Computing with finitely generated linear groups: foundations

Dane Flannery (NUI Galway, Ireland); joint work with Alla Detinko, Alexander Hulpke, Eamonn O’Brien

*Computational Aspects of Discrete Subgroups of Lie Groups*, June 2021
A *linear group* (aka *matrix group*) is a subgroup of some $\text{GL}(n, F)$, $F$ field. Linear groups are well suited to calculation and offer a concise way to work with (abstract) groups and related objects.

But there are serious obstacles to practical computing with linear groups over infinite $F$:

- **undecidability**, or lack of knowledge of decidability

- **computational complexity**; e.g., uncontrollable growth of entries during matrix multiplication.

Also, formerly a dearth of methods.

Nonetheless, linear groups over infinite $F$ occur often in applications. We want to compute effectively (symbolically) with these groups.
This talk is a brief look at foundations of an ongoing project to compute with finitely generated $G \leq \text{GL}(n, \mathbb{F})$.

Goals:

(i) Practical methodology applicable to any $\mathbb{F}$ and (finitely generated) input $G$.

(ii) Use of (i) to design and implement effective algorithms.

Implementations are available as part of the systems Magma and GAP. Sometimes these prove decidability of problems, for the first time.

N.B.: computing with matrix groups over finite fields is very well-established: the ‘Matrix Group Recognition Project’. 
Finite approximation

Fix notation: $G = \langle S \rangle \leq \text{GL}(n, \mathbb{F})$ finitely generated; $R$ is the subring of $\mathbb{F}$ generated by the entries of all $g \in S \cup S^{-1}$.

$R$ is a finitely generated integral domain and $G \leq \text{GL}(n, R)$.

Quotient fields of $R$ are finite.

**Lemma**

For each non-zero element $a$ of $R$, there exists a maximal ideal $\rho$ of $R$ such that $a \notin \rho$.

Thus $R$ is ‘approximated’ by finite fields: $R$ is residually a finite field. (If $\text{char } R = 0$ then $\text{char}(R/\rho)$ runs over almost all primes.)
If \( \rho \subset R \) is an ideal, then \( \varphi_\rho \) denotes the reduction modulo \( \rho \) congruence homomorphism \( R \to R/\rho \) on \( R \), and (by entrywise extension) on subsets of \( \text{Mat}(n, R) \). Also \( \varphi_\rho : \text{GL}(n, R) \to \text{GL}(n, R/\rho) \).

Mal’cev proved (uses lemma above):

**Theorem (Mal’cev)**

If \( g_1, \ldots, g_r \in \text{Mat}(n, R) \) are pairwise distinct, then \( \exists \) maximal ideal \( \rho \) of \( R \) such that \( \varphi_\rho(g_1), \ldots, \varphi_\rho(g_r) \in \text{Mat}(n, R/\rho) \) are pairwise distinct.

Therefore, finitely generated linear groups are residually finite.

Moreover, each finitely generated matrix group is approximated by matrix groups of the same degree over finite fields.
Theorem (Noether normalization)

Let $\mathbb{F}$ be finitely generated as a field, and let $\mathbb{E}$ be its prime subfield. There exist $\mathbb{E}$-algebraically independent elements $\xi_1, \ldots, \xi_m$ of $\mathbb{F}$, $m \geq 0$, such that $\mathbb{F}$ is a finite extension of the function field $\mathbb{E}(\xi_1, \ldots, \xi_m)$.

So ‘any $\mathbb{F}$’ really means one of the following (determined by $G$):

- an algebraic number field $\mathbb{P}$;
- an algebraic function field, i.e., finite extension of $\mathbb{E}(x_1, \ldots, x_m)$, $\mathbb{E} = \mathbb{F}_q$ or $\mathbb{P}$.

Such fields are supported by MAGMA, GAP. Our algorithms have been designed for such fields.
Computational finite approximation: constructing congruence homomorphisms

After defining $G$ over a field $\mathbb{F}$ containing $R$ that we can compute with, we apply congruence homomorphisms $\varphi_\rho$ for (maximal) ideals $\rho \subseteq R$.

