# Null cone membership for the left right action on tuples of matrices

Gabor Ivanyos[1], Jimmy Qiao[2], K V Subrahmanyam[3]

[1]Institute for Computer Science and Control, Hungarian Academy of Sciences, Budapest
[2]Center for Quantum Computation and Intelligent Systems, Univ of Technology, Sydney
[3]Chennai Mathematical Institute, Chennai

Tel Aviv University, Feb 09, 2016

# Outline

1. **Background and problem statement**
   - Problem statement
   - Invariant theory
2. **Using Gurvits algorithm**
3. **Progress via Blow-ups**
   - Regularity
   - Algorithmic and degree bounds
   - Degree bounds
   - Polynomial bound - degree of generation
   - Main lemma and blow ups using division algebras
   - Proof of the main lemma
   - Matrix of maximum rank
   - Division algebras

# Outline

1. **Background and problem statement**
   - Problem statement
   - Invariant theory
2. **Using Gurvits algorithm**
3. **Progress via Blow-ups**
   - Regularity
   - Algorithmic and degree bounds
   - Degree bounds
   - Polynomial bound - degree of generation
   - Main lemma and blow ups using division algebras
   - Proof of the main lemma

- $Mat(n, \mathbb{F})$ - $n \times n$ matrices with entries in $\mathbb{F}$.

## Problem statement

- $\mathsf{M}at(n, \mathbb{F})$ - $n \times n$ matrices with entries in $\mathbb{F}$.
- $B_1, B_2, \ldots, B_m \in \mathsf{M}at(n, \mathbb{F})$.

- $Mat(n, \mathbb{F})$ - $n \times n$ matrices with entries in $\mathbb{F}$.
- $B_1, B_2, \ldots, B_m \in Mat(n, \mathbb{F})$.
- $\mathcal{B}$ - $\mathbb{F}$-linear span of the matrices $\langle B_1, B_2, \ldots, B_m \rangle$.

- $Mat(n, \mathbb{F})$ - $n \times n$ matrices with entries in $\mathbb{F}$.
- $B_1, B_2, \ldots, B_m \in Mat(n, \mathbb{F})$.
- $\mathcal{B}$ - $\mathbb{F}$-linear span of the matrices $\langle B_1, B_2, \ldots, B_m \rangle$.

**Shrunk subspaces**

A subspace $U \leqslant \mathbb{F}^n$ is $c$-shrunk by $\mathcal{B}$ if there is a subspace $W \subseteq \mathbb{F}^n$ such that dim W $\leqslant \dim U - c$, and for all matrices $B$ in $\mathcal{B}$, $\langle BU \rangle \subseteq W$.

- $Mat(n, \mathbb{F})$ - $n \times n$ matrices with entries in $\mathbb{F}$.
- $B_1, B_2, \ldots, B_m \in Mat(n, \mathbb{F})$.
- $\mathcal{B}$ - $\mathbb{F}$-linear span of the matrices $\langle B_1, B_2, \ldots, B_m \rangle$.

## Shrunk subspaces

A subspace $U \leqslant \mathbb{F}^n$ is $c$-shrunk by $\mathcal{B}$ if there is a subspace $W \subseteq \mathbb{F}^n$ such that dim W $\leqslant \dim U - c$, and for all matrices $B$ in $\mathcal{B}$, $\langle BU \rangle \subseteq W$.

## Non commutative rank

$n - \max(c \in \{0, 1, \ldots, n\} \mid \exists subspace$ $c$-shrunk by $\mathcal{B})$ [FR04].

- $Mat(n, \mathbb{F})$ - $n \times n$ matrices with entries in $\mathbb{F}$.
- $B_1, B_2, \ldots, B_m \in Mat(n, \mathbb{F})$.
- $\mathcal{B}$ - $\mathbb{F}$-linear span of the matrices $\langle B_1, B_2, \ldots, B_m \rangle$.

## Shrunk subspaces

A subspace $U \leqslant \mathbb{F}^n$ is $c$-shrunk by $\mathcal{B}$ if there is a subspace $W \subseteq \mathbb{F}^n$ such that dim W $\leqslant \dim U - c$, and for all matrices $B$ in $\mathcal{B}$, $\langle BU \rangle \subseteq W$.

## Non commutative rank

$n - \max(c \in \{0, 1, \ldots, n\} \mid \exists \textit{subspace } c\text{-shrunk by } \mathcal{B})$ [FR04].

Problem NCrk: What is the noncommutative rank?

