Sp}(4, \mathbb{Z}_{p^2})$. The latter follows from Lemma 2.8 for $p > 3$; the remaining parts may be verified by GAP computations. □

2.4. **Computing the level.** In this subsection we develop an algorithm to compute the level M of an arithmetic group $H \leq \Gamma_n$, provided that the set $\pi(M)$ of primes dividing M is known. To fulfil this requirement, we determine the precise relationship between $\pi(M)$ and $\Pi(H)$.

2.4.1. By Corollary 2.2, $\Pi(H) \subseteq \pi(M)$. We will prove conversely that the odd part of $\pi(M)$ coincides with $\Pi(H)$. Furthermore, we show how to decide whether M is even.

Below, Σ stands for either SL or Sp (if $\Sigma = \mathrm{Sp}$ then of course the degree is even).

Lemma 2.9. *Let $n \geq 3$, p be a prime, $a \geq 1$, and $G = \Sigma(n, \mathbb{Z}_{p^a})$. Every proper normal subgroup of G lies in the solvable radical R of G, unless $G = \mathrm{Sp}(4, \mathbb{Z}_{2^a})$, which has a subgroup of index 2 containing $R = \ker \varphi_2$ (the only proper normal subgroup of G not in R).*

Proof. It is easily seen that R is the full preimage in G of the center of $\Sigma(n, p)$ under φ_p. If $G = \mathrm{Sp}(4, \mathbb{Z}_{2^a})$ then $G/R \cong \mathrm{Sym}(6)$. Excluding this case, G/R is simple. By Theorem 2.5 and induction, if $N \not\subseteq R$ is a proper normal subgroup of G then $n = 3$ or 4 and $p = a = 2$. GAP computations confirm that such an N does not exist in $\mathrm{SL}(3, \mathbb{Z}_4)$ or $\mathrm{SL}(4, \mathbb{Z}_4)$. The remainder of the proof is consigned as a straightforward exercise. □

We thank Derek Holt for sharing the next lemma and its proof with us. Recall that a *section* of a group G is a quotient of a subgroup of G.

Lemma 2.10. (D. F. Holt.) *Let S be a finite nonabelian simple group that is not a section of $\mathrm{PSp}(4, 2)$, i.e., S is not isomorphic to $\mathrm{Alt}(5)$ or $\mathrm{Alt}(6)$. Suppose that S is a section of a finite classical group G of degree n in characteristic p.*

Then there exists a finite classical group $\hat{G}$ of degree n in characteristic p, or of degree less than n, such that a subgroup of $\hat{G}/Z(\hat{G})$ is isomorphic to S.

Proof. Suppose that G is a counterexample with n minimal and $|G|$ minimal for this n, with S a quotient of $H \leq G$ and $|H|$ minimal as well. Since S is simple, it must be a section of $G/Z(G)$. We may therefore assume that $Z(G) \leq H$. When $H = G$, the non-solvable group $G/Z(G)$ is either simple (then the lemma holds for $\hat{G} = G$); or, if it is $O_4^+(q)$, a direct product of two copies of $\mathrm{PSL}(2, q)$ (then we can take $\hat{G} = \mathrm{PSL}(2, q)$). So suppose that $H \neq G$. We apply Aschbacher's theorem [1] to H.

If H is in class C_1, C_3, or C_4, then S is a section of a classical group of smaller degree in characteristic p, contrary to the minimality of n. If $H \in \mathrm{C}_2 \cup \mathrm{C}_7$ then either the same is true or S is a section of $\mathrm{Sym}(n)$ with $n \geq 5$. However, $\mathrm{Sym}(n)$ has a faithful representation of degree $n - 1$ (in any characteristic).

If $H \in \mathrm{C}_5 \cup \mathrm{C}_8$ then S is a section of a smaller classical group of degree n in characteristic p, contradicting minimality of $|G|$.

If $H \in \mathrm{C}_6$ then $n = r^k > 2$ is an odd prime power and P is a section of $\mathrm{PSp}(2k, r)$. Unless $k = r = 2$ we have $2k < n$. In the remaining case $k = r = 2$, S would have to be a section of $\mathrm{PSp}(4, 2)$; which was ruled out from the beginning. □

Lemma 2.11. *Let $n \geq 3$ and p, q be distinct primes. If $P = \mathrm{P}\Sigma(n,q)$ is a section of $\Sigma(n,p)$, then $P = \mathrm{PSL}(3,2)$ or $\mathrm{PSp}(4,2)$.*

Proof. Suppose that $P = \mathrm{P}\Sigma(n,q)$ is a section of the classical group $G = \Sigma(n,p)$. By Lemma 2.10, P will be isomorphic to a subgroup of $\hat{G}/Z(\hat{G})$ for a classical group $\hat{G}$ of degree less than n, or of degree n and in the same characteristic p as G. This implies that P has a faithful projective representation ρ of degree less than n, or of degree n in characteristic $p \neq q$.

Let $\Sigma = \mathrm{SL}$. By [25, p. 419], the smallest degree of a non-trivial projective representation of $\mathrm{PSL}(n,q)$ in characteristic $p \neq q$ and for $(n,q) \neq (3,2)$ is at least $q^{n-1} - 1 > n$. In characteristic q, the minimal degree is n by [24, p. 201]. So the existence of ρ disposes of this option.

Now let $\Sigma = \mathrm{Sp}$. The same references as above give the smallest degree $d_p(n,q)$ of a faithful projective representation of $\mathrm{PSp}(n,q)$ in characteristic q as $d_q(n,p) = n$, in coprime characteristic $p \neq q$ as $d_p(n,q) = \frac{1}{2}(q^{\frac{n}{2}} - 1)$ for odd q, $d_p(n,2) = 2^{\frac{n}{2}-2}(2^{\frac{n}{2}-1} - 1)$ for $n > 6$, and $d_p(6,2) = 7 > 6$. Unless $(n,q) = (4,3)$, the existence of ρ once more gives a contradiction.

The only remaining case is $P = \mathrm{PSp}(4,3)$ as a section of $\mathrm{PSp}(4,q)$ for $q \neq 3$. Inspection of the maximal subgroups of $\mathrm{PSp}(4,q)$ (see [6, Tables 8.12 and 8.13]) shows that this is impossible. □

By happenstance the exceptions of Lemma 2.11 are close to those of Theorem 2.5 and Lemma 2.9 (degree at most 4 and characteristic a power of 2). So the prime $p = 2$ will be treated as exceptional if the degree n is 3 or 4. If $n > 4$ or p is an odd prime then we call the pair (n,p) *unexceptional*.

Lemma 2.12. *Let $n \geq 3$, $a \geq 1$, $q \geq 3$ be odd, and p be a prime not dividing q such that (n,p) is unexceptional. Suppose that $U \leq \Sigma(n, \mathbb{Z}_{p^a q}) = \Sigma(n, \mathbb{Z}_{p^a}) \times \Sigma(n, \mathbb{Z}_q)$ maps onto $\Sigma(n, \mathbb{Z}_{p^a})$ under natural projection of the entire direct product onto its first factor. Then U contains $\Sigma(n, \mathbb{Z}_{p^a})$.*

Proof. The group U is a subdirect product of its projections A, B into $\Sigma(n, \mathbb{Z}_{p^a})$ and $\Sigma(n, \mathbb{Z}_q)$, respectively, where A is all of $\Sigma(n, \mathbb{Z}_{p^a})$. Assuming first that $q = r^b$ is a prime power, we claim that $B \leq U$, i.e., $U = A \times B$. If not, then A and B have isomorphic non-trivial quotients. By Lemma 2.9, any non-trivial quotient of A has a quotient isomorphic to $A/R \cong \mathrm{P}\Sigma(n,p)$, where R is the solvable radical of A. In turn, A/R must be a section of the radical quotient $\mathrm{P}\Sigma(n,r)$ of $\Sigma(n, \mathbb{Z}_q)$: but this contradicts Lemma 2.11.

