Computing with congruence subgroups of linear groups

Dane Flannery (joint with Alla Detinko and Alexander Hulpke)

Previously we realized strong approximation computationally for (finitely generated) dense groups $H \leq \Gamma(n, \mathbb{Q})$, $\Gamma = \mathrm{SL}$ or Sp.

That is, we showed how to determine all congruence images $\varphi_\rho(H)$ of H modulo the maximal ideals ρ of $R = \mathbb{Z}[1/\mu] \subseteq \mathbb{Q}$ such that $H \leq \Gamma(n, R)$.

Now we discuss algorithms for structural investigation of such H.

Again for convenience restrict to dense input $H \leq \mathrm{SL}(n, \mathbb{Z})$; however, the algorithms work for input dense $H \leq \Gamma(n, \mathbb{Q})$ generally.

The congruence subgroup property

$\mathrm{SL}(n,\mathbb{Q})$ and $\mathrm{SL}(n,\mathbb{Z})$ have very different normal subgroup structure.

For $\Gamma_n := \mathrm{SL}(n,\mathbb{Z})$, $n, m \geq 2$, let $\varphi_m\colon \mathrm{SL}(n,\mathbb{Z}) \twoheadrightarrow \mathrm{SL}(n,\mathbb{Z}_m)$ be the reduction modulo m congruence homomorphism.

Then $\Gamma_{n,m} := \ker \varphi_m$ on Γ_n is the *principal congruence subgroup* (PCS) *of level* m in Γ_n. Note that $\Gamma_{n,b} \leq \Gamma_{n,a} \Leftrightarrow a \big| b$.

A subgroup of Γ_n that contains some PCS is called a *congruence subgroup*.

Each congruence subgroup of Γ_n has finite index: it contains a normal subgroup of Γ_n with quotient $\mathrm{SL}(n,\mathbb{Z}_m)$ for some m.
Conversely, must finite-index $H \leq \Gamma_n$ be a congruence subgroup?

This question was raised long ago. If the answer is 'yes', then Γ_n has the *congruence subgroup property* (CSP).

Γ_2 does not have the CSP.

This was known to Klein. E.g., for large r the simple group $\mathrm{Alt}(r)$ *is not* a quotient of any $\mathrm{SL}(2, \mathbb{Z}_m)$; whereas $\mathrm{Alt}(r)$ *is* a quotient of $\mathrm{SL}(2, \mathbb{Z})$.

Note that Γ_2 is virtually free—i.e., it has a free subgroup of finite index ($\Gamma_{2,2} = \langle -1_n, H\rangle$ where $H = \left\langle \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} \right\rangle$ is free of rank 2)—whereas Γ_n for $n > 2$ is not virtually free.

Also note that there are implemented algorithms to decide whether a given finite-index subgroup of Γ_2 is a congruence subgroup.

However:

Theorem

If $n > 2$ then Γ_n has the CSP.

Independent proofs were given by Mennicke (1965), and by Bass, Milnor, Serre (1967; they proved that $\mathrm{Sp}(n, \mathbb{Z})$ for $n > 2$ also has the CSP). This theorem is actually a consequence of the following.

Theorem

For $m \geq 2$, let $E_{n,m}$ be the subgroup of Γ_n generated by all transvections $t_{i,j}(m)$, $i \neq j$. Then $\Gamma_{n,m}$ is the normal closure of $E_{n,m}$ in Γ_n.

Clearly $\Gamma_{n,m}$ contains the normal closure: each $t_{i,j}(m)$, the matrix with m in position (i, j), 1s down the main diagonal, and 0s elsewhere, is in $\Gamma_{n,m}$.

Computing the level

Proposition

Finding the level of a PCS in any given congruence subgroup of Γ_n is decidable.