Our computational duties then split in two: computing with $\varphi_\rho(G) \leq \text{GL}(n, R/\rho)$; computing with the congruence subgroup $G_\rho := G \cap \ker \varphi_\rho$.

$\varphi_\rho(G)$ is a matrix group over a finite field. We hand it to MGRP.

Although $G_\rho$ is finitely generated, computing a generating set of $G_\rho$ is out. Instead, we only need to compute ‘normal generators’ for $G_\rho$.
That is enough to find an enveloping algebra of $G_\rho$ in $\text{Mat}(n, \mathbb{F})$, which is enough to detect properties of $G_\rho$ of interest.
Normal subgroup generators

**Lemma**

Let $H$ be finitely generated, say $H = \langle h_1, \ldots, h_s \rangle$, and let $f : H \to K$ be a homomorphism such that $f(H) \leq K$ has a presentation

$$\langle \bar{h}_1, \ldots, \bar{h}_s \mid \mathcal{R} \rangle$$

where $\bar{h}_i := f(h_i)$ and $\mathcal{R} = \{ w_1(\bar{h}_1, \ldots, \bar{h}_s), \ldots, w_k(\bar{h}_1, \ldots, \bar{h}_s) \}$. Then $\ker f$ is the normal closure

$$\langle w_1(h_1, \ldots, h_s), \ldots, w_k(h_1, \ldots, h_s) \rangle^H.$$

Note the required format of the image presentation.
So, to handle $G_\rho$, we want a presentation for $\varphi_\rho(G) = \langle \varphi_\rho(S) \rangle$, say in $\text{GL}(n, q)$, of the required format.

Effecting congruence homomorphisms $\varphi_\rho$ is straightforward in practice. The main operations are

- reduction modulo rational primes;
- substitution for indeterminates in function fields.
Several aspects enhance efficiency of our algorithms, e.g.:

- transferring matrix algebra as much as possible to congruence images (over a finite field—ameliorate entry explosion);
- use of ‘short presentations’ in $\text{GL}(n, q)$;
- replacement of computation in the input group over infinite $\mathbb{F}$ by computation in related matrix algebras over $\mathbb{F}$. 
Application I: deciding finiteness

In applications of computational finite approximation, we need to find special ideals $\rho$ for congruence homomorphisms $\varphi_\rho$. The kind of $\rho$ sought is determined by the specific problem considered.

Theorem (Selberg–Wehrfritz)

Each finitely generated linear group $G$ has a normal subgroup $N$ of finite index whose finite order elements are all unipotent.

In particular, if $\text{char } F = 0$, then $G$ is (torsion-free)-by-finite.

When $N$ is a congruence subgroup $G_\rho$ for maximal $\rho$ in $R$, we call $\varphi_\rho$ an SW-homomorphism.

Proof of the Selberg–Wehrfritz theorem does not give $N$ as a $G_\rho$. 
Theorem

Let $\Delta$ be a Noetherian integral domain, and let $\rho$ be a maximal ideal of $\Delta$. If $g \in \text{GL}(n, \Delta) \cap \ker \varphi_{\rho}$ has finite order, then $|g|$ is a power of $\text{char}(\Delta/\rho)$.

So, if $\text{char} \mathbb{F} > 0$ and $\rho$ is any maximal ideal of $R$, then $\varphi_{\rho}$ is an SW-homomorphism. For $\text{char} \mathbb{F} = 0$ we have other results, enabling construction of SW-homomorphisms for all types of $\mathbb{F}$.

In summary:

Theorem (Finiteness Criteria)

Let $\varphi_{\rho}$ be an SW-homomorphism on $G \leq \text{GL}(n, R)$.

(i) Suppose that $\text{char} R = 0$. Then $G$ is finite $\iff$ $G_{\rho} = \{1_n\}$.

