Algorithms for arithmetic groups with the congruence subgroup property

Dane Flannery; joint work with Alla Detinko
National University of Ireland, Galway

Groups St Andrews 2013

Tits alternative: a finitely generated linear group over a field $\mathbb{F}$ either is SF (solvable-by-finite), or contains a noncyclic free subgroup.

We established uniform methodology for computing in the first class of the Alternative, essentially any $\mathbb{F}$: deciding virtual properties, further computing, e.g., calculating ranks of an SF group. (See also work of Assmann and Eick, Beals.)

Computing with finitely generated linear groups that are not SF is relatively unexplored. Some fundamental algorithmic problems undecidable.

As a starting point, we restrict to arithmetic (sub)groups in the second class of the Alternative. Grunewald and Segal proved decidability of algorithmic problems for 'explicitly given' groups.

A subgroup $H \leq \mathrm{GL}(n, \mathbb{Q})$ of an algebraic group $G \leq \mathrm{GL}(n, \mathbb{C})$ defined over $\mathbb{Q}$ is arithmetic if it is commensurable with $G_{\mathbb{Z}} := G \cap \mathrm{GL}(n, \mathbb{Z})$, i.e., $H \cap G_{\mathbb{Z}}$ has finite index in both H and $G_{\mathbb{Z}}$.

Fact (Bass-Lazard-Serre, Mennicke): for $n \geq 3$, $\Gamma_n = \mathrm{SL}(n, \mathbb{Z})$ has the congruence subgroup property (CSP): $H \leq_f \Gamma_n \Leftrightarrow H$ contains some principal congruence subgroup (PCS) $\Gamma_{n,m} =$ kernel of reduction mod m surjection $\varphi_m : \Gamma_n \to \mathrm{SL}(n, \mathbb{Z}_m)$. Note: Γ_2 does not have the CSP.

(Let R be a commutative ring with 1. The kernel of the congruence homomorphism $\varphi_I : \mathrm{GL}(n, R) \to \mathrm{GL}(n, R/I)$ induced by the natural map $R \to R/I$ is called a principal congruence subgroup.)

Key idea to compute with arithmetic groups in $\mathrm{SL}(n, \mathbb{Z})$, $n \geq 3$, is to use congruence homomorphism techniques and computing with matrix groups over finite rings.

Generation of congruence subgroups

Let $t_{ij}(m)$ for $i \neq j$ denote the transvection with m in position (i, j), 1s down the main diagonal, and zeros elsewhere.

Γ_n is generated by all transvections $t_{ij} = t_{ij}(1)$.

In fact Γ_n, thus $\mathrm{SL}(n, \mathbb{Z}_m)$, is 2-generated.

Lemma. For $n \geq 3$, and any $i \neq j$, $\Gamma_{n,m} = \langle t_{ij}(m) \rangle^{\Gamma_n}$.

Lemma. A PCS of $\mathrm{SL}(n, \mathbb{Z}_m)$ for $n \geq 3$ is φ_m(a PCS of Γ_n).

Sury and Venkataramana proved that if $n \geq 3$ then $\Gamma_{n,m}$ has generating set

$$\{t_{ij}(m)^g \mid 1 \leq i < j \leq n,\, g \in \Sigma\},$$

where

$$\Sigma = \{1_n, (k,l), 1_n - 2e_{ii} - 2e_{i+1,i+1} + e_{i+1,i} \mid 1 \leq k < l \leq n,\, 1 \leq i \leq n-1\};$$

(k,l) denoting the permutation matrix obtained from 1_n by swapping rows k and l, and $e_{rs} = t_{rs} - 1_n$.

Note that the number of generators is independent of m.

It is not known whether the above is a minimal-sized generating set for $\Gamma_{n,m}$; although we know that $\Gamma'_{n,m} = \Gamma_{n,m^2}$ and $\Gamma_{n,m}/\Gamma_{n,m^2}$ has rank n^2-1, so a generating set for $\Gamma_{n,m}$ has size $\geq n^2-1$.

Maximal congruence subgroups

Let $n \geq 3$.

Lemma. $H \leq_f \mathrm{GL}(n, \mathbb{Z})$ contains a unique maximal PCS (of Γ_n); i.e., $\exists$ unique $m > 0$ such that $\Gamma_{n,m} \leq H$, and $\Gamma_{n,k} \leq H \Rightarrow \Gamma_{n,k} \leq \Gamma_{n,m}$.

Note that $\Gamma_{n,m_1} \leq \Gamma_{n,m_2} \Leftrightarrow m_2$ divides m_1.

Corollary. Each subgroup of $\mathrm{GL}(n, \mathbb{Z}_m)$ contains a (perhaps trivial) unique maximal PCS of $\mathrm{SL}(n, \mathbb{Z}_m)$.

Subnormality

For $R = \mathbb{Z}$ or $\mathbb{Z}_m$, let $Z_{n,k}$ denote the inverse image of the scalars of $\mathrm{GL}(n, R/kR)$ in $\mathrm{GL}(n, R)$ under φ_k.

The level $\ell(h)$ of $h = [h_{ij}]_{ij} \in \mathrm{GL}(n, R)$ is the ideal of R generated by

$$\{h_{ij} \mid i \neq j,\, 1 \leq i, j \leq n\} \cup \{h_{ii} - h_{jj} \mid 1 \leq i, j \leq n\}.$$

Then $\ell(A) := \sum_{a \in A} \ell(a)$ for $A \subseteq \mathrm{GL}(n, R)$.