Proof. Γ_n has a known finite presentation. Let $H \leq \Gamma_n$ be a congruence subgroup, so H is finitely generated. Assume that H is given by a finite generating set. Express each generator of H as a word in generators of Γ_n. Compute $c = |\Gamma_n : H|$ by coset enumeration. Let $K = \cap_{g \in \Gamma_n} gHg^{-1}$, the core of H; so $K \trianglelefteq \Gamma_n$ and $|\Gamma_n : K|$ divides $m := c!$. Hence $t_{i,j}(m) = t_{i,j}(1)^m \in K$, implying that $E_{n,m} \leq K$. Then H contains the Γ_n-normal closure $\Gamma_{n,m}$ of $E_{n,m}$. □

Two principal congruence subgroups generate a congruence subgroup; the intersection of any two of them is a PCS.

Proposition

Let $a, b \in \mathbb{N}$, and put $d = \gcd(a, b)$, $l = \operatorname{lcm}(a, b)$. Then

(i) $\Gamma_{n,a}\Gamma_{n,b} = \Gamma_{n,d}$;

(ii) $\Gamma_{n,a} \cap \Gamma_{n,b} = \Gamma_{n,l}$.

By (i), $\exists$ a unique maximal PCS in any congruence subgroup H of Γ_n: the PCS of Γ_n of least level in H; it contains every PCS contained in H.

Say that a congruence subgroup has level ℓ if its maximal PCS has level ℓ.

Main problem: compute the level of a given congruence subgroup of Γ_n.

The solution of this problem is connected to the main problem of the previous lecture, and thus to SAT.

Lemma

If k and m are coprime then φ_k surjects $\Gamma_{n,m} \leq \Gamma_n$ onto $\mathrm{SL}(n, \mathbb{Z}_k)$.

Proof. Use that m is invertible modulo k and the fact (again) that $\mathrm{SL}(n, \mathbb{Z}_k)$ is generated by transvections $t_{i,j} = t_{i,j}(1)$. □

So a congruence subgroup of Γ_n surjects onto $\mathrm{SL}(n, p)$ modulo almost all primes p. By SAT ($\equiv$ density for finitely generated subgroups of Γ_n):

Each congruence subgroup of Γ_n is dense.

Let $H \leq \Gamma_n$ be a congruence subgroup, of level ℓ. Recall: by running `PrimesForDense`, we can compute the set $\Pi(H)$ of primes p such that $\varphi_p(H) \neq \mathrm{SL}(n, p)$.

By the lemma, if k is a prime not dividing ℓ, then $\varphi_k(H) = \mathrm{SL}(n, \mathbb{Z}_k)$. So, denoting the set of prime divisors of $r \in \mathbb{N}$ by $\pi(r)$:

$\Pi(H) \subseteq \pi(\ell)$.

We have almost a full converse.

Theorem (DFH, 2018)

Let $n \geq 3$ and let $H \leq \Gamma_n$ be a congruence subgroup, of level ℓ. Then $\pi(\ell) \setminus \{2\} \subseteq \Pi(H)$.

The proof of this theorem is long. It uses knowledge of the subgroup structure of $\mathrm{SL}(n, \mathbb{Z}_{p^k})$ for primes p. We also need a theorem of Holt on simple sections of finite classical groups.

Note that we can decide when ℓ is even, and there is a version of the above theorem in degree 2 (DFH, 2023). So for all degrees $n \geq 2$:

If $H \leq \Gamma_n$ is a congruence subgroup, of level ℓ, then $\pi(\ell)$ can be found once $\Pi(H)$ is known.

To explain how the above may be turned into an algorithm to compute the level of a given congruence subgroup of Γ_n, we make the following definition, for any $H \leq \Gamma_n$.

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

i.e., $\delta_H(m) = |\mathrm{SL}(n, \mathbb{Z}_m) : \varphi_m(H)|$ can be computed in $\mathrm{SL}(n, \mathbb{Z}_m)$.

Lemma (DFH, 2018)

Suppose that $\delta_H(kp^a) = \delta_H(kp^{a+1})$ for p prime, $a \geq 1$, and $p \nmid k$. Then

(i) $\delta_H(kp^b) = \delta_H(kp^a)\ \forall\, b \geq a$;

(ii) $\delta_H(lp^b) = \delta_H(lp^a)\ \forall\, b \geq a$ and multiples l of k s.t. $\pi(l) = \pi(k)$.