(ii) Suppose that $\text{char} R = p > 0$. Then $G$ is finite $\iff$ $G_{\rho}$ is a finite $p$-group (i.e., is unipotent).
IsFinite($S$)

Input: a finite subset $S$ of $\text{GL}(n, R)$, $\text{char } R = p \geq 0$.
Output: true if $G = \langle S \rangle$ is finite; false otherwise.

1. Select SW-homomorphism $\varphi_{\rho}$ and compute $\varphi_{\rho}(G) \leq \text{GL}(n, q)$, $|R/\rho| = q$.
2. $N := \text{NormalGenerators}(S, \varphi_{\rho})$.
3. If $p = 0$ and $N = \{1_n\}$,
   or $p > 0$ and $\langle N \rangle^G$ is unipotent,
   then return true;
   else return false.

Note: step 3 for $p > 0$ is a matrix algebra computation, using the output of step 2 (the full normal closure $G_\rho$ of $\langle N \rangle$ cannot be computed directly by a standard recursion).
Application II: deciding virtual properties

To decide the Tits class of $G$, i.e., to test whether $G$ is virtually solvable (solvable-by-finite, SF), we rely on a theorem by Mal’cev–Lie–Kolchin: an SF linear group has a unipotent-by-abelian (i.e., triangularizable) normal subgroup of finite index.

Recall that by Tits’ theorem, if $G$ is not SF then it contains a non-abelian free subgroup $F$; our algorithm doesn’t produce such $F$.

Our approach is different to previous ones (over $\mathbb{Q}$, by Beals, Dixon, Assmann & Eick); again, uniform and works over any $\mathbb{F}$.

Relies on criteria by Wehrfritz for $G_\rho$ to be unipotent-by-abelian if $G$ is SF.
Theorem (Wehrfritz, 2010)

Let $G \leq \text{GL}(n, R)$ be solvable-by-finite, and let $\rho$ an ideal of $R$. Then $G_\rho$ is unipotent-by-abelian if

(i) $R/\rho$ has prime characteristic greater than $n$; or

(ii) $R$ is a Dedekind domain of characteristic zero, $\rho$ is a maximal ideal of $R$, $\text{char}(R/\rho) = p > 2$, and $p \not\in \rho^{p-1}$.

$G_\rho$ in (ii) is Zariski-connected.

If $\rho$ is an ideal of $R$ such that $G_\rho$ is unipotent-by-abelian for SF $G \leq \text{GL}(n, R)$, then we call $\varphi_\rho$ a $W$-homomorphism. Just as for SW-homomorphisms, we can construct $W$-homomorphisms for all main types of $\mathbb{F}$. 

IsSolvableByFinite($S$)

Input: finite $S \subseteq \text{GL}(n, R)$.
Output: true if $G = \langle S \rangle$ is solvable-by-finite; false otherwise.

1. Select $\rho \subseteq R$ such that $\phi_\rho$ is a $W$-homomorphism, and compute $\phi_\rho(G)$.
2. $N := \text{NormalGenerators}(S, \phi_\rho)$.
3. Return true if $\langle N \rangle^G$ is unipotent-by-abelian; else return false.

Step 3 is again an enveloping algebra computation.

We test other virtual properties: roughly, $G$ is $X$-by-finite (for $X \in \{\text{nilpotent, abelian, central}\}$) $\iff$ $W$-congruence subgroup $G_\rho$ is $X$. 
Software

Much of the preceding has been implemented; joint work with Eamonn O’Brien.

Procedures are available in releases of Magma. See

https://magma.maths.usyd.edu.au/magma/handbook/matrix_groups_over_infinite_fields
From finite to strong approximation

To answer questions in the first Tits class, one maximal ideal suffices.

But ‘most’ linear groups are not solvable-by-finite.

The next phase is computing with dense subgroups of algebraic groups. Here, need more than one ideal & typically not maximal.

Ongoing work with Alla Detinko and Alexander Hulpke.

Much more detail in: Expositiones Mathematicae 37:4, 2019, 454–484.
http://www.maths.nuigalway.ie/~dane/Expositiones.pdf