Theorem (J. S. Wilson). For $n \geq 3$, $H \leq \mathrm{GL}(n, R)$ is subnormal if and only if

$$\Gamma_{n,k^e} \leq H \leq Z_{n,k} \qquad (\dagger)$$

for some k, $e > 0$. If $(\dagger)$ holds then $e \geq d - 1$ where d is the depth of H; and the least possible e is bounded above by a function of n and d only.

As special cases we obtain

Proposition. Suppose that $H \leq \widehat{\Gamma}_n = \mathrm{GL}(n, R)$ has level l. Then

$$\Gamma_{n,l} \leq H^{\widehat{\Gamma}_n} = \langle H, \Gamma_{n,l} \rangle \leq Z_{n,l}.$$

Corollary. $H \trianglelefteq \widehat{\Gamma}_n$ if and only if $\ell(H)$ is the level of the maximal PCS in H.

Lemma. $H \leq \Gamma_n = \mathrm{SL}(n, R)$ is normal in Γ_n precisely when it is normal in $\widehat{\Gamma}_n$: $H^{\Gamma_n} = H^{\widehat{\Gamma}_n}$.

Note: if $H = \langle S \rangle$ then $\ell(H) = \ell(S)$.

Let $m = p_1^{k_1} \cdots p_t^{k_t}$ where the p_i are distinct primes and $k_i \geq 1$.

Define a ring isomorphism $\chi : \mathbb{Z}_m \to \mathbb{Z}_{p_1^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{k_t}}$ by

$$\chi(a) = (a_1, \ldots, a_t), \qquad a_i \equiv a \bmod p_i^{k_i}.$$

Proposition.

(i) χ extends to isomorphisms $\mathrm{GL}(n, \mathbb{Z}_m) \to \times_{i=1}^{t} \mathrm{GL}\left(n, \mathbb{Z}_{p_i^{k_i}}\right)$ and $\mathrm{SL}(n, \mathbb{Z}_m) \to \times_{i=1}^{t} \mathrm{SL}\left(n, \mathbb{Z}_{p_i^{k_i}}\right)$.

(ii) Let $I = \langle a \rangle$ be an ideal of $\mathbb{Z}_m$, and let I_i be the ideal of $\mathbb{Z}_{p_i^{k_i}}$ generated by $a_i \equiv a \bmod p_i^{k_i}$. Denote by K_I, K_{I_i} the kernels of φ_I, φ_{I_i} on $\mathrm{GL}(n, \mathbb{Z}_m)$, $\mathrm{GL}\left(n, \mathbb{Z}_{p_i^{k_i}}\right)$ respectively. Then

- $\chi(K_I) = \times_{i=1}^{t} K_{I_i}$;
- $\chi(K_I \cap \mathrm{SL}(n, \mathbb{Z}_m)) = \times_{i=1}^{t} (K_{I_i} \cap \mathrm{SL}(n, \mathbb{Z}_m))$.

To answer computational questions about $H \leq \mathrm{GL}(n, \mathbb{Z}_{p^k})$, consider $\varphi_p : \mathrm{GL}(n, \mathbb{Z}_{p^k}) \rightarrow \mathrm{GL}(n, p)$.

Approach is then twofold: computing with $\varphi_p(H)$ in $\mathrm{GL}(n, p)$, and computing in the finite nilpotent group (p-group) $\ker \varphi_p \cap H$.

We take advantage of efficient algorithms available for both cases.

This yields algorithms to, e.g.,

- test membership
- construct presentations
- test subnormality and bound depth
- test solvability, nilpotency etc.

for subgroups of $\mathrm{GL}(n, \mathbb{Z}_m)$.

Let H be a finitely generated subgroup of $\Gamma_n = \mathrm{SL}(n, \mathbb{Z})$, $n \geq 3$.

Vital assumption: H contains some $\Gamma_{n,m}$ for known m.

We apply the menu of algorithms for computing with subgroups of $\varphi_m(\Gamma_n) = \mathrm{SL}(n, \mathbb{Z}_m)$, and established knowledge of PCS in Γ_n.

Some procedures straightforward, e.g.;

- `IsSubgroup`(L, H): for finitely generated $L \leq \Gamma_n$, returns `true` if and only if $\varphi_m(L) \leq \varphi_m(H)$.
- `Normalizer`(H) returns $N_{\Gamma_n}(H)$, which is the full preimage in Γ_n of $N_{\mathrm{SL}(n,\mathbb{Z}_m)}(\varphi_m(H))$.

Theorem. If $\Gamma_{n,r}$ is the maximal PCS in H, then $\varphi_m(\Gamma_{n,r})$ is the maximal PCS in $\varphi_m(H)$.

$\mathtt{IsSubnormal}(H)$

Output: `true` and an upper bound d on its depth if H is subnormal in Γ_n; `false` otherwise.

1. $l_1 := \mathtt{Level}(H)$, $l_2 := \mathtt{Level}(\mathtt{MaxPCS}(H))$.
2. If $\nexists\, e$ such that $l_2 \big| l_1^e$ then return `false`, else return `true` and $d := e' + 1$ where $e' :=$ least e such that $l_2 \big| l_1^e$.

$\mathtt{IsNormal}(H)$ returns `true` iff $l_2 = l_1$.