As noted, $\Pi(H)$ gives the set $\pi(\ell)$ of all primes dividing the level ℓ of a congruence subgroup $H \leq \Gamma_n$.

The above lemma leads to the main idea of our level algorithm:

- Grow exponents on each prime $p|\ell$ as δ_H-values (fixing other prime divisors of ℓ) increase.
- The exact p-power dividing ℓ is reached as soon as δ_H-values stabilize. (Proof of this claim uses the above lemma. See the theorem below.)

`LevelMaxPCS`$(X, \mathcal{S})$

INPUT: a generating set X for $H \leq \Gamma_n$, a set $\mathcal{S}$ of primes.

OUTPUT: an integer k.

For each $p \in \mathcal{S}$

$\nu_p := 1$; $z_p :=$ the product of all primes in $\mathcal{S} \setminus \{p\}$.

While $\delta_H(p^{\nu_p+1} \cdot z_p) > \delta_H(p^{\nu_p} \cdot z_p)$

$\nu_p \leftarrow \nu_p + 1$.

Return $k :=$ the product of all p^{ν_p} for $p \in \mathcal{S}$.

Theorem (DFH, 2018)

If $H = \langle X \rangle$ is a congruence subgroup of level ℓ in Γ_n, then `LevelMaxPCS` with input X and $\mathcal{S} = \pi(\ell)$ terminates, returning ℓ.

All computation for `LevelMaxPCS` is in groups over finite rings $\mathbb{Z}_m$. For this, $\exists$ a standard reduction to prime-power m (implicit in earlier proofs).

Let $m = m_1 \cdots m_t$, m_i powers of distinct primes. Define $\alpha\colon \mathbb{Z}_m \to \oplus_{i=1}^{t} \mathbb{Z}_{m_i}$ by $\alpha(a) = (a_1, \ldots, a_t)$ where $a_i \equiv a \bmod m_i$. By the Chinese remainder theorem, α is a ring isomorphism.

Lemma

The above map α extends to a ring isomorphism from $\mathrm{Mat}(n, \mathbb{Z}_m)$ onto $\mathrm{Mat}(n, \mathbb{Z}_{m_1}) \oplus \cdots \oplus \mathrm{Mat}(n, \mathbb{Z}_{m_t})$, which restricts to group isomorphisms

$$\mathrm{GL}(n, \mathbb{Z}_m) \to \mathrm{GL}(n, \mathbb{Z}_{m_1}) \times \cdots \times \mathrm{GL}(n, \mathbb{Z}_{m_t})$$

and

$$\mathrm{SL}(n, \mathbb{Z}_m) \to \mathrm{SL}(n, \mathbb{Z}_{m_1}) \times \cdots \times \mathrm{SL}(n, \mathbb{Z}_{m_t}).$$

The congruence closure

Congruence subgroups are dense. In the opposite direction we have the following deep result, another consequence of strong approximation (see Theorem 2, p. 391 of *Subgroup growth* by Lubotzky & Segal).

Theorem

If $H \leq \Gamma_n$ is finitely generated and dense, then the intersection of all congruence subgroups of Γ_n that contain H is also a congruence subgroup.

So the dense group H has a *congruence closure*: $\exists$ a congruence subgroup $\mathrm{cl}(H)$ of Γ_n such that $H \leq \mathrm{cl}(H)$ and $\mathrm{cl}(H) \leq C$ for every congruence subgroup C containing H.

Lemma

Let H be a finitely generated dense subgroup of Γ_n. Then

(i) $\mathrm{cl}(H) = \Gamma_{n,\ell} H$ where ℓ is the level of $\mathrm{cl}(H)$;

(ii) $\Pi(\mathrm{cl}(H)) = \Pi(H)$.

Say that dense finitely generated $H \leq \Gamma_n$ has level ℓ if $\mathrm{cl}(H)$ has level ℓ.

Theorem (DFH, 2023)

`LevelMaxPCS` with input finitely generated dense $H \leq \Gamma_n$ and the set of primes $\mathcal{S}$ dividing the level of $\mathrm{cl}(H)$ returns the level of H.

