

Deciding finiteness of matrix groups

Dane Flannery (joint work with Alla Detinko & Eamonn O'Brien)

National University of Ireland, Galway

Edinburgh, July 30, 2009

Introduction

Introduction

Deciding finiteness is a fundamental computational problem for any class of potentially infinite groups.

Introduction

Deciding finiteness is a fundamental computational problem for any class of potentially infinite groups.

While not decidable in general, this problem is decidable for finitely generated matrix groups over a field.

Introduction

Deciding finiteness is a fundamental computational problem for any class of potentially infinite groups.

While not decidable in general, this problem is decidable for finitely generated matrix groups over a field.

We provide practical algorithms for deciding finiteness of matrix groups, that have been implemented (in MAGMA), perform well for a range of input, and are publicly available.

Introduction

Deciding finiteness is a fundamental computational problem for any class of potentially infinite groups.

While not decidable in general, this problem is decidable for finitely generated matrix groups over a field.

We provide practical algorithms for deciding finiteness of matrix groups, that have been implemented (in MAGMA), perform well for a range of input, and are publicly available.

The main technique is classical: change of the ground domain via *congruence* (or *Minkowski*) *homomorphism*.

Key: deciding finiteness over function fields.

Key: deciding finiteness over function fields.

Lemma Let G be a finitely generated subgroup of $GL(n, \mathbb{F})$, \mathbb{F} any field.

Key: deciding finiteness over function fields.

Lemma Let G be a finitely generated subgroup of $GL(n, \mathbb{F})$, \mathbb{F} any field. Then $G \leq GL(n, \mathbb{E})$ for some finite extension \mathbb{E} of a function field over the prime subfield of \mathbb{F} .

Key: deciding finiteness over function fields.

Lemma Let G be a finitely generated subgroup of $GL(n, \mathbb{F})$, \mathbb{F} any field. Then $G \leq GL(n, \mathbb{E})$ for some finite extension \mathbb{E} of a function field over the prime subfield of \mathbb{F} .

Note that if \mathbb{K}/\mathbb{L} is a finite field extension of degree l , then a subgroup of $GL(n, \mathbb{K})$ is isomorphic to a subgroup of $GL(nl, \mathbb{L})$.

Key: deciding finiteness over function fields.

Lemma Let G be a finitely generated subgroup of $GL(n, \mathbb{F})$, \mathbb{F} any field. Then $G \leq GL(n, \mathbb{E})$ for some finite extension \mathbb{E} of a function field over the prime subfield of \mathbb{F} .

Note that if \mathbb{K}/\mathbb{L} is a finite field extension of degree l , then a subgroup of $GL(n, \mathbb{K})$ is isomorphic to a subgroup of $GL(nl, \mathbb{L})$.

Therefore, if we can decide finiteness of f.g. matrix groups over

Key: deciding finiteness over function fields.

Lemma Let G be a finitely generated subgroup of $GL(n, \mathbb{F})$, \mathbb{F} any field. Then $G \leq GL(n, \mathbb{E})$ for some finite extension \mathbb{E} of a function field over the prime subfield of \mathbb{F} .

Note that if \mathbb{K}/\mathbb{L} is a finite field extension of degree l , then a subgroup of $GL(n, \mathbb{K})$ is isomorphic to a subgroup of $GL(nl, \mathbb{L})$.

Therefore, if we can decide finiteness of f.g. matrix groups over

- $\mathbb{Q}(X_1, \dots, X_m)$ for $m \geq 0$;

Key: deciding finiteness over function fields.

Lemma Let G be a finitely generated subgroup of $GL(n, \mathbb{F})$, \mathbb{F} any field. Then $G \leq GL(n, \mathbb{E})$ for some finite extension \mathbb{E} of a function field over the prime subfield of \mathbb{F} .

Note that if \mathbb{K}/\mathbb{L} is a finite field extension of degree l , then a subgroup of $GL(n, \mathbb{K})$ is isomorphic to a subgroup of $GL(nl, \mathbb{L})$.

Therefore, if we can decide finiteness of f.g. matrix groups over

- $\mathbb{Q}(X_1, \dots, X_m)$ for $m \geq 0$;
- $\mathbb{Z}_p(X_1, \dots, X_m)$ for $m > 0$;

Key: deciding finiteness over function fields.

Lemma Let G be a finitely generated subgroup of $GL(n, \mathbb{F})$, \mathbb{F} any field. Then $G \leq GL(n, \mathbb{E})$ for some finite extension \mathbb{E} of a function field over the prime subfield of \mathbb{F} .

Note that if \mathbb{K}/\mathbb{L} is a finite field extension of degree l , then a subgroup of $GL(n, \mathbb{K})$ is isomorphic to a subgroup of $GL(nl, \mathbb{L})$.

Therefore, if we can decide finiteness of f.g. matrix groups over

- $\mathbb{Q}(X_1, \dots, X_m)$ for $m \geq 0$;
- $\mathbb{Z}_p(X_1, \dots, X_m)$ for $m > 0$;

then (subject to special representation of input) we can decide finiteness of matrix groups defined over any field.

History

History

Zero characteristic

History

Zero characteristic

Over \mathbb{Q} : Babai, Beals & Rockmore (1993).

History

Zero characteristic

Over \mathbb{Q} : Babai, Beals & Rockmore (1993).

Over function fields: Rockmore, Tan & Beals (1999).

History

Zero characteristic

Over \mathbb{Q} : Babai, Beals & Rockmore (1993).