Suppose now that $q = r^b s$ with r prime and $\gcd(r,s) = 1$. By the preceding paragraph, $\Sigma(n, \mathbb{Z}_{p^a}) \leq \varphi_{p^a r^b}(U)$. Thus $U \cap \Sigma(n, \mathbb{Z}_{p^a s})$ projects onto $\Sigma(n, \mathbb{Z}_{p^a})$ modulo p^a. The lemma follows by induction. □

Theorem 2.13. *Let $n > 2$ and $H \leq \Gamma_n$ be arithmetic of level $M > 1$. Suppose that (n, p) is unexceptional and $\varphi_p(H) = \Sigma(n, p)$. Then $p \nmid M$.*

Proof. Assume that $\varphi_{p^{k-1}}(H) = \Sigma(n, \mathbb{Z}_{p^{k-1}})$ for some $k \geq 2$. Then $\varphi_{p^k}(H)$ is a supplement of $\ker \varphi_{p^{k-1}}$ in $\Sigma(n, \mathbb{Z}_{p^k})$, so $\varphi_{p^k}(H) = \Sigma(n, \mathbb{Z}_{p^k})$ by Theorem 2.5. Hence $\varphi_{p^k}(H) = \mathrm{SL}(n, \mathbb{Z}_{p^k})$ for all $k \geq 1$ by induction.

If $M = p^a q$ with $\gcd(p, q) = 1$ then $\Gamma_{n,q} \leq H$ by Lemma 2.12. Since H has level M, this forces $a = 0$. □

Corollary 2.14. *Suppose that $H \leq \Gamma_n$ is arithmetic, $n > 2$, and $\varphi_p(H) = \varphi_p(\Gamma_n)$ for all odd primes p. Then the level of H is a 2-power. If additionally $n \geq 5$ and $\varphi_2(H) = \varphi_2(\Gamma_n)$ then $H = \Gamma_n$.*

Remark 2.15. There are finitely generated subgroups H of Γ_n with infinite index such that $\Pi(H) = \emptyset$; see [21, 39].

Let $H \leq \Gamma_n$ for $n > 2$. Define

$$\delta_H(m) = |\Gamma_n : \Gamma_{n,m} H|.$$

That is, $\delta_H(m) = |\varphi_m(\Gamma_n) : \varphi_m(H)|$. We record a few properties of the delta function.

Lemma 2.16. *Let m, m' be positive integers.*

(a) *If $m \,|\, m'$ then $\delta_H(m) \,|\, \delta_H(m')$.*
(b) *Suppose that H is arithmetic of level M, so $\delta_H(M) = |\Gamma_n : H|$. Then*
  (i) *$\delta_H(m) \,|\, \delta_H(M)$*
  (ii) *$\delta_H(m) = \delta_H(M)$ if and only if $M \,|\, m$.*

The next theorem gives a criterion to test whether M is even (when $2 \notin \Pi$).

Theorem 2.17. *Let $n > 2$ and $H \leq \Gamma_n$ be arithmetic of level $M > 1$. Let q be the product of all odd primes in $\Pi(H)$. Then M is even if and only if $\delta_H(q) < \delta_H(4q)$.*

Proof. By Theorem 2.13, q is the product of all odd primes dividing M.

If M is odd then $\Gamma_{n,4q}\Gamma_{n,M} = \Gamma_{n,q}$, so $\delta_H(4q) = \delta_H(q)$.

For the rest of the proof, suppose that M is even: say $M = 2^l s$, $l \geq 1$, $s \geq 1$ odd. By Lemma 2.16, $\delta_H(s) < \delta_H(2^k s)$ for $1 \leq k \leq l$. So choose the least k and least multiple r of q dividing s such that $\delta_H(r) < \delta_H(2^k r)$. Then let $m = 2^k r$, $A = \varphi_{2^k}(H)$, $B = \varphi_r(H)$, and $N = \varphi_m(\Gamma_{n,r} \cap H)$.

If $A \neq \Sigma(n, \mathbb{Z}_{2^k})$ then by the same argument as in the first paragraph of the proof of Theorem 2.13 (here avoiding the exceptions for $p = 2$ in small degrees), $\varphi_4(H) \neq \Sigma(n, \mathbb{Z}_4)$. So $\delta_H(q) < \delta_H(4q)$.

Henceforth $A = \Sigma(n, \mathbb{Z}_{2^k})$. Then $\varphi_{2^k}(N)$ is a proper (normal) subgroup of A: otherwise, $\Gamma_{n,r} \leq \Gamma_n = (\Gamma_{n,r} \cap H)\Gamma_{n,2^k} \Rightarrow \Gamma_{n,r} \leq (\Gamma_{n,r} \cap H)(\Gamma_{n,2^k} \cap \Gamma_{n,r}) \Rightarrow$

$\Gamma_{n,r} \leq (\Gamma_{n,r} \cap H)\Gamma_{n,m} \Rightarrow \delta_H(r) = \delta_H(m)$. By Lemma 2.9, $\varphi_{2^k}(N)R \neq A$ where R is the solvable radical of A. Since R contains the kernel of φ_2 on A, $\varphi_2(N) \neq \Sigma(n,2)$. We conclude that $\delta_H(r) < \delta_H(2r)$. Therefore $k = 1$.

Let $L = \varphi_m(\Gamma_{n,2} \cap H)$. Then $L \neq \varphi_m(H)$ and $A/\varphi_2(N) \cong B/\varphi_r(L)$. Let K be the kernel of φ_q on $\varphi_r(H)$, i.e., $K = \varphi_r(H) \cap \varphi_r(\Gamma_{n,q}) = \varphi_r(H \cap \Gamma_{n,q})$. We show that $K\varphi_r(L) \neq B$. This will imply that $\varphi_{2q}(H)$ is a proper subdirect product of $A = \varphi_2(H)$ and $\varphi_q(H)$, so $\delta_H(q) < \delta_H(2q) \leq \delta_H(4q)$ as desired.

If $A/\varphi_2(N)$ is solvable then $|A : \varphi_2(N)| = 2$ by Lemma 2.9. Thus $K\varphi_r(L) \neq B$ because K has odd order. If $A/\varphi_2(N)$ is not solvable then neither is $B/\varphi_r(L)$, and the result again follows. □

For $n > 2$ and any $H \leq \Gamma_n$, define

$$\tilde{\Pi}(H) = \begin{cases} \{2\} \cup \Pi(H) & \text{if } n \leq 4,\ 2 \notin \Pi(H), \text{ and } \delta_H(4q) > \delta_H(q) \\ \Pi(H) & \text{otherwise} \end{cases} \tag{3}$$

where q is the product of all odd primes in $\Pi(H)$. Combining Theorems 2.13 and 2.17 yields the next theorem.

Theorem 2.18. *If H is arithmetic of level $M > 1$ then $\pi(M) = \tilde{\Pi}(H)$.*

We leave the problem of finding $\Pi(H)$ aside for the moment, returning to it in Section 3.

