From finite to strong approximation

Dane Flannery (joint with Alla Detinko and Alexander Hulpke)

In lectures 2 and 3, we move on to computing with finitely generated linear groups in the second (i.e., non-SF) case of the Tits alternative.

Some new features:

- One (maximal) ideal of the coefficient ring defining a congruence homomorphism sufficed in previous algorithms, e.g., to test finiteness and decide the Tits alternative. Now we consider multiple ideals for a fixed input group.
- Congruence images in previous algorithms are matrix groups over finite fields, for which there is established computational machinery; now we need to compute with congruence image groups over rings $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$, m not necessarily prime.

Decidability looms larger. E.g., testing membership of elements of $\mathrm{GL}(n, \mathbb{Q})$ in a given finitely generated SF subgroup of $\mathrm{GL}(n, \mathbb{Q})$ is decidable (Kopytov, 1968); but membership testing in the non-SF group $\mathrm{GL}(n, \mathbb{Q})$, $n \geq 4$ is undecidable by Mihailova's result.

Note also that while we can test virtual solvability of finitely generated linear groups, no general method to test freeness of finitely generated linear groups is known.

Motivation for design of algorithms in this lecture and the next stems partially from applications (experimentation with small-degree groups arising in problems from topology, number theory, etc.).

Linear algebraic groups

The *Zariski topology* on $\mathbb{F}^m$ is defined as follows: $S \subseteq \mathbb{F}^m$ is closed (S is an *algebraic* set) if $\exists\ \mathcal{P} \subseteq \mathbb{F}[\mathbf{x}] = \mathbb{F}[\mathrm{x}_1, \ldots, \mathrm{x}_m]$ such that

$$S = \{(a_1, \ldots, a_m) \in \mathbb{F}^m \mid f(a_1, \ldots, a_m) = 0 \text{ for all } f(\mathbf{x}) \in \mathcal{P}\}.$$

A closed set is the set of zeros for a finite set of polynomials (Hilbert).

We identify $\mathrm{Mat}(n, \mathbb{F})$ as an $\mathbb{F}$-vector space with $\mathbb{F}^{n^2}$ and endow it with the Zariski topology.

A *(linear) algebraic group* is a subgroup of $\mathrm{GL}(n, \mathbb{F})$ closed in the subspace topology on $\mathrm{GL}(n, \mathbb{F})$.

E.g., $\mathrm{SL}(n, \mathbb{F})$, $\mathrm{Sp}(n, \mathbb{F})$, other classical groups are algebraic.

To recall: $\mathrm{Sp}(n,R)$ for a commutative ring R with 1 and $n=2m$ is the subgroup of $\mathrm{GL}(n,R)$ consisting of all h such that

$$h^\top J_n h = J_n \ \text{ where } \ J_n = \begin{bmatrix} 0_m & 1_m \\ -1_m & 0_m \end{bmatrix}.$$

It can be shown that $\mathrm{Sp}(n,R) \le \mathrm{SL}(n,R)$.

Topological terms henceforth are with respect to the Zariski topology on linear groups.

An algebraic subgroup G of $\mathrm{GL}(n,\mathbb{C})$ is a $\mathbb{Q}$-*group* (*defined over* $\mathbb{Q}$) if its defining polynomials have all coefficients in $\mathbb{Q}$.

E.g., $\mathrm{SL}(n,\mathbb{C})$ and $\mathrm{Sp}(n,\mathbb{C})$ are $\mathbb{Q}$-groups.

Density

For a commutative ring R with 1, $\Gamma(n,R) := \mathrm{SL}(n,R)$ or $\mathrm{Sp}(n,R)$.

At this stage, our algorithms applying strong approximation for linear groups accept finitely generated dense subgroups of $\Gamma(n,\mathbb{Q})$.

Testing density in $\Gamma(n,\mathbb{Q})$ is thus an initial problem (and of fundamental interest otherwise): given finitely generated $H \le \Gamma(n,\mathbb{Q})$, is the closure of H in $\Gamma(n,\mathbb{Q})$—which is a subgroup—equal to $\Gamma(n,\mathbb{Q})$?

For this see the Rivin theorem below. We have simpler density tests in special cases, say prime degree. E.g., testing density in $\mathrm{SL}(2,\mathbb{Q}) \equiv$ testing virtual solvability.