Over function fields: Rockmore, Tan & Beals (1999).

Over function fields: Detinko & Flannery (2008).

History

Zero characteristic

Over \mathbb{Q} : Babai, Beals & Rockmore (1993).

Over function fields: Rockmore, Tan & Beals (1999).

Over function fields: Detinko & Flannery (2008).

Positive characteristic

History

Zero characteristic

Over \mathbb{Q} : Babai, Beals & Rockmore (1993).

Over function fields: Rockmore, Tan & Beals (1999).

Over function fields: Detinko & Flannery (2008).

Positive characteristic

Rockmore, Tan & Beals (1999).

History

Zero characteristic

Over \mathbb{Q} : Babai, Beals & Rockmore (1993).

Over function fields: Rockmore, Tan & Beals (1999).

Over function fields: Detinko & Flannery (2008).

Positive characteristic

Rockmore, Tan & Beals (1999).

Ivanyos (2001).

History

Zero characteristic

Over \mathbb{Q} : Babai, Beals & Rockmore (1993).

Over function fields: Rockmore, Tan & Beals (1999).

Over function fields: Detinko & Flannery (2008).

Positive characteristic

Rockmore, Tan & Beals (1999).

Ivanyos (2001).

Detinko (2001).

History

Zero characteristic

Over \mathbb{Q} : Babai, Beals & Rockmore (1993).

Over function fields: Rockmore, Tan & Beals (1999).

Over function fields: Detinko & Flannery (2008).

Positive characteristic

Rockmore, Tan & Beals (1999).

Ivanyos (2001).

Detinko (2001).

Detinko, Flannery & O'Brien (preprint, 2009).

Preliminaries

Preliminaries

Let $\mathbb{F} = \mathbb{E}(X_1, \dots, X_m)$, \mathbb{E} a number field or finite field \mathbb{F}_q , $m \geq 1$.

Preliminaries

Let $\mathbb{F} = \mathbb{E}(X_1, \dots, X_m)$, \mathbb{E} a number field or finite field \mathbb{F}_q , $m \geq 1$.

Let $G = \langle \mathcal{S} \rangle$, $\mathcal{S} = \{S_1, \dots, S_r\} \subseteq \text{GL}(n, \mathbb{F})$.

Preliminaries

Let $\mathbb{F} = \mathbb{E}(X_1, \dots, X_m)$, \mathbb{E} a number field or finite field \mathbb{F}_q , $m \geq 1$.

Let $G = \langle \mathcal{S} \rangle$, $\mathcal{S} = \{S_1, \dots, S_r\} \subseteq \text{GL}(n, \mathbb{F})$.

Then $G \leq \text{GL}(n, R)$,

Preliminaries

Let $\mathbb{F} = \mathbb{E}(X_1, \dots, X_m)$, \mathbb{E} a number field or finite field \mathbb{F}_q , $m \geq 1$.

Let $G = \langle \mathcal{S} \rangle$, $\mathcal{S} = \{S_1, \dots, S_r\} \subseteq \text{GL}(n, \mathbb{F})$.

Then $G \leq \text{GL}(n, R)$, $R = \frac{1}{f} \mathbb{E}[X_1, \dots, X_m]$,

Preliminaries

Let $\mathbb{F} = \mathbb{E}(X_1, \dots, X_m)$, \mathbb{E} a number field or finite field \mathbb{F}_q , $m \geq 1$.

Let $G = \langle \mathcal{S} \rangle$, $\mathcal{S} = \{S_1, \dots, S_r\} \subseteq \text{GL}(n, \mathbb{F})$.

Then $G \leq \text{GL}(n, R)$, $R = \frac{1}{f} \mathbb{E}[X_1, \dots, X_m]$, where $f = f(X_1, \dots, X_m)$ is the l.c.m. of denominators of the non-zero entries of S_i and S_i^{-1} , $1 \leq i \leq r$.

Preliminaries

Let $\mathbb{F} = \mathbb{E}(X_1, \dots, X_m)$, \mathbb{E} a number field or finite field \mathbb{F}_q , $m \geq 1$.

Let $G = \langle \mathcal{S} \rangle$, $\mathcal{S} = \{S_1, \dots, S_r\} \subseteq \text{GL}(n, \mathbb{F})$.

Then $G \leq \text{GL}(n, R)$, $R = \frac{1}{f} \mathbb{E}[X_1, \dots, X_m]$, where $f = f(X_1, \dots, X_m)$ is the l.c.m. of denominators of the non-zero entries of S_i and S_i^{-1} , $1 \leq i \leq r$.

Say $\alpha = (\alpha_1, \dots, \alpha_m) \in \mathbb{E}^{(m)}$ is \mathcal{S} -admissible if $f(\alpha) \neq 0$.

Preliminaries

Let $\mathbb{F} = \mathbb{E}(X_1, \dots, X_m)$, \mathbb{E} a number field or finite field \mathbb{F}_q , $m \geq 1$.

Let $G = \langle \mathcal{S} \rangle$, $\mathcal{S} = \{S_1, \dots, S_r\} \subseteq \text{GL}(n, \mathbb{F})$.

Then $G \leq \text{GL}(n, R)$, $R = \frac{1}{f} \mathbb{E}[X_1, \dots, X_m]$, where $f = f(X_1, \dots, X_m)$ is the l.c.m. of denominators of the non-zero entries of S_i and S_i^{-1} , $1 \leq i \leq r$.