2.4.2. Now we aim for our promised algorithm to compute M from $\pi(M)$.

Lemma 2.19.

(i) *Suppose that $\delta_H(kp^a) = \delta_H(kp^{a+1})$ for some prime p, positive integer a, and k coprime to p. Then $\delta_H(kp^b) = \delta_H(kp^a)$ for all $b \geq a$.*

(ii) *Let p, a, and k be as in* (i)*. Then $\delta_H(lp^b) = \delta_H(lp^a)$ for all $b \geq a$ and any multiple l of k such that $\pi(l) = \pi(k)$.*

Proof. (i) If $b > a+1$ is minimal subject to $\delta_H(kp^b) \neq \delta_H(kp^a)$ then $\delta_H(kp^{b-2}) = \delta_H(kp^{b-1}) = \delta_H(kp^a)$. So $\Gamma_{n,kp^{b-2}} \leq \Gamma_{n,kp^{b-1}}H$, implying that $\Gamma_{n,kp^{b-2}} \cap H$ is a proper supplement of $\Gamma_{n,kp^{b-1}}$ in $\Gamma_{n,kp^{b-2}}$. Since

$$\Gamma_{n,kp^{b-2}}/\Gamma_{n,kp^b} \cong \Gamma_{n,p^{b-2}}/\Gamma_{n,p^b},$$

with $\Gamma_{n,kp^{b-1}}/\Gamma_{n,kp^b}$ corresponding to $\Gamma_{n,p^{b-1}}/\Gamma_{n,p^b}$ under the isomorphism, this contradicts Lemma 2.7.

(ii) Suppose that there are $b \geq a$, and l divisible by k with $\pi(l) = \pi(k)$, such that $\delta_H(lp^b) \neq \delta_H(lp^{b+1})$. By (i), $\delta_H(kp^b) = \delta_H(kp^{b+1})$. Define $\bar{H} = \Gamma_{n,kp^b} \cap \Gamma_{n,lp^{b+1}}H$. We observe that $\Gamma_{n,kp^b} = \Gamma_{n,kp^{b+1}}\bar{H}$ and $\bar{H}/\Gamma_{n,lp^{b+1}}$ is a proper subgroup of

$$\Gamma_{n,kp^b}/\Gamma_{n,lp^{b+1}} = \Gamma_{n,lp^b}/\Gamma_{n,lp^{b+1}} \times \Gamma_{n,kp^{b+1}}/\Gamma_{n,lp^{b+1}}.$$

The factors of this direct product have coprime orders: one is isomorphic to the p-group $\Gamma_{n,p^b}/\Gamma_{n,p^{b+1}}$; the other is isomorphic to $\Gamma_{n,k}/\Gamma_{n,l}$, which is a p'-group because $\pi(l) = \pi(k)$. Hence $\Gamma_{n,kp^{b+1}}\bar{H} = \Gamma_{n,kp^{b+1}}K$ for some $K < \Gamma_{n,lp^b}$ in $\bar{H}$ such that $K \cap \Gamma_{n,kp^{b+1}} = \Gamma_{n,lp^{b+1}}$. But then $\Gamma_{n,kp^{b+1}}\bar{H} \neq \Gamma_{n,kp^b}$. □

The following procedure computes the level of an arithmetic group H. The idea is to add higher powers of prime divisors of the level while δ_H increases, until δ_H reaches a stabilized value as dictated by Lemma 2.19. (We keep the specification of input and output completely general at this stage.)

`LevelMaxPCS`(S, σ)

Input: a generating set S for a subgroup $H \leq \Gamma_n$; a finite set σ of primes.
Output: an integer N.

For each $p \in \sigma$ let $\mu_p = 1$ and $z_p = \prod_{q\in\sigma, q\neq p} q$.
While $\exists\, p \in \sigma$ such that $\delta_H(p^{\mu_p+1} \cdot z_p) > \delta_H(p^{\mu_p} \cdot z_p)$
    increment μ_p by 1 and repeat.
Return $N = \prod_{p\in\sigma} p^{\mu_p}$.

Remark 2.20. The test for even M in Theorem 2.17 (which is invoked only when $n \leq 4$ and we have discovered that $2 \notin \Pi(H)$) makes a similar comparison of indices δ_H, and can be implemented using the same subroutines as above.

Remark 2.21. A reader might ask whether `LevelMaxPCS` is unduly complicated: perhaps the least p^a such that $\delta_H(p^a) = \delta_H(p^{a+1})$ is the p-part of the level of an input arithmetic group? This supposition is false, as the following example (constructed from a subdirect product of $\Gamma_{3,3}/\Gamma_{3,9} \cong C_3^8$ with a subgroup of $\mathrm{PSL}(3,5)$ of order 3) illustrates. Let

$$H = \Big\langle \Gamma_{3,45}, \begin{pmatrix} 1 & 30 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} -29 & 0 & -30 \\ 0 & 1 & 0 \\ 30 & 0 & 31 \end{pmatrix}, \begin{pmatrix} -29 & -45 & 15 \\ 30 & 1 & 30 \\ 30 & 0 & 31 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 0 & 0 \\ 15 & -29 & -30 \\ 30 & 30 & 31 \end{pmatrix}, \begin{pmatrix} 16 & 15 & 0 \\ -255 & -239 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 16 & 15 & 30 \\ -255 & -239 & 15 \\ 0 & 0 & 1 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 0 & 30 \\ 0 & 1 & 30 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 10 & 0 & 9 \\ 36 & -137 & 66 \\ -99 & -453 & 22 \end{pmatrix} \Big\rangle.$$

Then $\delta_H(3) = \delta_H(9) = 5616$, $\delta_H(5) = \delta_H(25) = 124000$, $\delta_H(15) = 696384000$, and $\delta_H(45) = 2089152000$. Hence H has level 45, not 15.

This example is a phenomenon of mixed primes: if the level of H is a prime-power p^r for unexceptional (n,p), and $\delta_H(p^a) = \delta_H(p^{a+1})$ for $a \geq 1$, then $r \leq a$.

The next theorem justifies correctness of `LevelMaxPCS` in our main situation.

Theorem 2.22. *If $H = \langle S \rangle$ is arithmetic of level M then* `LevelMaxPCS` *with input S and $\sigma = \pi(M)$ terminates, returning M.*

Proof. The values of δ_H encountered in the while-loop are bounded, because $\delta_H(m)$ divides $\delta_H(M)$ for all m. Thus `LevelMaxPCS` terminates.

If p^a is the p-part of M, and $q \big| M$ is coprime to p, then $\delta_H(p^{a+1}q) = \delta_H(p^a q)$. So the output N of `LevelMaxPCS` must divide M. Since $\pi(N) = \pi(M)$, this implies that $\delta_H(M) = \delta_H(N)$ by Lemma 2.19; and $M \big| N$ by Lemma 2.16. □

3. Computing with Zariski dense subgroups

Let $n > 2$ and H be a finitely generated subgroup of $\Gamma_n = \mathrm{SL}(n,\mathbb{Z})$ or $\mathrm{Sp}(n,\mathbb{Z})$. We describe how to compute $\Pi(H)$ when H is arithmetic, or, more generally, dense. This relies on knowing a transvection $t \in H$ (which is true of all groups in Section 4); and we restrict to odd degree n for $\Gamma_n = \mathrm{SL}(n,\mathbb{Z})$. Note that if H is arithmetic then it contains transvections, whereas if H is dense then it need not even contain a unipotent element [40, Proposition 5.3].