Singletons are closed, so a dense subgroup of $\Gamma(n,\mathbb{Q})$ must be infinite.

Theorem (Rivin)

Let $H \leq G$ where G is a simple algebraic subgroup of $\mathrm{GL}(n, \mathbb{F})$, $\mathbb{F}$ algebraically closed and $\operatorname{char} \mathbb{F} = 0$. Then H is dense in $G \Leftrightarrow H$ is infinite and the adjoint representation of H on the Lie algebra of G is irreducible.

Note $G \leq \mathrm{GL}(n, \mathbb{F})$ is *irreducible* if the only subspaces of $\mathbb{F}^n$ that G leaves invariant are $\mathbb{F}^n$ and $\{\mathbf{0}\}$. G is *absolutely irreducible* if G stays irreducible as a subgroup of $\mathrm{GL}(n, \mathbb{E})$ for every field extension $\mathbb{E}/\mathbb{F}$.

We can take G in the theorem to be $\Gamma(n, \mathbb{F})$. The adjoint representation $\mathrm{ad} \colon H \to \mathrm{GL}(n^2 - 1, \mathbb{F})$ or $\mathrm{GL}(\frac{n^2+n}{2}, \mathbb{F})$ is induced by conjugation action of H on the Lie algebra $\mathfrak{sl}(n, \mathbb{F}) = \{x \in \mathrm{Mat}(n, \mathbb{F}) \mid \mathrm{trace}(x) = 0\}$ or $\mathfrak{sp}(n, \mathbb{F}) = \{x \in \mathrm{Mat}(n, \mathbb{F}) \,|\, x^\top J_n = -J_n x\}$ as relevant.

To apply the Rivin density criterion, recall that we can test finiteness. Absolute irreducibility can be tested via an enveloping algebra basis.

Let $H \leq \mathrm{GL}(n, \mathbb{F})$ be finitely generated, say $H = \langle X \rangle$ where $X = X^{-1}$. Task: compute a basis for the enveloping algebra $\langle H \rangle_{\mathbb{F}}$ of H. (The latter is the smallest subalgebra of $\mathrm{Mat}(n, \mathbb{F})$ that contains H: the $\mathbb{F}$-span of H.)

Theorem (Burnside)

$H \leq \mathrm{GL}(n, \mathbb{F})$ is absolutely irreducible $\Leftrightarrow \dim(\langle H \rangle_{\mathbb{F}}) = n^2$.

A basis $\mathcal{B}$ of $\langle H \rangle_{\mathbb{F}}$ can be computed by a simple recursion. Initialize $\mathcal{B} = \{1_n\}$. While $\exists\, x \in X$ and $b \in \mathcal{B}$ s.t. $xb \notin \mathrm{span}_{\mathbb{F}}(\mathcal{B})$, do $\mathcal{B} \leftarrow \mathcal{B} \cup \{xb\}$. This recursion terminates as dimensions are $\leq n^2$. Always $\mathcal{B}$ comprises linearly independent elements of H, and at termination $H \subseteq \mathrm{span}_{\mathbb{F}}(\mathcal{B})$.

Strong approximation for linear groups

Let $R = \mathbb{Z}[1/\mu]$ for some integer $\mu \geq 1$, and let φ_m be the reduction modulo m congruence homomorphism on $\mathrm{Mat}(n, R)$, $m \in \mathbb{N}$ coprime to μ.

Note: finitely generated $H \leq \Gamma(n, \mathbb{Q})$ is contained in some $\Gamma(n, R)$.

Starting point for our discussion of strong approximation is the observation that $\varphi_m \colon \Gamma(n, R) \to \Gamma(n, \mathbb{Z}_m)$ is surjective $\forall\, m \geq 2$.

Proof. Fact: $\Gamma(n, \mathbb{Z}_m)$ is generated by *transvections*; for $\Gamma = \mathrm{SL}$ these are the $t_{i,j}$ for $i \neq j$, with 1 in position (i, j), 1s on the diagonal, 0s elsewhere. Each of these generators is the mod-m image of an element of $\Gamma(n, \mathbb{Z}) \leq \Gamma(n, R)$. □

Which finitely generated $H < \Gamma(n, R)$ have this same property $\varphi_m(H) = \Gamma(n, \mathbb{Z}_m)$, say not for all, rather for all but finitely many m?