Say $\alpha = (\alpha_1, \dots, \alpha_m) \in \mathbb{E}^{(m)}$ is \mathcal{S} -admissible if $f(\alpha) \neq 0$.

Note: when \mathbb{E} is finite, $\mathbb{E}^{(m)}$ may not contain admissible α ;

Preliminaries

Let $\mathbb{F} = \mathbb{E}(X_1, \dots, X_m)$, \mathbb{E} a number field or finite field \mathbb{F}_q , $m \geq 1$.

Let $G = \langle \mathcal{S} \rangle$, $\mathcal{S} = \{S_1, \dots, S_r\} \subseteq \text{GL}(n, \mathbb{F})$.

Then $G \leq \text{GL}(n, R)$, $R = \frac{1}{f} \mathbb{E}[X_1, \dots, X_m]$, where $f = f(X_1, \dots, X_m)$ is the l.c.m. of denominators of the non-zero entries of S_i and S_i^{-1} , $1 \leq i \leq r$.

Say $\alpha = (\alpha_1, \dots, \alpha_m) \in \mathbb{E}^{(m)}$ is \mathcal{S} -admissible if $f(\alpha) \neq 0$.

Note: when \mathbb{E} is finite, $\mathbb{E}^{(m)}$ may not contain admissible α ; for convenience, we assume that it does.

Congruence homomorphisms

Congruence homomorphisms

For an \mathcal{S} -admissible $\alpha = (\alpha_1, \dots, \alpha_m)$,

Congruence homomorphisms

For an \mathcal{S} -admissible $\alpha = (\alpha_1, \dots, \alpha_m)$, define $\varphi_\alpha : R \rightarrow \mathbb{E}$ as the (congruence) homomorphism with kernel $\langle X_i - \alpha_i : 1 \leq i \leq m \rangle$.

Congruence homomorphisms

For an \mathcal{S} -admissible $\alpha = (\alpha_1, \dots, \alpha_m)$, define $\varphi_\alpha : R \rightarrow \mathbb{E}$ as the (congruence) homomorphism with kernel $\langle X_i - \alpha_i : 1 \leq i \leq m \rangle$.

φ_α extends to $\text{Mat}(n, R)$, as an \mathbb{E} -algebra homomorphism.

Congruence homomorphisms

For an \mathcal{S} -admissible $\alpha = (\alpha_1, \dots, \alpha_m)$, define $\varphi_\alpha : R \rightarrow \mathbb{E}$ as the (congruence) homomorphism with kernel $\langle X_i - \alpha_i : 1 \leq i \leq m \rangle$.

φ_α extends to $\text{Mat}(n, R)$, as an \mathbb{E} -algebra homomorphism.

Notation:

Congruence homomorphisms

For an \mathcal{S} -admissible $\alpha = (\alpha_1, \dots, \alpha_m)$, define $\varphi_\alpha : R \rightarrow \mathbb{E}$ as the (congruence) homomorphism with kernel $\langle X_i - \alpha_i : 1 \leq i \leq m \rangle$.

φ_α extends to $\text{Mat}(n, R)$, as an \mathbb{E} -algebra homomorphism.

Notation: if $\mathcal{M} \subseteq \text{Mat}(n, R)$ and \mathbb{K} is a subfield of \mathbb{F} then

Congruence homomorphisms

For an \mathcal{S} -admissible $\alpha = (\alpha_1, \dots, \alpha_m)$, define $\varphi_\alpha : R \rightarrow \mathbb{E}$ as the (congruence) homomorphism with kernel $\langle X_i - \alpha_i : 1 \leq i \leq m \rangle$.

φ_α extends to $\text{Mat}(n, R)$, as an \mathbb{E} -algebra homomorphism.

Notation: if $\mathcal{M} \subseteq \text{Mat}(n, R)$ and \mathbb{K} is a subfield of \mathbb{F} then

- $\langle \mathcal{M} \rangle_{\mathbb{K}}$ denotes the \mathbb{K} -enveloping algebra of \mathcal{M} ;

Congruence homomorphisms

For an \mathcal{S} -admissible $\alpha = (\alpha_1, \dots, \alpha_m)$, define $\varphi_\alpha : R \rightarrow \mathbb{E}$ as the (congruence) homomorphism with kernel $\langle X_i - \alpha_i : 1 \leq i \leq m \rangle$.

φ_α extends to $\text{Mat}(n, R)$, as an \mathbb{E} -algebra homomorphism.

Notation: if $\mathcal{M} \subseteq \text{Mat}(n, R)$ and \mathbb{K} is a subfield of \mathbb{F} then

- $\langle \mathcal{M} \rangle_{\mathbb{K}}$ denotes the \mathbb{K} -enveloping algebra of \mathcal{M} ;
- $\mathcal{M}(\alpha) := \varphi_\alpha(\mathcal{M})$.

Congruence homomorphisms

For an \mathcal{S} -admissible $\alpha = (\alpha_1, \dots, \alpha_m)$, define $\varphi_\alpha : R \rightarrow \mathbb{E}$ as the (congruence) homomorphism with kernel $\langle X_i - \alpha_i : 1 \leq i \leq m \rangle$.

φ_α extends to $\text{Mat}(n, R)$, as an \mathbb{E} -algebra homomorphism.

Notation: if $\mathcal{M} \subseteq \text{Mat}(n, R)$ and \mathbb{K} is a subfield of \mathbb{F} then

- $\langle \mathcal{M} \rangle_{\mathbb{K}}$ denotes the \mathbb{K} -enveloping algebra of \mathcal{M} ;
- $\mathcal{M}(\alpha) := \varphi_\alpha(\mathcal{M})$.