We also provide a simple algorithm to test density of H. Here again H should contain a known transvection, and n is odd if $\Gamma_n = \mathrm{SL}(n,\mathbb{Z})$. Less restricted density testing algorithms are discussed in Subsection 3.2. Then Subsection 3.3 extends `LevelMaxPCS` to dense input groups.

3.1. Density and transvections.

We formulate various conditions for density. The first result is truly fundamental (see [27], [31], and [35, Theorem 2.4]).

Theorem 3.1. *H is dense if and only if $\varphi_p(H) = \varphi_p(\Gamma_n)$ for some prime $p > 3$.*

Let $\mathbb{F}$ be a field. An element t of $\mathrm{GL}(n,\mathbb{F})$ is a *transvection* if it is unipotent and $1_n - t$ has rank 1.

Theorem 3.2 ([43])**.** *Let $n > 2$ and p be an odd prime. If $G \leq \mathrm{GL}(n,p)$ is irreducible and generated by transvections, then either $G = \mathrm{SL}(n,p)$ or G is conjugate to $\mathrm{Sp}(n,p)$.*

Corollary 3.3. *Suppose that $n > 2$, p is an odd prime, and $G \leq \mathrm{GL}(n,p)$ has a transvection t such that the normal closure $\langle t \rangle^G$ is irreducible. Then G contains $\mathrm{SL}(n,p)$ or a conjugate of $\mathrm{Sp}(n,p)$. In particular, $\mathrm{SL}(n,p) \leq G$ for odd n.*

Lemma 3.4. *Suppose that G is an irreducible subgroup of $\mathrm{GL}(n,\mathbb{F})$ and $t \in G$ is a transvection such that $\langle t \rangle^G$ is reducible. Then G is imprimitive.*

Proof. By Clifford's Theorem, $\mathbb{F}^n = W_1 \oplus \cdots \oplus W_k$ where $k > 1$ and the W_i are irreducible modules for $\langle t \rangle^G$. Then $t|_{W_i}$ must be a transvection for some i, and $t|_{W_j} = 1_{W_j}$ for $j \neq i$. Thus $\mathbb{F}^n$ has more than one homogeneous component. □

Corollary 3.5. *If $H \leq \Gamma_n$ has a transvection t such that $\langle t \rangle^H$ is not absolutely irreducible, then H is not dense.*

Proof. We may assume that H is absolutely irreducible, so that H is imprimitive by Lemma 3.4. Since $\varphi_p(\Gamma_n)$ is (absolutely) primitive, $\varphi_p(H) \neq \varphi_p(\Gamma_n)$ for almost all primes p. □

Corollary 3.6. *Let $G \leq \mathrm{GL}(n, \mathbb{F})$ and $t \in G$ be a transvection. Then $\langle t \rangle^G$ is irreducible if and only if G is primitive.*

Proof. One direction follows from [43, (1.9)], the other from Lemma 3.4. □

In Proposition 3.7 and Lemma 3.8, $H \leq \mathrm{SL}(n, \mathbb{Z})$ for odd $n > 2$, or $H \leq \mathrm{Sp}(n, \mathbb{Z})$ for $n > 2$.

Proposition 3.7. *Suppose that H contains a transvection t. Then H is dense if and only if $\langle t \rangle^H$ is absolutely irreducible.*

Proof. Put $N = \langle t \rangle^H$. If H is dense then it is absolutely irreducible and primitive; so N is absolutely irreducible by Corollary 3.6.

Suppose that N is absolutely irreducible. Since there exists an odd prime p such that $\varphi_p(N)$ is absolutely irreducible, and $\varphi_p(N)$ contains the transvection $\varphi_p(t)$, Theorem 3.1 and Corollary 3.3 imply that H is dense. □

Lemma 3.8. *H is dense if and only if there are a prime $p > 3$ and a transvection $t \in \varphi_p(H)$ such that $\langle t \rangle^{\varphi_p(H)}$ is irreducible.*

Proof. If H is dense then $\varphi_p(H) = \mathrm{SL}(n, p)$ or $\mathrm{Sp}(n, p)$ for a prime $p > 3$. Therefore $\varphi_p(H)$ contains a transvection t, and $\langle t \rangle^{\varphi_p(H)} = \varphi_p(H)$ is irreducible. The converse follows from Theorem 3.1 and Corollary 3.3. □

Lemma 3.9. *Suppose that $n > 2$ is prime and H is an absolutely irreducible subgroup of $\mathrm{SL}(n, \mathbb{Z})$ containing a transvection. Then H is dense.*

Proof. Let $t \in H$ be a transvection. If $\langle t \rangle^H$ is not absolutely irreducible then it is monomial. But t is certainly not monomial. Proposition 3.7 gives the result. □

3.2. **Algorithms to test density and compute Π.** Assume that n is odd if $\Gamma_n = \mathrm{SL}(n, \mathbb{Z})$, and we know a transvection t in $H \leq \Gamma_n$. By Proposition 3.7, testing density of H is the same as testing absolute irreducibility of $N = \langle t \rangle^H$. The latter may be carried out using the procedure `BasisAlgebraClosure` in [14, p. 401].

This returns a basis of the enveloping algebra $\langle N \rangle_{\mathbb{Q}}$, as words over an input generating set S for H. So we have the following density testing algorithm.

`IsDense`(S, t)

Input: a finite subset S of Γ_n and a transvection $t \in H = \langle S \rangle$.
Output: `true` if H is dense; `false` otherwise.

$\mathcal{A} =$ `BasisAlgebraClosure`(t, S).
Return `true` if $|\mathcal{A}| = n^2$; else return `false`.

Remark 3.10. (i) When n is prime, it suffices to test whether H itself is absolutely irreducible (Lemma 3.9).

(ii) By Corollary 3.5, if $\langle t \rangle^H$ is not absolutely irreducible then H is not dense. If $\langle t \rangle^H$ is absolutely irreducible and n is even then $\varphi_p(H)$ could be conjugate to $\mathrm{Sp}(n, p)$, so we must proceed by other means to decide whether H is dense.

We now discuss computing Π for dense $H = \langle S \rangle \leq \Gamma_n$, given a transvection $t \in H$. Let $\mathcal{A} = \{A_1, \ldots, A_{n^2}\} \subseteq H$ be a basis of $\langle \langle t \rangle^H \rangle_{\mathbb{Q}}$. Form the matrix $[\mathrm{tr}(A_i A_j)]_{ij}$ and denote its determinant by d. Let Π_1 be the set consisting of $\pi(d)$ together with the prime divisors of all non-zero non-diagonal entries of t. Then $\Pi \subseteq \Pi_1$. To obtain Π, we check whether $\varphi_p(H) = \varphi_p(\Gamma_n)$ for p running over Π_1. Call this process `PrimesForDense`(S, t).

If we have an upper bound on the primes in $\Pi(H)$ then we can find $\Pi(H)$. Such a bound may be derived from [7, pp. 10–11] (a quantitative version of strong approximation). Alternatively, we could use a Hadamard-type inequality for the matrix determinant associated to a basis $\mathcal{A}$ as above. However, the bounds resulting from either approach are impractically large.

Our algorithms in this subsection need an input transvection. As noted, a dense group may not contain unipotent elements. Moreover, unipotent elements are 'rare' [29]. We make some brief remarks about density testing (in any degree $n > 2$) without this constraint.

