Towards efficient computing with matrix groups over infinite domains

Alla Detinko (joint work with Dane Flannery)

National University of Ireland, Galway

CGAC, Columbus, 21-25 March 2010

1. Preliminaries: finitely generated linear groups

Given $S = \{g_1, \ldots, g_r\}$, $g_i \in GL(n, F)$, $1 \leq i \leq r$, F is a field.

Let $G = \langle S \rangle$. Then $G \subseteq GL(n, R)$ for a finitely generated integral domain $R \subseteq F$ defined by entries of matrices in $S \cup S^{-1}$.

Lemma. R is 'approximated' by finite fields, i.e.

- for each maximal ideal ρ of R, R/ρ is a finite field;
- the intersection of maximal ideals of R is zero.

Theorem. The group G is residually finite. Moreover, G is approximated by matrix groups of degree n over finite fields.

Theorem (Selberg). The group G contains a normal subgroup N of finite index such that torsion elements of N are unipotent. In particular, if $\mathrm{char}\, F = 0$ then N is torsion-free.

Definition. We will call subgroups of G satisfying the Selberg Theorem 'Selberg subgroups'.

2 Computing with finitely generated linear groups

2.1 Congruence homomorphism techniques

Given an ideal $\rho \subseteq R$, define the congruence homomorphism $\varphi_\rho : GL(n, R) \to GL(n, R/\rho)$.

Notation

- $\ker \varphi_\rho := \Gamma_\rho$ (principal congruence subgroup).
- $G \cap \Gamma_\rho := G_\rho$ (congruence subgroup).

Method: Reduction to finite fields via construction of a congruence homomorphism φ_ρ such that Γ_ρ is a Selberg subgroup.

2.2 Selberg congruence subgroups

Lemma. Each torsion element of Γ_ρ is a p-element, where $p = \mathrm{char}(R/\rho)$.

Corollary.

- If $\mathrm{char}(R/\rho) = 0$ then Γ_ρ is torsion-free.
- If $\mathrm{char}\, R = p > 0$ then each torsion element of Γ_ρ is unipotent.

Lemma. Let R be a Dedekind domain, $\mathrm{char}\, R = 0$, $\rho \subseteq R$ be an ideal, $\mathrm{char}(R/\rho) = p > 2$. If $p \notin \rho^2$ then Γ_ρ is torsion-free.

2.3 Main domains

Lemma. For a subfield $\mathbb{P} \subseteq F$ there exist $x_1, \ldots, x_m \in F$ $(m \geq 0)$ algebraically independent over $\mathbb{P}$ such that F is a finite extension of $\mathbb{P}(x_1, \ldots, x_m)$.

Examples: main domains

1. $\mathbb{Q}$ and algebraic number fields.
2. $L = \mathbb{P}(x_1, \ldots, x_m)$, $\mathbb{P}$ is a number field or $\mathbb{F}_q$.
3. A finite extension of L.

Examples: congruence homomorphisms

Notation. For an integral domain A and $\mu \in A \setminus \{0\}$, $\frac{1}{\mu}A$ is the ring of fractions with denominators in the monoid $\langle \mu \rangle \subseteq A$.

Let $F = \mathbb{Q}$. Then $R = \frac{1}{c}\mathbb{Z}$, $c \in \mathbb{Z}$. Define $\rho = p\mathbb{Z}$, $p \neq 2$, $p \nmid c$. Then $\varphi_\rho(G) \subseteq GL(n, p)$ and G_ρ is *torsion-free*.

Let $F = \mathbb{P}(x_1, \ldots, x_m)$, $\mathbb{P} = \mathbb{Q}$ or $\mathbb{F}_p$. Then $R = \frac{1}{\mu}\mathbb{P}[x_1, \ldots, x_m]$, $\mu = \mu(x_1, \ldots, x_m) \in \mathbb{P}[x_1, \ldots, x_m]$. Define $\rho = \langle (x_1 - \alpha_1), \ldots, (x_m - \alpha_m) \rangle$ for some α_i such that $\mu(\alpha_1, \ldots, \alpha_m) \neq 0$.

- If $\mathbb{P} = \mathbb{Q}$ then $\alpha_i \in \mathbb{Q}$, $\varphi_\rho(G) \subseteq GL(n, \mathbb{Q})$, and G_ρ is *torsion-free*.
- If $\mathbb{P} = \mathbb{F}_p$ then $\alpha_i \in \bar{\mathbb{F}}_p$, $\varphi_\rho(G) \subseteq GL(n, \mathbb{F}_{p^t})$, and torsion elements of G_ρ are *p-elements*.