Theorem Suppose G is finite, α is \mathcal{S} -admissible.

Congruence homomorphisms

For an \mathcal{S} -admissible $\alpha = (\alpha_1, \dots, \alpha_m)$, define $\varphi_\alpha : R \rightarrow \mathbb{E}$ as the (congruence) homomorphism with kernel $\langle X_i - \alpha_i : 1 \leq i \leq m \rangle$.

φ_α extends to $\text{Mat}(n, R)$, as an \mathbb{E} -algebra homomorphism.

Notation: if $\mathcal{M} \subseteq \text{Mat}(n, R)$ and \mathbb{K} is a subfield of \mathbb{F} then

- $\langle \mathcal{M} \rangle_{\mathbb{K}}$ denotes the \mathbb{K} -enveloping algebra of \mathcal{M} ;
- $\mathcal{M}(\alpha) := \varphi_\alpha(\mathcal{M})$.

Theorem Suppose G is finite, α is \mathcal{S} -admissible. Then the kernel of φ_α on $\langle G \rangle_{\mathbb{E}}$ is contained in the radical of $\langle G \rangle_{\mathbb{F}}$.

Corollary Suppose G is finite, α is \mathcal{S} -admissible.

Corollary Suppose G is finite, α is \mathcal{S} -admissible.

- (i) If $\text{char } \mathbb{F} = 0$ then φ_α is an isomorphism on $\langle G \rangle_{\mathbb{E}}$.

Corollary Suppose G is finite, α is \mathcal{S} -admissible.

- (i) If $\text{char } \mathbb{F} = 0$ then φ_α is an isomorphism on $\langle G \rangle_{\mathbb{F}}$.
- (ii) If $\text{char } \mathbb{F} > 0$ and G is completely reducible

Corollary Suppose G is finite, α is \mathcal{S} -admissible.

- (i) If $\text{char } \mathbb{F} = 0$ then φ_α is an isomorphism on $\langle G \rangle_{\mathbb{E}}$.
- (ii) If $\text{char } \mathbb{F} > 0$ and G is completely reducible then φ_α is an isomorphism on $\langle G \rangle_{\mathbb{E}}$.

Corollary Suppose G is finite, α is \mathcal{S} -admissible.

- (i) If $\text{char } \mathbb{F} = 0$ then φ_α is an isomorphism on $\langle G \rangle_{\mathbb{E}}$.
- (ii) If $\text{char } \mathbb{F} > 0$ and G is completely reducible then φ_α is an isomorphism on $\langle G \rangle_{\mathbb{E}}$.

Lemma (Finiteness Criterion)

Let $\alpha \in \mathbb{E}^{(m)}$ be \mathcal{S} -admissible.

Corollary Suppose G is finite, α is \mathcal{S} -admissible.

- (i) If $\text{char } \mathbb{F} = 0$ then φ_α is an isomorphism on $\langle G \rangle_{\mathbb{E}}$.
- (ii) If $\text{char } \mathbb{F} > 0$ and G is completely reducible then φ_α is an isomorphism on $\langle G \rangle_{\mathbb{E}}$.

Lemma (Finiteness Criterion)

Let $\alpha \in \mathbb{E}^{(m)}$ be \mathcal{S} -admissible.

- (i) Let $\text{char } \mathbb{F} = 0$.

Corollary Suppose G is finite, α is \mathcal{S} -admissible.

- (i) If $\text{char } \mathbb{F} = 0$ then φ_α is an isomorphism on $\langle G \rangle_{\mathbb{E}}$.
- (ii) If $\text{char } \mathbb{F} > 0$ and G is completely reducible then φ_α is an isomorphism on $\langle G \rangle_{\mathbb{E}}$.

Lemma (Finiteness Criterion)

Let $\alpha \in \mathbb{E}^{(m)}$ be \mathcal{S} -admissible.

- (i) Let $\text{char } \mathbb{F} = 0$. Then G is finite if and only if

Corollary Suppose G is finite, α is \mathcal{S} -admissible.

- (i) If $\text{char } \mathbb{F} = 0$ then φ_α is an isomorphism on $\langle G \rangle_{\mathbb{E}}$.
- (ii) If $\text{char } \mathbb{F} > 0$ and G is completely reducible then φ_α is an isomorphism on $\langle G \rangle_{\mathbb{E}}$.

Lemma (Finiteness Criterion)

Let $\alpha \in \mathbb{E}^{(m)}$ be \mathcal{S} -admissible.

- (i) Let $\text{char } \mathbb{F} = 0$. Then G is finite if and only if $G(\alpha)$ is finite and $\dim_{\mathbb{E}} \langle G \rangle_{\mathbb{E}} = \dim_{\mathbb{E}} \langle G(\alpha) \rangle_{\mathbb{E}}$.

Corollary Suppose G is finite, α is \mathcal{S} -admissible.

- (i) If $\text{char } \mathbb{F} = 0$ then φ_α is an isomorphism on $\langle G \rangle_{\mathbb{E}}$.
- (ii) If $\text{char } \mathbb{F} > 0$ and G is completely reducible then φ_α is an isomorphism on $\langle G \rangle_{\mathbb{E}}$.

Lemma (Finiteness Criterion)

Let $\alpha \in \mathbb{E}^{(m)}$ be \mathcal{S} -admissible.