A dense group is absolutely irreducible and not solvable-by-finite. Both of these properties can be readily tested [14], which serves as a preliminary check. Note that if H is absolutely irreducible and contains a non-trivial unipotent element (e.g., a transvection) then H is not solvable-by-finite.

Monte-Carlo and deterministic algorithms for density testing are given in [34]. In Section 5, we compare our implementations of these algorithms and `IsDense`. Further afield, see [10] for an algorithm to compute Zariski closures, which could be applied to test density.

3.3. **Computing the minimal arithmetic overgroup.** Let $n > 2$ and $H = \langle S \rangle < \Gamma_n$ be dense. As Martin Kassabov has pointed out, there are only finitely many arithmetic subgroups of Γ_n containing H [23]. Their intersection is the *minimal* arithmetic overgroup of H. We generalize Theorems 2.18 and 2.22, thereby proving that `LevelMaxPCS` terminates for input H, returning the level of its minimal arithmetic overgroup.

Lemma 3.11. *If l is the level of the minimal arithmetic overgroup of H then $\pi(l) = \tilde{\Pi}(H)$ as defined in* (3)*.*

Proof. Let C be the overgroup. For any m we have $\Gamma_{n,m}H = \Gamma_{n,m}C$, because $C = \Gamma_{n,l}H$ is contained in the arithmetic group $\Gamma_{n,m}H$. Thus $\Pi(C) = \Pi(H)$, and $\delta_H(m) = \delta_H(m')$ if and only if $\delta_C(m) = \delta_C(m')$. The assertion is now evident from Theorem 2.18. □

Theorem 3.12. `LevelMaxPCS` *with input S and $\tilde{\Pi}(H)$ terminates, returning the level of the minimal arithmetic overgroup C of H.*

Proof. Since $\delta_H(m) \leq |\Gamma_n : C|$ for all m, `LevelMaxPCS` terminates. Say the output is M. By Lemma 3.11, $\pi(M) = \pi(l)$ and M divides l. Then $\delta_C(M) = \delta_C(l)$ by Lemma 2.19, so l divides M. □

4. Experimental results

We implemented the algorithms of Sections 2 and 3 in GAP, relying on the packages 'matgrp' [20] and 'recog' [33]. In this section we describe how we used our implementation to solve problems for important classes of groups that have been the focus of much activity. Times quoted for all experiments are in seconds, on a 3.7 GHz Quad-Core late 2013 Mac Pro with 32 GB memory.

4.1. **Small subgroups of $\mathrm{SL}(3,\mathbb{Z})$.** Lubotzky [28] asked whether every arithmetic subgroup of $\Gamma_n = \mathrm{SL}(n,\mathbb{Z})$ for $n > 2$ has a 2-generator subgroup of finite index. To support an affirmative answer to this question, the following groups were studied in [26, p. 414]. Let $G = \langle x, y, z \mid zxz^{-1} = xy,\ zyz^{-1} = yxy \rangle$ and $F = \langle x, y \rangle \leq G$. For $T \in \mathbb{Z}$ define the homomorphism $\beta_T : G \to \mathrm{SL}(3,\mathbb{Z})$ by

$$x \mapsto X_T = \begin{pmatrix} -1+T^3 & -T & T^2 \\ 0 & -1 & 2T \\ -T & 0 & 1 \end{pmatrix}, \quad y \mapsto Y_T = \begin{pmatrix} -1 & 0 & 0 \\ -T^2 & 1 & -T \\ T & 0 & -1 \end{pmatrix},$$

$$z \mapsto Z_T = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & T^2 \\ 0 & 1 & 0 \end{pmatrix}.$$

Lemma 4.1. (Cf. [26, Theorem 2.6].) *If $T \neq 0$ then $\beta_T(F)$ is dense.*

Proof. The element $b_1 = X_T^{-1}Y_T^3X_TY_T^2X_TY_T^{-1}X_T$ is a transvection [26, p. 418]. As $\beta_T(F)$ is absolutely irreducible, the result follows from Lemma 3.9. □

Theorem 4.2. ([26, Theorem 3.1].) *If $T \neq 0$ then $\beta_T(F)$ is arithmetic.*

Earlier attempts to compute $|\Gamma_3 : \beta_T(F)|$ failed [26, pp. 419, 423]. We compute these indices by first determining $\pi(M)$ from $\texttt{PrimesForDense}(\{X_T, Y_T\}, b_1)$ via Theorem 2.18. Then $M = \texttt{LevelMaxPCS}(\{X_T, Y_T\}, \pi(M))$. Table 1 displays sample results.

T	M	Index	Time
-1	11	$7{\cdot}19$	6.1
-2	2^6	$2^{19}7$	6.7
1	5	31	5.6
2	2^5	$2^{17}7$	6
3	3^373	$2^33^{11}13{\cdot}1801$	29.2
4	2^723	$2^{31}7^279$	16
5	5^3367	$2^43^25^{10}13{\cdot}31{\cdot}3463$	143.8
6	2^83^35	$2^{29}3^{10}7{\cdot}13{\cdot}31$	26.5
7	7^31021	$2^53^45{\cdot}7^{10}19{\cdot}347821$	570.7
8	$2^{10}191$	$2^{46}7^213^231$	98.6
9	3^62179	$2^33^{27}7{\cdot}13{\cdot}226201$	1652.1
10	$2^55^311{\cdot}17$	$2^{26}3{\cdot}5^{10}7^219{\cdot}31{\cdot}307$	50.7
11	$5{\cdot}11^3797$	$2^45^27{\cdot}11^{10}19{\cdot}31{\cdot}157{\cdot}4051$	1344.6
12	2^73^3647	$2^{35}3^{10}7{\cdot}13{\cdot}211{\cdot}1987$	721.4
13	$13^329{\cdot}227$	$2^43^27{\cdot}13^{11}61{\cdot}67{\cdot}73{\cdot}709$	246
14	2^67^3257	$2^{28}3^37^{11}19{\cdot}61{\cdot}1087$	195.5
15	$3^35^367{\cdot}151$	$2^93^{14}5^{10}7^313{\cdot}31^21093$	272.5
16	$2^{13}5{\cdot}307$	$2^{63}3^37{\cdot}31{\cdot}43{\cdot}733$	259.3
18	2^53^61093	$2^{23}3^{27}7{\cdot}13^2398581$	844
19	$19^367{\cdot}307$	$2^43^95{\cdot}7^219^{10}31{\cdot}43{\cdot}127{\cdot}733$	466.6
20	2^75^32999	$2^{36}3{\cdot}5^{10}7{\cdot}13{\cdot}31{\cdot}613{\cdot}1129$	13309.4
50	$2^55^623{\cdot}1019$	$2^{24}3{\cdot}5^{25}7^331{\cdot}79{\cdot}148483$	2584.7
100	$2^75^629{\cdot}67{\cdot}193$	$2^{42}3^55^{25}7^413{\cdot}31^267{\cdot}1783$	892.6

TABLE 1.

Remark 4.3. Lubotzky's question has been answered affirmatively [32].