Since $\Pi(\mathrm{cl}(H)) = \Pi(H)$, after running `PrimesForDense` on H we can compute $\mathcal{S}$ from $\Pi(H)$ as before.

Arithmetic subgroups

Let $G \leq \mathrm{GL}(n, \mathbb{C})$ be a $\mathbb{Q}$-group. If $H \leq G \cap \mathrm{GL}(n, \mathbb{Q})$ and $H \cap \mathrm{GL}(n, \mathbb{Z})$ has finite index in each of H and $G \cap \mathrm{GL}(n, \mathbb{Z})$, then H is an *arithmetic subgroup* of G. In particular, finite-index subgroups of Γ_n are arithmetic.

Note that finite-index subgroups of Γ_n are dense.

Suppose that $H \leq \Gamma_n$ is finitely generated dense, and we have computed the level ℓ of H using `LevelMaxPCS` and `PrimesForDense`.
If $\delta_H(\ell) = |\Gamma_n : \mathrm{cl}(H)| = |\mathrm{SL}(n, \mathbb{Z}_\ell) : \varphi_\ell(H)|$ is not big, then to test whether H is arithmetic, we are encouraged to attempt coset enumeration.

On the other hand, if $|\Gamma_n : \mathrm{cl}(H)|$ is small, but coset enumeration for H in Γ_n fails to terminate, then we might suspect that H is *thin*: dense and of infinite index in Γ_n.

It is unknown whether arithmeticity testing is decidable in general. It is certainly semidecidable (coset enumeration confirms arithmeticity of H if H is indeed arithmetic).

Arithmeticity testing algorithms exist in special cases, e.g., for input subgroups of solvable $\mathbb{Q}$-groups; see de Graaf, Detinko, Flannery (2015).

Suppose that $H \leq \Gamma_n$ for $n \geq 3$ is known to be arithmetic, by whatever means; so H is dense.

By CSP, H is a congruence subgroup. If we have computed the level ℓ of $H = \mathrm{cl}(H)$, then other problems for H can be solved.

E.g., membership testing (easy: $g \in \Gamma_n$ is in $H \Leftrightarrow \varphi_\ell(g) \in \varphi_\ell(H)$), and the orbit-stabilizer problem for H acting on $\mathbb{Z}^n$ (DFH 2015).

Implementation and experimentation

As noted, computing with congruence images $\varphi_m(H)$ in $\mathrm{GL}(n, \mathbb{Z}_m)$ can be reduced to the case of m a power of a prime p.

For computing in $\mathrm{GL}(n, \mathbb{Z}_{p^k})$, p prime, a 'trivial Fitting' method is used; as a main step this factors out the solvable radical of $\varphi_{p^k}(H)$.

`LevelMaxPCS` and associated procedures have been implemented and tested in GAP by exhaustive experimentation. For GAP code see Alexander's github page `https://github.com/hulpke/arithmetic`

Experiments are fully discussed in, e.g., DFH (2015, 2018, 2023).

See the talks next week by Alexander and Alla Detinko for more details.

References

- H. Bass, J. Milnor, J. and J.-P. Serre, Solution of the congruence subgroup problem for $\mathrm{SL}_n\,(n \geq 3)$ and $\mathrm{Sp}_{2n}\,(n \geq 2)$, Inst. Hautes Études Sci. Publ. Math. 33 (1967).
- J. L. Mennicke, Finite factor groups of the unimodular group, Ann. of Math. (2) 81 (1965).
- A. Lubotzky and D. Segal, *Subgroup growth*, Birkhäuser, 2003.
- A. S. Detinko, D. L. Flannery, and A. Hulpke, Algorithms for arithmetic groups with the congruence subgroup property, J. Algebra 421 (2015).
- A. S. Detinko, D. L. Flannery, and A. Hulpke, Zariski density and computing in arithmetic groups, Math. Comp. 87 (2018).
- A. S. Detinko, D. L. Flannery, and A. Hulpke, Zariski density and computing with S-integral groups, J. Algebra 624 (2023).