- (i) Let $\text{char } \mathbb{F} = 0$. Then G is finite if and only if $G(\alpha)$ is finite and $\dim_{\mathbb{E}} \langle G \rangle_{\mathbb{E}} = \dim_{\mathbb{E}} \langle G(\alpha) \rangle_{\mathbb{E}}$.
- (ii) Suppose $\text{char } \mathbb{F} > 0$ and G is completely reducible.

Corollary Suppose G is finite, α is \mathcal{S} -admissible.

- (i) If $\text{char } \mathbb{F} = 0$ then φ_α is an isomorphism on $\langle G \rangle_{\mathbb{E}}$.
- (ii) If $\text{char } \mathbb{F} > 0$ and G is completely reducible then φ_α is an isomorphism on $\langle G \rangle_{\mathbb{E}}$.

Lemma (Finiteness Criterion)

Let $\alpha \in \mathbb{E}^{(m)}$ be \mathcal{S} -admissible.

- (i) Let $\text{char } \mathbb{F} = 0$. Then G is finite if and only if $G(\alpha)$ is finite and $\dim_{\mathbb{E}} \langle G \rangle_{\mathbb{E}} = \dim_{\mathbb{E}} \langle G(\alpha) \rangle_{\mathbb{E}}$.
- (ii) Suppose $\text{char } \mathbb{F} > 0$ and G is completely reducible. Then G is finite if and only if $\dim_{\mathbb{E}} \langle G \rangle_{\mathbb{E}} = \dim_{\mathbb{E}} \langle G(\alpha) \rangle_{\mathbb{E}}$.

Computing a basis of an enveloping algebra can be done in standard fashion; call the procedure `BasisEnvAlgebra` here.

Computing a basis of an enveloping algebra can be done in standard fashion; call the procedure `BasisEnvAlgebra` here.

For a field \mathbb{K} , and f.g. $H = \langle \mathcal{T} \rangle \leq \text{GL}(n, \mathbb{K})$, `BasisEnvAlgebra`(\mathcal{T}, \mathbb{K}) returns a basis of $\langle H \rangle_{\mathbb{K}}$ consisting of elements of H .

Computing a basis of an enveloping algebra can be done in standard fashion; call the procedure `BasisEnvAlgebra` here.

For a field \mathbb{K} , and f.g. $H = \langle \mathcal{T} \rangle \leq GL(n, \mathbb{K})$, `BasisEnvAlgebra`(\mathcal{T}, \mathbb{K}) returns a basis of $\langle H \rangle_{\mathbb{K}}$ consisting of elements of H .

N.B. we only ever invoke `BasisEnvAlgebra` for the enveloping algebra of a finite group over \mathbb{E} (a number field or finite field).

Computing a basis of an enveloping algebra can be done in standard fashion; call the procedure `BasisEnvAlgebra` here.

For a field \mathbb{K} , and f.g. $H = \langle \mathcal{T} \rangle \leq \mathrm{GL}(n, \mathbb{K})$, `BasisEnvAlgebra`(\mathcal{T}, \mathbb{K}) returns a basis of $\langle H \rangle_{\mathbb{K}}$ consisting of elements of H .

N.B. we only ever invoke `BasisEnvAlgebra` for the enveloping algebra of a finite group over \mathbb{E} (a number field or finite field).

Almost all computing is thereby transferred from the function field to the more manageable coefficient field—in contrast to earlier algorithms.

Characteristic zero

Characteristic zero

`IsFiniteMatGroupFuncNF(\mathcal{S})`

Characteristic zero

`IsFiniteMatGroupFuncNF(\mathcal{S})`

Input: a finite subset \mathcal{S} of $GL(n, \mathbb{F})$, $\mathbb{F} = \mathbb{E}(X_1, \dots, X_m)$, \mathbb{E} a number field.

Characteristic zero

`IsFiniteMatGroupFuncNF(\mathcal{S})`

Input: a finite subset \mathcal{S} of $GL(n, \mathbb{F})$, $\mathbb{F} = \mathbb{E}(X_1, \dots, X_m)$, \mathbb{E} a number field.

Output: ‘true’ if $G = \langle \mathcal{S} \rangle$ is finite; ‘false’ otherwise.

Characteristic zero

`IsFiniteMatGroupFuncNF(\mathcal{S})`

Input: a finite subset \mathcal{S} of $GL(n, \mathbb{F})$, $\mathbb{F} = \mathbb{E}(X_1, \dots, X_m)$, \mathbb{E} a number field.

Output: ‘true’ if $G = \langle \mathcal{S} \rangle$ is finite; ‘false’ otherwise.

(I) $\mathcal{S}(\alpha) := \{S_i(\alpha) \mid S_i \in \mathcal{S}\}$ for \mathcal{S} -admissible $\alpha \in \mathbb{E}^{(m)}$.

Characteristic zero

`IsFiniteMatGroupFuncNF(\mathcal{S})`

Input: a finite subset \mathcal{S} of $\mathrm{GL}(n, \mathbb{F})$, $\mathbb{F} = \mathbb{E}(X_1, \dots, X_m)$, \mathbb{E} a number field.

Output: ‘true’ if $G = \langle \mathcal{S} \rangle$ is finite; ‘false’ otherwise.

- (I) $\mathcal{S}(\alpha) := \{S_i(\alpha) \mid S_i \in \mathcal{S}\}$ for \mathcal{S} -admissible $\alpha \in \mathbb{E}^{(m)}$.
- (II) If $\langle \mathcal{S}(\alpha) \rangle$ is infinite or $S_i(\alpha) = S_j(\alpha)$ for $i \neq j$ then return ‘false’.