Another representation $\rho_k : G \to \Gamma_3$ is defined in [26, p. 414] by

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

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

If $k \in \{0, 2, 3, 4, 5\}$ then $\rho_k(F)$ is arithmetic. Since a transvection in each group is known [26, p. 419], as before we can use `PrimesForDense` to find Π, then `LevelMaxPCS` with Theorem 2.18 to compute levels. The $\rho_k(F)$ and $\rho_k(G)$ relate to open conjectures in [26, Section 5]. Table 2 solves the main problem, namely finding indices in Γ_3. The last column states the time to compute $|\Gamma_3 : \rho_k(G)|$.

k	Level	$\lvert\Gamma_3 : \rho_k(G)\rvert$	$\lvert\Gamma_3 : \rho_k(F)\rvert$	Time
0	11	$7{\cdot}19$	$2{\cdot}5{\cdot}7{\cdot}19$	6
2	$2^2 5{\cdot}7$	$2^{12}3^2 5{\cdot}7^2 19{\cdot}31$	$2^{12}3^3 5{\cdot}7^2 19{\cdot}31$	15.4
3	13	$2^2 3{\cdot}13^2 61$	$2^3 3^2 13^2 61$	7
4	$3^3 7$	$2^4 3^{11} 7^2 13{\cdot}19$	$2^6 3^{13} 7^2 13{\cdot}19$	11.3
5	$2^2 19{\cdot}31$	$2^{10}3^3 5{\cdot}31^2 127{\cdot}331$	$2^{11}3^5 5{\cdot}31^2 127{\cdot}331$	49.1

TABLE 2.

4.2. **Monodromy groups.** Let $f(\mathrm{x}) = \prod_{j=1}^{n}(\mathrm{x} - a_j) = \mathrm{x}^n + A_{n-1}\mathrm{x}^{n-1} + \cdots + A_0$ and $g(\mathrm{x}) = \prod_{j=1}^{n}(\mathrm{x} - b_j) = \mathrm{x}^n + B_{n-1}\mathrm{x}^{n-1} + \cdots + B_0$ where $a_j = e^{2\pi \mathrm{i}\alpha_j}$ and $b_j = e^{2\pi \mathrm{i}\beta_j}$ for $\alpha_j, \beta_j \in \mathbb{C}$, $1 \le j \le n$. The group H generated by the companion matrices

$$A = \begin{pmatrix} 0 & \cdots & 0 & -A_0 \\ 1 & \cdots & 0 & -A_1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & -A_{n-1} \end{pmatrix}, \quad B = \begin{pmatrix} 0 & \cdots & 0 & -B_0 \\ 1 & \cdots & 0 & -B_1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & -B_{n-1} \end{pmatrix}$$

of $f(\mathrm{x})$ and $g(\mathrm{x})$ is the *hypergeometric group* corresponding to $f(\mathrm{x})$ and $g(\mathrm{x})$. It is the monodromy group of a hypergeometric ordinary differential equation (see [4, pp. 331–332], [5, p. 334], [38, p. 592]).

Suppose that $f(\mathrm{x})$, $g(\mathrm{x}) \in \mathbb{Z}[\mathrm{x}]$ are reciprocal ($f(\mathrm{x}) = \mathrm{x}^n f(1/\mathrm{x})$ and $g(\mathrm{x}) = \mathrm{x}^n g(1/\mathrm{x})$) with no common roots in $\mathbb{C}$. Further suppose that they constitute a primitive pair (there do not exist $f_1(\mathrm{x})$, $g_1(\mathrm{x}) \in \mathbb{Z}[\mathrm{x}]$ and $k \ge 2$ such that $f(\mathrm{x}) = f_1(\mathrm{x}^k)$ and $g(\mathrm{x}) = g_1(\mathrm{x}^k)$). Then $H \le \mathrm{Sp}(\Omega, \mathbb{Z})$ for some non-degenerate integral symplectic form Ω on $\mathbb{Z}^n$ [38, p. 592].

There are 14 pairs $(f(\mathrm{x}), g(\mathrm{x}))$ with $g(\mathrm{x}) \in \mathbb{Z}[\mathrm{x}]$ coprime to $f(\mathrm{x}) = (\mathrm{x}-1)^4$ such that the roots of $g(\mathrm{x})$ are roots of unity [38, pp. 595, 615]. The group $H = \langle A, B\rangle$ in these cases is a monodromy group associated with Calabi-Yau threefolds. Seven such H are arithmetic, and the rest are thin [5, 37, 38]. In [9, p. 175], H is shown to be $\mathrm{GL}(4,\mathbb{Q})$-conjugate to $G(d,k) := \langle U, T\rangle \leq \mathrm{Sp}(4,\mathbb{Z})$ where

$$U = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ d & d & 1 & 0 \\ 0 & -k & -1 & 1 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Note that conjugation preserves arithmeticity [21, p. 87]. For $d_2 \mid d_1$, let $\hat{G}(d_1, d_2)$ be the subgroup of $\mathrm{Sp}(4,\mathbb{Z})$ consisting of all h satisfying

$$h \equiv \begin{pmatrix} 1 & * & * & * \\ 0 & * & * & * \\ 0 & 0 & 1 & 0 \\ 0 & * & * & * \end{pmatrix} \bmod d_1 \quad \text{and} \quad h \equiv \begin{pmatrix} 1 & * & * & * \\ 0 & 1 & * & * \\ 0 & 0 & 1 & 0 \\ 0 & 0 & * & 1 \end{pmatrix} \bmod d_2.$$

If $d_1 = d$ and $d_2 = \gcd(d,k)$ then $\hat{G}(d_1,d_2)$ is an arithmetic subgroup of $\mathrm{Sp}(4,\mathbb{Z})$ containing $G(d,k)$. By [9, Appendix],

$$|\mathrm{Sp}(4,\mathbb{Z}) : \hat{G}(d_1,d_2)| = d_1^4 \cdot \textstyle\prod_{p\mid d_1}(1-p^{-4}) \cdot d_2^2 \cdot \prod_{p\mid d_2}(1-p^{-2}). \tag{4}$$

The overgroup $\hat{G}(d_1,d_2)$ could be used to investigate properties of $G(d,k)$, such as bounds on $|\mathrm{Sp}(4,\mathbb{Z}) : G(d,k)|$; cf. [18, p. 6]. Our implementation enables us to complete such tasks quickly, including those not completed in [18, p. 6]. Also, for the first time we can determine the minimal arithmetic overgroup of $G(d,k)$.

We compute $\Pi(G(d,k))$ via `PrimesForDense` with input transvection T, then the level and index of $G(d,k)$ via `LevelMaxPCS`. See Table 3.

The arithmetic $G(d,k)$ appear in rows 1–7. For $G(d,k)$ in any other row, we report the level and index of its minimal arithmetic overgroup. The first column defines $(\alpha_1,\alpha_2,\alpha_3,\alpha_4)$ for A, as $\alpha_3 = 1-\alpha_2$ and $\alpha_4 = 1-\alpha_1$. 'Time' is time to compute the level M, 'Index G' is index of the minimal arithmetic overgroup in $\mathrm{Sp}(4,\mathbb{Z})$, and 'Index $\hat{G}$' is $|\mathrm{Sp}(4,\mathbb{Z}) : \hat{G}(d_1,d_2)|$ from (4).

Remark 4.4. Table 3 shows that $\hat{G}(d_1,d_2)$ need not be the minimal arithmetic overgroup of $G(d,k)$. For instance, if $G(d,k)$ is arithmetic then it could differ from $\hat{G}(d_1,d_2)$. Also note that arithmeticity of groups of small index could in principle be determined by a coset enumeration once generators have been expressed as words in generators of Sp.