Dense subgroups of certain connected $\mathbb{Q}$-groups have the *strong approximation property*, giving positive answers to the above question. This is a deep result. Our sole interest is the following consequence.

Strong approximation theorem (SAT)

Let H be a finitely generated dense subgroup of $\Gamma(n, \mathbb{Q})$. Then there exists a finite set $\mathcal{P}$ of primes such that $\varphi_p(H) = \Gamma(n, p)$ for all primes $p \notin \mathcal{P}$.

Subgroup growth by Lubotzky & Segal, pp. 389–398, has a proof for $H \leq \Gamma(n, R) = \mathrm{SL}(n, \mathbb{Z})$, using Matthews, Vaserstein and Weisfeiler (1984).

Indeed, from now on $\Gamma(n,R) = \mathrm{SL}(n,\mathbb{Z})$; results have superficial changes for $\mathrm{SL}(n,\mathbb{Z}[1/\mu])$ with $\mu > 1$, and adapt (using other ideas) to $\mathrm{Sp}(n,R)$.

To realize SAT computationally, we provide an algorithm to compute the set $\Pi(H)$ of 'exceptional primes' for dense $H \leq \mathrm{SL}(n,\mathbb{Z})$.

Precisely:

$$\forall \text{ primes } \ p, \ \varphi_p(H) \neq \mathrm{SL}(n,p) \iff p \in \Pi(H).$$

Our algorithm to compute $\Pi(H)$ is suggested by Matthews, Vaserstein and Weisfeiler (1984).

We use the Rivin density criterion, and proofs depend on a theorem of Aschbacher (1984) which categorizes maximal subgroups of $\mathrm{SL}(n,p)$ into eight 'geometric' classes and one 'almost simple' class (bedrock of the Matrix Group Recognition Project).

Let $\mathrm{ad}\colon \mathrm{SL}(n,\mathbb{F}) \to \mathrm{GL}(n^2-1,\mathbb{F})$ be the adjoint representation.

Theorem Λ (DFH, 2019)

There exists a function $\lambda\colon \mathbb{N} \to \mathbb{N}$ such that if $G \leq \mathrm{SL}(n,p)$, $\mathrm{ad}(G)$ is absolutely irreducible, and $|G| > \lambda(n)$, then $G = \mathrm{SL}(n,p)$.

Good estimates of $\lambda(n)$ for $n \leq 12$ have been derived from tables in Bray et al. (2013). Theorem Λ directs focus on (i) congruence image orders; (ii) adjoint absolute irreducibility.

Bounded orders

Lemma

Let $H \leq \mathrm{GL}(n, \mathbb{Z})$ be finitely generated and infinite. If $k \in \mathbb{N}$, then for almost all primes p, $\varphi_p(H)$ has an element of order greater than k.

Proof. Cf. proof of Mal'cev's result. There exists infinite-order $h \in H$ (finitely generated periodic linear groups are finite; Schur). Let m_i be the gcd of all non-zero entries of $h^i - 1_n$. If $p \nmid \mathrm{lcm}(m_1, \ldots, m_k)$, then $\varphi_p(h)^i \neq 1_n$ for $1 \leq i \leq k$; so $|\varphi_p(h)| > k$. □

For infinite $H \leq \mathrm{GL}(n, \mathbb{Z})$ and $k \in \mathbb{N}$, `PrimesForOrder`(H, k) returns all primes p such that each element of $\varphi_p(H)$ has order $\leq k$. This output obviously contains all primes p such that $|\varphi_p(H)| \leq k$.

Absolute irreducibility

Lemma

If $H \leq \mathrm{GL}(n, \mathbb{Z})$ is absolutely irreducible (over $\mathbb{Q}$), then $\varphi_p(H) \leq \mathrm{GL}(n, p)$ is absolutely irreducible for almost all primes p.

Proof. Let $\{a_1, \ldots, a_{n^2}\} \subseteq H$ be a $\mathbb{Q}$-basis of $\langle H \rangle_{\mathbb{Q}}$. Let Δ be the determinant of any matrix whose columns are the a_i (written as vectors of length n^2). Then $\varphi_p(H)$ is absolutely irreducible for all primes $p \nmid \Delta$. □

The proof furnishes a procedure `PrimesForAbsIrred` that accepts absolutely irreducible $H \leq \mathrm{SL}(n, \mathbb{Z})$, computes Δ from a basis of $\langle H \rangle_{\mathbb{Q}}$ (found by the recursive procedure given earlier), and returns all primes p such that $\varphi_p(H)$ is not absolutely irreducible.