Characteristic zero

`IsFiniteMatGroupFuncNF(\mathcal{S})`

Input: a finite subset \mathcal{S} of $GL(n, \mathbb{F})$, $\mathbb{F} = \mathbb{E}(X_1, \dots, X_m)$, \mathbb{E} a number field.

Output: ‘true’ if $G = \langle \mathcal{S} \rangle$ is finite; ‘false’ otherwise.

- (I) $\mathcal{S}(\alpha) := \{S_i(\alpha) \mid S_i \in \mathcal{S}\}$ for \mathcal{S} -admissible $\alpha \in \mathbb{E}^{(m)}$.
- (II) If $\langle \mathcal{S}(\alpha) \rangle$ is infinite or $S_i(\alpha) = S_j(\alpha)$ for $i \neq j$ then return ‘false’.
- (III) $\mathcal{A}(\alpha) := \text{BasisEnvAlgebra}(\mathcal{S}(\alpha), \mathbb{E}) = \{A_1(\alpha), \dots, A_d(\alpha)\}$.

Characteristic zero

IsFiniteMatGroupFuncNF(\mathcal{S})

Input: a finite subset \mathcal{S} of $GL(n, \mathbb{F})$, $\mathbb{F} = \mathbb{E}(X_1, \dots, X_m)$, \mathbb{E} a number field.

Output: ‘true’ if $G = \langle \mathcal{S} \rangle$ is finite; ‘false’ otherwise.

- (I) $\mathcal{S}(\alpha) := \{S_i(\alpha) \mid S_i \in \mathcal{S}\}$ for \mathcal{S} -admissible $\alpha \in \mathbb{E}^{(m)}$.
- (II) If $\langle \mathcal{S}(\alpha) \rangle$ is infinite or $S_i(\alpha) = S_j(\alpha)$ for $i \neq j$ then return ‘false’.
- (III) $\mathcal{A}(\alpha) := \text{BasisEnvAlgebra}(\mathcal{S}(\alpha), \mathbb{E}) = \{A_1(\alpha), \dots, A_d(\alpha)\}$.
Let \mathcal{A} be the canonical pre-image $\{A_1, \dots, A_d\} \subseteq G$ of $\mathcal{A}(\alpha)$.

Characteristic zero

IsFiniteMatGroupFuncNF(\mathcal{S})

Input: a finite subset \mathcal{S} of $GL(n, \mathbb{F})$, $\mathbb{F} = \mathbb{E}(X_1, \dots, X_m)$, \mathbb{E} a number field.

Output: ‘true’ if $G = \langle \mathcal{S} \rangle$ is finite; ‘false’ otherwise.

- (I) $\mathcal{S}(\alpha) := \{S_i(\alpha) \mid S_i \in \mathcal{S}\}$ for \mathcal{S} -admissible $\alpha \in \mathbb{E}^{(m)}$.
- (II) If $\langle \mathcal{S}(\alpha) \rangle$ is infinite or $S_i(\alpha) = S_j(\alpha)$ for $i \neq j$ then return ‘false’.
- (III) $\mathcal{A}(\alpha) := \text{BasisEnvAlgebra}(\mathcal{S}(\alpha), \mathbb{E}) = \{A_1(\alpha), \dots, A_d(\alpha)\}$.
Let \mathcal{A} be the canonical pre-image $\{A_1, \dots, A_d\} \subseteq G$ of $\mathcal{A}(\alpha)$.
Suppose $A_i(\alpha)S_j(\alpha) = \sum_{k=1}^d a_k A_k(\alpha)$, $a_k \in \mathbb{E}$.

Characteristic zero

IsFiniteMatGroupFuncNF(\mathcal{S})

Input: a finite subset \mathcal{S} of $GL(n, \mathbb{F})$, $\mathbb{F} = \mathbb{E}(X_1, \dots, X_m)$, \mathbb{E} a number field.

Output: ‘true’ if $G = \langle \mathcal{S} \rangle$ is finite; ‘false’ otherwise.

- (I) $\mathcal{S}(\alpha) := \{S_i(\alpha) \mid S_i \in \mathcal{S}\}$ for \mathcal{S} -admissible $\alpha \in \mathbb{E}^{(m)}$.
- (II) If $\langle \mathcal{S}(\alpha) \rangle$ is infinite or $S_i(\alpha) = S_j(\alpha)$ for $i \neq j$ then return ‘false’.
- (III) $\mathcal{A}(\alpha) := \text{BasisEnvAlgebra}(\mathcal{S}(\alpha), \mathbb{E}) = \{A_1(\alpha), \dots, A_d(\alpha)\}$.
Let \mathcal{A} be the canonical pre-image $\{A_1, \dots, A_d\} \subseteq G$ of $\mathcal{A}(\alpha)$.
Suppose $A_i(\alpha)S_j(\alpha) = \sum_{k=1}^d a_k A_k(\alpha)$, $a_k \in \mathbb{E}$.
If $A_i S_j \neq \sum_{k=1}^d a_k A_k$ for some i, j , then return ‘false’;

Characteristic zero

IsFiniteMatGroupFuncNF(\mathcal{S})

Input: a finite subset \mathcal{S} of $GL(n, \mathbb{F})$, $\mathbb{F} = \mathbb{E}(X_1, \dots, X_m)$, \mathbb{E} a number field.