(α_1, α_2)	(d, k)	M	Index G	Time	Index $\hat{G}$
$(\frac{1}{10}, \frac{3}{10})$	$(1, 3)$	2	6	5.8	1
$(\frac{1}{6}, \frac{1}{6})$	$(1, 2)$	2	10	5.4	1
$(\frac{1}{6}, \frac{1}{4})$	$(2, 3)$	2^3	$2^6 3 \cdot 5$	7.1	$3 \cdot 5$
$(\frac{1}{6}, \frac{1}{3})$	$(3, 4)$	$2^2 3^2$	$2^9 3^5 5^2$	12.6	$2^4 5$
$(\frac{1}{4}, \frac{1}{4})$	$(4, 4)$	2^6	$2^{20} 3^2 5$	10.1	$2^6 3^2 5$
$(\frac{1}{4}, \frac{1}{3})$	$(6, 5)$	$2^3 3^2$	$2^{10} 3^6 5^2$	15.6	$2^4 3 \cdot 5^2$
$(\frac{1}{3}, \frac{1}{3})$	$(9, 6)$	$2 \cdot 3^5$	$2^8 3^{14} 5^2$	19.2	$2^7 3^4 5$
$(\frac{1}{5}, \frac{2}{5})$	$(5, 5)$	$2 \cdot 5^3$	$2^8 3^3 5^8 13$	11.9	$2^7 3^2 13$
$(\frac{1}{8}, \frac{3}{8})$	$(2, 4)$	2^4	$2^{11} 3^2 5$	7.3	$3^2 5$
$(\frac{1}{12}, \frac{5}{12})$	$(1, 4)$	2^2	$2^5 5$	5.8	1
$(\frac{1}{2}, \frac{1}{2})$	$(16, 8)$	2^{10}	$2^{40} 3^2 5$	20.1	$2^{16} 3^2 5$
$(\frac{1}{3}, \frac{1}{2})$	$(12, 7)$	$2^5 3^2$	$2^{17} 3^6 5^2$	25	$2^8 3 \cdot 5^2$
$(\frac{1}{4}, \frac{1}{2})$	$(8, 6)$	2^7	$2^{24} 3^2 5$	12.3	$2^8 3^2 5$
$(\frac{1}{6}, \frac{1}{2})$	$(4, 5)$	2^5	$2^{13} 3 \cdot 5$	9.9	$2^4 3 \cdot 5$

TABLE 3.

5. COMPARISON OF DENSITY TESTING ALGORITHMS

We now compare our implementations of the density testing algorithms suggested in [34] and Subsection 3.2.

`IsDenseIR1` is [34, Algorithm 1]. It accepts a finite subset S of $\Gamma_n = \mathrm{SL}(n, \mathbb{Z})$ or $\mathrm{Sp}(n, \mathbb{Z})$, $n > 2$, and tests whether $H = \langle S \rangle$ is dense. This is a Monte Carlo algorithm based on random choice of elements in H that have characteristic polynomial with large Galois group. Such elements are ubiquitous, in contrast to unipotent elements. `IsDenseIR1` returns `true` if it detects non-commuting g, $h \in H$ such that h has infinite order, and the Galois group of the characteristic polynomial of g is $\mathrm{Sym}(n)$ if $\Gamma_n = \mathrm{SL}(n, \mathbb{Z})$ or $C_2 \wr \mathrm{Sym}(n/2)$ if $\Gamma_n = \mathrm{Sp}(n, \mathbb{Z})$. An output message `true` means that H is dense, whereas `false` means that suitable g, h were not found (in that event, H may still be dense). We use an intrinsic GAP function to compute Galois groups. Attempts at selecting random elements by the default method for finite groups, product replacement [8], failed due to entry explosion in a precomputation step. So we took random words in the generators of length up to 50. These elements might be of poor quality. Indeed, sometimes the algorithm as implemented did not establish density. For G_1 below this happened about 40% of the time. The error rate could be reduced by a better choice of random elements, or by an iteration over more random elements, but at the cost of runtime.

The algorithm of [34, p. 23], which we call `IsDenseIR2`, is deterministic. It accepts a finitely generated subgroup H of a semisimple algebraic group $\mathcal{G}(\mathbb{F})$, $\operatorname{char}\mathbb{F} = 0$, and tests whether H is finite and whether the adjoint representation of H in $\mathrm{GL}(m, \mathbb{F})$ is absolutely irreducible, where m is the dimension of the Lie algebra of $\mathcal{G}(\mathbb{F})$. By incorporating methods from [13], this algorithm can be implemented over any field $\mathbb{F}$ of characteristic 0.

In Table 4, N is number of generators, and IR1, IR2, DFH are runtimes for our GAP implementations of `IsDenseIR1`, `IsDenseIR2`, `IsDense`, respectively.

Group	n	N	Output	IR1	IR2	DFH
G_1	5	4	true	0.01	11600	0.2
G_2	3	3	true	0.02	0.2	0.04
G_3	7	48	true	0.05	–	5
G_4	3	3	true	0.01	4.2	0.2
G_5	3	3	true	0.01	7.2	0.3
G_6	3	3	true	0.01	8.4	0.2
G_7	5	15	false	0.01	16200	0.5
G_8	5	10	false	0.01	24.4	0.7
G_9	11	13	false	0.01	–	1.2

TABLE 4.

The test groups G_i were selected to vary n, N, and group structure. We know a transvection in each group (often as one of the generators).

G_1, G_2, G_3 are arithmetic. G_1 is $\mathrm{SL}(5, \mathbb{Z})$, but not on the canonical generating set of elementary matrices. The congruence image of $G_2 \leq \mathrm{SL}(3, \mathbb{Z})$ is a $\{7, 79\}$-Hall subgroup of $\mathrm{SL}(3, \mathbb{Z}_{2^3 23^2})$. It has level $2^3 23^2$ and index $2^2 43^2 11^2 23^{11}$. $G_3 \leq \mathrm{SL}(7, \mathbb{Z})$ is generated by $E_{7,3^4 57^2}$ and the block diagonal matrices $\operatorname{diag}(h_1, h_2, 1)$ where $h_1 \in \beta_2(G)$ and $h_2 \in \rho_4(G)$ for G, β_T, ρ_k as in Subsection 4.1. It is arithmetic of level $3^8 5^2 7^4$.

G_4, G_5, G_6 are the groups generated by the transvections

$$T_1 = \begin{pmatrix} 1 & x^2+1 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad T_2 = \begin{pmatrix} 1 & 0 & 0 \\ x & 1 & x+1 \\ 0 & 0 & 1 \end{pmatrix},$$

$$T_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -x+1 & x^2 & 1 \end{pmatrix}$$

for $x = 11$, 99, 998 respectively. By [22], these groups are free and surject onto $\mathrm{SL}(3, p)$ modulo p for all primes p (`PrimesForDense` tells us that $\Pi(G_i) = \emptyset$

too); i.e., they are thin. As these G_i also surject modulo 4, they are congruent to $\mathrm{SL}(3,\mathbb{Z}_m)$ modulo m for $m \geq 2$.

The last three groups are not dense. G_7 is generated by $\mathrm{diag}(h_1,h_2) \in \mathrm{SL}(5,\mathbb{Z})$ where h_1, h_2 are generators of $\beta_5(G)$, $\mathrm{SL}(2,\mathbb{Z})$ respectively, together with the upper triangular elementary matrices. G_8 is the group of 5×5 upper unitriangular matrices. G_9 is generated by $\mathrm{diag}(h_1,h_2) \in \mathrm{SL}(11,\mathbb{Z})$ where h_1, h_2 range over generating sets for $\mathrm{SL}(6,\mathbb{Z})$ and $\mathrm{SL}(5,\mathbb{Z})$, respectively, together with five randomly chosen upper unitriangular matrices.