Computing $\Pi(H)$

The following procedure accepts finitely generated dense $H \leq \mathrm{SL}(n, \mathbb{Z})$ and returns $\Pi(H)$.

```
PrimesForDense($H$)
Step 1. Take $\lambda$ as in Theorem $\Lambda$ and do
    $\mathcal{P} := \texttt{PrimesForOrder}(H, \lambda(n)) \cup \texttt{PrimesForAbsIrred}(\mathrm{ad}(H))$.
Step 2. Compute and return $\{p \in \mathcal{P} \mid \varphi_p(H) \neq \mathrm{SL}(n, p)\}$.
```

Step 1 terminates by Rivin's density theorem and subprocedure definitions. Since $\varphi_p(\mathrm{ad}(H)) = \mathrm{ad}(\varphi_p(H))$, if $p \notin \mathcal{P}$ is prime, then $\varphi_p(H) = \mathrm{SL}(n, p)$ by Theorem Λ. So $\mathcal{P} \supseteq \Pi(H)$, and step 2 weeds out spurious primes.

Another major result (Weigel, 1996), is that surjection of finitely generated $H \leq \mathrm{SL}(n, \mathbb{Z})$ onto $\mathrm{SL}(n, p)$ modulo one prime $p \geq 5$ implies that H is dense: so surjects modulo almost all primes p. Cf. Lubotzky (1999).

The next theorem is a slight extension of these facts, merging density, SAT, and 'one for almost all'.

Theorem (DFH, 2019)

The following are equivalent, for finitely generated $H \leq \mathrm{SL}(n, \mathbb{Q})$:

(i) H is dense;

(ii) H surjects onto $\mathrm{SL}(n, p)$ modulo p for almost all primes p;

(iii) H surjects onto $\mathrm{SL}(n, p)$ modulo p for some odd prime $p \nmid n$.

`PrimesForDense` yields a lower bound on p as in part (ii).

A computational drawback of `PrimesForDense` is reliance on the adjoint representation, forcing computation in degree about n^4; expensive.

We have other approaches to compute $\Pi(H)$ that avoid the adjoint. These use deeper knowledge of maximal subgroups of $\mathrm{SL}(n,p)$ in each Aschbacher class: see Bray et al. (2013).

Computations in $\mathrm{GL}(n,p)$ required by `PrimesForDense` are performed using the GAP package recog by Neunhöffer and Seress.

Our SAT algorithms have been implemented and thoroughly tested in GAP. See `https://www.math.colostate.edu/~hulpke/arithmetic.g` and, e.g., DFH (2019) for details of experiments calculating $\Pi(H)$ for various $H \leq \mathrm{SL}(n,\mathbb{Z})$, $n \leq 9$.

References

- I. Rivin, Large Galois groups with applications to Zariski density. `http://arxiv.org/abs/1312.3009v4`
- A. Lubotzky and D. Segal, *Subgroup growth*, Birkhäuser, 2003 (Window 9, pp. 389–398).
- C. R. Matthews, L. N. Vaserstein, and B. Weisfeiler, Congruence properties of Zariski-dense subgroups. I, Proc. London Math. Soc. 48 (1984).
- A. Lubotzky, One for almost all: generation of $\mathrm{SL}(n, p)$ by subsets of $\mathrm{SL}(n, \mathbf{Z})$, Contemp. Math. 243 (1999).
- T. Weigel, On the profinite completion of arithmetic groups of split type, *Lois d'algèbres et variétés algébriques (Colmar, 1991)*, Travaux en Cours 50, 1996, pages 79–101.

References (continued)

- M. Aschbacher, On the maximal subgroups of the finite classical groups Invent. Math. 76 (1984).
- J. Bray, D. F. Holt, and C. Roney-Dougal, *The maximal subgroups of the low-dimensional finite classical groups*, LMS Lecture Note Ser. 407, 2013.
- M. Neunhöffer, and Á. Seress, The GAP package recog, *Constructive recognition of permutation and matrix groups*. `https://www.gap-system.org/Packages/recog.html`
- A. S. Detinko, D. L. Flannery, and A. Hulpke, The strong approximation theorem and computing with linear groups, J. Algebra 529 (2019).