Output: ‘true’ if $G = \langle \mathcal{S} \rangle$ is finite; ‘false’ otherwise.

- (I) $\mathcal{S}(\alpha) := \{S_i(\alpha) \mid S_i \in \mathcal{S}\}$ for \mathcal{S} -admissible $\alpha \in \mathbb{E}^{(m)}$.
- (II) If $\langle \mathcal{S}(\alpha) \rangle$ is infinite or $S_i(\alpha) = S_j(\alpha)$ for $i \neq j$ then return ‘false’.
- (III) $\mathcal{A}(\alpha) := \text{BasisEnvAlgebra}(\mathcal{S}(\alpha), \mathbb{E}) = \{A_1(\alpha), \dots, A_d(\alpha)\}$.
Let \mathcal{A} be the canonical pre-image $\{A_1, \dots, A_d\} \subseteq G$ of $\mathcal{A}(\alpha)$.
Suppose $A_i(\alpha)S_j(\alpha) = \sum_{k=1}^d a_k A_k(\alpha)$, $a_k \in \mathbb{E}$.
If $A_i S_j \neq \sum_{k=1}^d a_k A_k$ for some i, j , then return ‘false’;
else return ‘true’.

Notes

Notes

- Testing finiteness in $GL(n, \mathbb{E})$ can be done using e.g. algorithms of Babai, Beals & Rockmore (1993); available procedures in **GAP** and **MAGMA**.

Notes

- Testing finiteness in $GL(n, \mathbb{E})$ can be done using e.g. algorithms of Babai, Beals & Rockmore (1993); available procedures in **GAP** and **MAGMA**.
- Reports ‘false’ at steps (II) and (III) are correct, since φ_α is an isomorphism on $\langle G \rangle_{\mathbb{E}}$ if G is finite.
- Report ‘true’ at step (III) is correct: at that stage \mathcal{A} is known to be a basis of $\langle G \rangle_{\mathbb{E}} = \langle \mathcal{S} \rangle_{\mathbb{E}}$.

Notes

- Testing finiteness in $GL(n, \mathbb{E})$ can be done using e.g. algorithms of Babai, Beals & Rockmore (1993); available procedures in **GAP** and **MAGMA**.
- Reports ‘false’ at steps (II) and (III) are correct, since φ_α is an isomorphism on $\langle G \rangle_{\mathbb{E}}$ if G is finite.
- Report ‘true’ at step (III) is correct: at that stage \mathcal{A} is known to be a basis of $\langle G \rangle_{\mathbb{E}} = \langle \mathcal{S} \rangle_{\mathbb{E}}$.
- Almost all computing in `IsFiniteMatGroupFuncNF` is over the number field \mathbb{E} .

Positive characteristic

Positive characteristic

Now let $G \leq \mathrm{GL}(n, \mathbb{F})$, $\mathbb{F} = \mathbb{F}_q(X_1, \dots, X_m)$.

Positive characteristic

Now let $G \leq \mathrm{GL}(n, \mathbb{F})$, $\mathbb{F} = \mathbb{F}_q(X_1, \dots, X_m)$.

Now if G is finite it need not be completely reducible;

Positive characteristic

Now let $G \leq \mathrm{GL}(n, \mathbb{F})$, $\mathbb{F} = \mathbb{F}_q(X_1, \dots, X_m)$.

Now if G is finite it need not be completely reducible; φ_α can have non-trivial (unipotent) kernel on finite G .

Positive characteristic

Now let $G \leq \mathrm{GL}(n, \mathbb{F})$, $\mathbb{F} = \mathbb{F}_q(X_1, \dots, X_m)$.

Now if G is finite it need not be completely reducible; φ_α can have non-trivial (unipotent) kernel on finite G .

Finiteness criterion: G is conjugate to a block triangular group

$$\begin{pmatrix} G_1 & * & \cdots & * \\ 0 & G_2 & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & G_\ell \end{pmatrix}$$

Positive characteristic

Now let $G \leq \mathrm{GL}(n, \mathbb{F})$, $\mathbb{F} = \mathbb{F}_q(X_1, \dots, X_m)$.

Now if G is finite it need not be completely reducible; φ_α can have non-trivial (unipotent) kernel on finite G .

Finiteness criterion: G is conjugate to a block triangular group

$$\begin{pmatrix} G_1 & * & \cdots & * \\ 0 & G_2 & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & G_\ell \end{pmatrix}$$

which is finite if and only if each block G_i is finite.

To obtain the G_i , we use the following lemma and linear algebra procedure.

To obtain the G_i , we use the following lemma and linear algebra procedure.

Lemma The nullspace of the radical of $\langle G \rangle_{\mathbb{F}}$ is a non-zero G -module.

To obtain the G_i , we use the following lemma and linear algebra procedure.

Lemma The nullspace of the radical of $\langle G \rangle_{\mathbb{F}}$ is a non-zero G -module.

For finite G , and a non-zero element J of $\ker \varphi_{\alpha}$ ($\subseteq \text{rad} \langle G \rangle_{\mathbb{F}}$), the procedure `ModuleViaNullspace`(\mathcal{S}, J) returns a non-zero proper G -submodule of the underlying space V (in the nullspace of J).