Remark. $\mathbb{Q}$ and $\mathbb{F}_p$ can be replaced by finite extensions.

Conclusion.

(i) A Selberg congruence subgroup always exists;
(ii) We can always construct $\rho \subseteq R$ such that Γ_ρ is a Selberg subgroup.

Convention. In what follows Γ_ρ is always a Selberg subgroup.

3. Deciding finiteness and related problems

3.1 Preliminaries

• Kopytov (1968): the finiteness problem is decidable for matrix groups over $\mathbb{Q}$.

• Babai, Beals and Rockmore (1993): algorithms for deciding finiteness for matrix groups over $\mathbb{Q}$, based on Burnside's finiteness criteria.

• Ivanyos (2001); Rockmore, Tan, Beals (1999): deciding finiteness for matrix groups over function fields.

3.2 Deciding finiteness and Selberg congruence homomorphisms

Lemma.

- Let $\mathrm{char}\, F = 0$. Then G is finite if and only if G_ρ is trivial.
- Let $\mathrm{char}\, F = p > 0$. Then G is finite if and only if G_ρ is a p-group.

`IsFinite` $[\mathrm{char}\, F = 0]$

1. Construct $\varphi_\rho(G) \subseteq GL(n, q)$.
2. Test whether G_ρ is trivial.

`IsFinite` $[\mathrm{char}\, F = p > 0]$

1. Construct $\varphi_\rho(G) \subseteq GL(n, q)$.
2. Test whether G_ρ is unipotent.

3.3 Deciding finiteness: special methods and cases

Applying presentations

1. Find a presentation of $\varphi_\rho(G)$ and a list K of 'normal generators' of G_ρ.
2. Test whether $K = \{1_n\}$ if $\operatorname{char} F = 0$, and $\langle K \rangle^G$ is unipotent otherwise.

Function fields: scheme

`IsFinite` $[F = \mathbb{P}(x_1, \ldots, x_m), \mathbb{P} = \mathbb{Q}$ or $\mathbb{F}_q]$

1. Construct $\varphi_\rho(G) \subseteq GL(n, \mathbb{Q})$ (resp. $GL(n, \mathbb{F}_{p^t})$).
2. Test whether $\varphi_\rho(G)$ is finite (if $\operatorname{char} \mathbb{P} = 0$).
3. Compare $\dim \langle G \rangle_{\mathbb{P}}$ and $\dim \langle \varphi_\rho(G) \rangle_{\mathbb{P}}$.

Remark. Step 3 does not require computing a basis of $\langle G \rangle_{\mathbb{P}}$, and most of the computing is performed over $\mathbb{Q}$ (resp. a finite field) rather than over F.

References

- A. Detinko, D. Flannery, J. Symbolic Comp 44 (2009), 1037–1043.
- AD, DF, E. O'Brien, J. Algebra 311 (2009), 4151–4160.
- AD, DF, EO'B, Implementation in Magma v2.16 (2009).

3.4 Related algorithms

Lemma. Let $G \subseteq GL(n, R)$, G finite. Then there exists a maximal ideal ρ of R such that $G \cong \varphi_\rho(G)$, $\varphi_\rho(G) \subseteq GL(n, q)$.

Conclusion: for a finite subgroup of $GL(n, F)$ one can construct an isomorphic copy in $GL(n, q)$.

Applications: computing the order of G; structural investigation of G via algorithms for matrix groups over finite fields.

4 Conclusion: further algorithms

4.1 Nilpotency testing and computing with nilpotent matrix groups over infinite fields

Method:
(i) Semisimple splitting.
(ii) Selberg congruence homomorphism.
(iii) Nilpotency testing and construction of a presentation of the congruence image.

Details:
- A. Detinko, D. Flannery, J. Symbolic Comput. 43 (2008), 8 –26.
- B. Eick, AD, DF, GAP package *Nilmat*: implementation over $\mathbb{Q}$.
- E. O'Brien, AD, DF, implementation over $\mathbb{Q}$, number fields, function fields etc., in Magma v2.16.

4.2 Other algorithms

State-of-the-art, further algorithms, open problems, solutions and methods: see the survey

A. Detinko, B. Eick, D. Flannery 'Computing with matrix groups over infinite fields', London Mathematical Society Lecture Note Series, to appear.

`http://larmor.nuigalway.ie/~detinko/DEF_survey.pdf`