More detail is available at `http://www.math.colostate.edu/~hulpke/examples/densityex.g`.

We write '$-$' in Table 4 if `IsDenseIR2` did not terminate within 12 hours. This occurred for input of degree greater than 5 (the adjoint representation leads to calculation in an $(n^2-1)^2$-dimensional lattice). Finally, remember that `IsDense` facilitates the computation of $\Pi(H)$ for dense input H, unlike `IsDenseIR1` and `IsDenseIR2`.

Acknowledgments. We are indebted to Professors Willem de Graaf, Derek Holt, Martin Kassabov, and T. N. Venkataramana for their vital assistance.

The first and second authors were supported by the Irish Research Council (grants 'MatGpAlg' and 'MatGroups') and Science Foundation Ireland (grant 11/RFP.1/MTH/3212). The third author was supported by Simons Foundation Collaboration Grant 244502.

REFERENCES

1. M. Aschbacher, *On the maximal subgroups of the finite classical groups*, Invent. Math. **76** (1984), 496–514.
2. H. Bass, J. Milnor, and J.-P. Serre, *Solution of the congruence subgroup problem for* SL_n $(n \geq 3)$ *and* Sp_{2n} $(n \geq 2)$, Inst. Hautes Études Sci. Publ. Math. (1967), no. 33, 59–137.
3. B. Beisiegel, *Die Automorphismengruppen homozyklischer p-Gruppen*, Arch. Math. (Basel) **29** (1977), no. 4, 363–366.
4. F. Beukers and G. Heckman, *Monodromy for the hypergeometric function* ${}_nF_{n-1}$, Invent. Math. **95** (1989), 325–354.
5. C. Brav and H. Thomas, *Thin monodromy in* $\mathrm{Sp}(4)$, Compositio Math. **150** (2014), 333–343.
6. 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.
7. E. Breuillard, *Approximate subgroups and super-strong approximation*, `http://arxiv.org/abs/1407.3158v2`.
8. F. Celler, C.R. Leedham-Green, S. Murray, A. C. Niemeyer, and E. A. O'Brien, *Generating random elements of a finite group*, Comm. Algebra **23** (1995), no. 13, 4931–4948.
9. Y. Chen, Y. Yang, and N. Yui, *Monodromy of Calabi-Yau differential equations* (with an appendix by Cord Erdenberger), J. Reine Angew. Math. **616** (2008), 167–203.

10. H. Derksen, E. Jeandel, and P. Koiran, *Quantum automata and algebraic groups*, J. Symbolic Comput. **39** (2005), 357–371.
11. A. S. Detinko, D. L. Flannery, and A. Hulpke, *Algorithms for arithmetic groups with the congruence subgroup property*, J. Algebra **421** (2015), 234–259.
12. ———, *Strong approximation and experimenting with linear groups*, preprint (2016).
13. 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.
14. ———, *Algorithms for the Tits alternative and related problems*, J. Algebra **344** (2011), 397–406.
15. The GAP Group, GAP – Groups, Algorithms, and Programming, `http://www.gap-system.org`
16. F. Grunewald and D. Segal, *Some general algorithms. I. Arithmetic groups*, Ann. of Math. (2) **112** (1980), no. 3, 531–583.
17. A. J. Hahn and O. T. O'Meara, The Classical Groups and K-theory, Grundlehren der Mathematischen Wissenschaften, vol. 291, Springer-Verlag, Berlin, 1989.
18. J. Hofmann and D. van Straten, *Some monodromy groups of finite index in* $\mathrm{Sp}_4(\mathbb{Z})$, `http://arxiv.org/abs/1312.3063v1`.
19. A. Hulpke, *Computing generators of groups preserving a bilinear form over residue class rings*, J. Symbolic Comput. **50** (2013), 298–307.
20. A. Hulpke, The GAP package `matgrp`, `http://www.math.colostate.edu/~hulpke/matgrp/`
21. J. E. Humphreys, Arithmetic Groups, Lecture Notes in Mathematics **789**, Springer-Verlag, Berlin, 1980.
22. S. P. Humphries, *Free subgroups of* $\mathrm{SL}(n,\mathbb{Z})$, $n > 2$, *generated by transvections*, J. Algebra **116** (1988), 155–162.
23. M. Kassabov, private communication.
24. P. Kleidman and M. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Mathematical Society Lecture Note Series, vol. 129, Cambridge University Press, Cambridge, 1990.
25. V. Landazuri and G. M. Seitz, *On the minimal degrees of projective representations of the finite Chevalley groups*, J. Algebra **32** (1974), 418–443.
26. D. D. Long and A. W. Reid, *Small subgroups of* $\mathrm{SL}(3,\mathbb{Z})$, Exper. Math. **20** (2011), no. 4, 412–425.
27. 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.
28. ———, *Dimension function for discrete groups*, Proceedings of Groups St Andrews 1985, London Math. Soc. Lecture Note Ser. **121**, Cambridge Univ. Press, Cambridge, 1986, pp. 254–262.
29. A. Lubotzky and C. Meiri, *Sieve methods in group theory I: powers in linear groups*. J. Amer. Math. Soc. **25** (2012), no. 4, 1119–1148.
30. A. Lubotzky and D. Segal, Subgroup Growth, Birkhäuser, Basel, 2003.
31. C. Matthews, L. N. Vaserstein, and B. Weisfeiler, *Congruence properties of Zariski-dense subgroups. I*, Proc. London Math. Soc. (3) **48** (1984), no. 3, 514–532.
32. C. Meiri, *Generating pairs for finite index subgroups of* $\mathrm{SL}(n,\mathbb{Z})$, `http://arxiv.org/abs/1511.07798v1`
33. M. Neunhöffer, Á. Seress, et al., The GAP package `recog`, *a collection of group recognition methods*, `http://gap-packages.github.io/recog/`

34. I. Rivin, *Large Galois groups with applications to Zariski density*, `http://arxiv.org/abs/1312.3009v4`
35. ———, *Zariski density and genericity*, Int. Math. Res. Not. IMRN 2010, no. 19, 3649–3657.
36. 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.
37. S. Singh, *Arithmeticity of four hypergeometric monodromy groups associated to Calabi-Yau threefolds*, `http://arxiv.org/abs/1308.4039v6`.
38. S. Singh and T. Venkataramana, *Arithmeticity of certain symplectic hypergeometric groups*, Duke Math. J. **163** (2014), no. 3, 591–617.
39. G. A. Soifer and T. N. Venkataramana, *Finitely generated profinitely dense free groups in higher rank semi-simple groups*, Transform. Groups **5** (2000), no. 1, 93–100.
40. T. N. Venkataramana, *Zariski dense subgroups of arithmetic groups*, J. Algebra **108** (1987), 325–339.
41. T. Weigel, *On a certain class of Frattini extensions of finite Chevalley groups*, Groups of Lie type and their geometries (Como, 1993), 281–288, London Math. Soc. Lecture Note Ser. **207**, Cambridge Univ. Press, Cambridge, 1995.
42. ———, *On the profinite completion of arithmetic groups of split type*, Lois d'algèbres et variétés algébriques (Colmar, 1991), 79–101, Travaux en Cours, **50**, Hermann, Paris, 1996.
43. A. E. Zalesskii, V. N. Serežkin, *Linear groups generated by transvections*, Izv. Akad. Nauk SSSR Ser. Mat. **40** (1976), no. 1, 26–49 (Russian).