IsFiniteMatGroupFuncFF(\mathcal{S})

- (I) Let α be \mathcal{S} -admissible.
 If $S_i(\alpha) = S_j(\alpha)$ for $i \neq j$ set $D := S_i - S_j$ and go to step (IV).
- (II) $\mathcal{A}(\alpha) := \text{BasisEnvAlgebra}(\mathcal{S}(\alpha), \mathbb{F}_q) = \{A_1(\alpha), \dots, A_d(\alpha)\}$.
 $\mathcal{A} := \{A_1, \dots, A_d\}$.
- (III) If $A_i S_j \neq \sum_{k=1}^d a_k A_k$, $a_k \in \mathbb{F}_q$, where $A_i(\alpha) S(\alpha) = \sum_{k=1}^d a_k A_k(\alpha)$,
 then set $D := A_i S_j - \sum_{k=1}^d a_k A_k$;
 else return ‘true’.
- (IV) If $U_1 := \text{ModuleViaNullspace}(\mathcal{S}, D)$ is zero then return ‘false’;
 else let ρ be the projection on G w.r.t. U_1 and $U_2 = V/U_1$, and go
 to step (III) replacing \mathcal{S} by $\{\rho(S_1)|_{U_k}, \dots, \rho(S_r)|_{U_k}\}$ and \mathcal{A} by
 $\{\rho(A_1)|_{U_k}, \dots, \rho(A_d)|_{U_k}\}$, $k = 1, 2$.

Notes

- If G is finite completely reducible then this algorithm will run the same as the characteristic zero one.
- We have a simplified version of this algorithm for testing finiteness of nilpotent subgroups of $\mathrm{GL}(n, \mathbb{F})$.
- We can compute orders of input G found to be finite, via a randomized procedure that constructs an isomorphic copy of G over a finite field (extension of \mathbb{E}).

Some experimental data

Some experimental data

Some results of testing finiteness in $GL(n, \mathbb{F}_q(X))$, on a 3.0 GHz machine with 4GB RAM running MAGMA V2.15-10:

Group	n	r	q	Time.1	Time.2
G_{11}	40	2	5^7	1646	-
G_{12}	40	10	5^7	1124	-
G_{21}	54	20	29^4	806	-
G_{22}	54	23	29^4	474	-
G_{31}	36	520	7^8	2506	113
G_{32}	36	522	7^8	252	20

Some experimental data

Some results of testing finiteness in $GL(n, \mathbb{F}_q(X))$, on a 3.0 GHz machine with 4GB RAM running MAGMA V2.15-10:

Group	n	r	q	Time.1	Time.2
G_{11}	40	2	5^7	1646	-
G_{12}	40	10	5^7	1124	-
G_{21}	54	20	29^4	806	-
G_{22}	54	23	29^4	474	-
G_{31}	36	520	7^8	2506	113
G_{32}	36	522	7^8	252	20

G_{i1}, G_{i2} are finite, infinite respectively;

Some experimental data

Some results of testing finiteness in $GL(n, \mathbb{F}_q(X))$, on a 3.0 GHz machine with 4GB RAM running MAGMA V2.15-10:

Group	n	r	q	Time.1	Time.2
G_{11}	40	2	5^7	1646	-
G_{12}	40	10	5^7	1124	-
G_{21}	54	20	29^4	806	-
G_{22}	54	23	29^4	474	-
G_{31}	36	520	7^8	2506	113
G_{32}	36	522	7^8	252	20

G_{i1}, G_{i2} are finite, infinite respectively; G_{1j} are absolutely irreducible,

Some experimental data

Some results of testing finiteness in $GL(n, \mathbb{F}_q(X))$, on a 3.0 GHz machine with 4GB RAM running MAGMA V2.15-10:

Group	n	r	q	Time.1	Time.2
G_{11}	40	2	5^7	1646	-
G_{12}	40	10	5^7	1124	-
G_{21}	54	20	29^4	806	-
G_{22}	54	23	29^4	474	-
G_{31}	36	520	7^8	2506	113
G_{32}	36	522	7^8	252	20

G_{i1}, G_{i2} are finite, infinite respectively; G_{1j} are absolutely irreducible, G_{2j} & G_{3j} are not completely reducible,

Some experimental data

Some results of testing finiteness in $GL(n, \mathbb{F}_q(X))$, on a 3.0 GHz machine with 4GB RAM running MAGMA V2.15-10:

Group	n	r	q	Time.1	Time.2
G_{11}	40	2	5^7	1646	-
G_{12}	40	10	5^7	1124	-
G_{21}	54	20	29^4	806	-
G_{22}	54	23	29^4	474	-
G_{31}	36	520	7^8	2506	113
G_{32}	36	522	7^8	252	20

G_{i1}, G_{i2} are finite, infinite respectively; G_{1j} are absolutely irreducible, G_{2j} & G_{3j} are not completely reducible, G_{3j} are nilpotent.

Some experimental data

Some results of testing finiteness in $GL(n, \mathbb{F}_q(X))$, on a 3.0 GHz machine with 4GB RAM running MAGMA V2.15-10:

Group	n	r	q	Time.1	Time.2
G_{11}	40	2	5^7	1646	-
G_{12}	40	10	5^7	1124	-
G_{21}	54	20	29^4	806	-
G_{22}	54	23	29^4	474	-
G_{31}	36	520	7^8	2506	113
G_{32}	36	522	7^8	252	20

G_{i1}, G_{i2} are finite, infinite respectively; G_{1j} are absolutely irreducible, G_{2j} & G_{3j} are not completely reducible, G_{3j} are nilpotent.

Time.2 reports times for the nilpotent version of the main algorithm.