# Related problem

**Commutative rank**

The maximum of the rank of matrices in $\mathcal{B}$?

# Related problem

**Commutative rank**

The maximum of the rank of matrices in $\mathcal{B}$?

Problem Rk: What is the commutative rank? [Edm67]

# Related problem

**Commutative rank**

The maximum of the rank of matrices in $\mathcal{B}$?

Problem Rk: What is the commutative rank? [Edm67]

- Rk $\leqslant$ NCrk.

# Related problem

**Commutative rank**

The maximum of the rank of matrices in $\mathcal{B}$?

Problem Rk: What is the commutative rank? [Edm67]

- Rk $\leqslant$ NCrk.
- For the family of $3 \times 3$ skew symmetric matrices, 2=Rk $<$ NCrk=3.

# Related problem

**Commutative rank**

The maximum of the rank of matrices in $\mathcal{B}$?

Problem Rk: What is the commutative rank? [Edm67]

- Rk $\leqslant$ NCrk.
- For the family of $3 \times 3$ skew symmetric matrices, 2=Rk < NCrk=3.

**Theorem - Gurvits**

Over $\mathbb{Q}$, given a matrix space $\langle \mathcal{B} \rangle$ there is a deterministic polynomial time algorithm which will output Rk=$n$, or NCrk $< n$, and its output is guaranteed to be correct when either $NCrk(\mathcal{B}) < n$ or $\mathrm{Rk}(\mathcal{B}) = n$.

# Related problem

**Commutative rank**

The maximum of the rank of matrices in $\mathcal{B}$?

Problem Rk: What is the commutative rank? [Edm67]

- Rk $\leqslant$ NCrk.
- For the family of $3 \times 3$ skew symmetric matrices, 2=Rk < NCrk=3.

**Theorem - Gurvits**

Over $\mathbb{Q}$, given a matrix space $\langle \mathcal{B} \rangle$ there is a deterministic polynomial time algorithm which will output Rk=$n$, or NCrk $< n$, and its output is guaranteed to be correct when either $NCrk(\mathcal{B}) < n$ or $\mathrm{Rk}(\mathcal{B}) = n$.

The algorithm may give a wrong answer in the case when $n = NCrk > Rk$.

# Left right action

- $\mathcal{X} = \{X_1, X_2, \ldots, X_m\}$, $X_k$, an $n \times n$ matrix with variable entries $x_{ij}^k$.

# Left right action

- $\mathcal{X} = \{X_1, X_2, \ldots, X_m\}$, $X_k$, an $n \times n$ matrix with variable entries $x_{ij}^k$.
- $\mathrm{SL}_n \times \mathrm{SL}_n \curvearrowright \mathcal{X}$,

# Left right action

- $\mathcal{X} = \{ X_1, X_2, \ldots, X_m \}$, $X_k$, an $n \times n$ matrix with variable entries $x_{ij}^k$.
- $\mathrm{SL}_n \times \mathrm{SL}_n \curvearrowright \mathcal{X}$,
$(A, B) \cdot \{ X_1, X_2, \ldots, X_m \} = \{ AX_1B^t, AX_2B^t, \ldots, AX_mB^t \}$.

# Left right action

- $\mathcal{X} = \{X_1, X_2, \ldots, X_m\}$, $X_k$, an $n \times n$ matrix with variable entries $x_{ij}^k$.
- $\mathrm{SL}_n \times \mathrm{SL}_n \curvearrowright \mathcal{X}$,
  $(A, B) \cdot \{X_1, X_2, \ldots, X_m\} = \{AX_1B^t, AX_2B^t, \ldots, AX_mB^t\}$.

## Classical invariant theory questions

- What are the polynomial functions invariant under the action? -
- The ring of invariants is known to be finitely generated - bound on the degree in which this is generated?

# Left right action

- $\mathcal{X} = \{X_1, X_2, \ldots, X_m\}$, $X_k$, an $n \times n$ matrix with variable entries $x_{ij}^k$.
- $\mathrm{SL}_n \times \mathrm{SL}_n \curvearrowright \mathcal{X}$,
  $(A, B) \cdot \{X_1, X_2, \ldots, X_m\} = \{AX_1B^t, AX_2B^t, \ldots, AX_mB^t\}$.

**Classical invariant theory questions**

- What are the polynomial functions invariant under the action? - well understood characteristic zero fields,[Sch91, DZ01, ANS07], infinite fields [DZ01].
- The ring of invariants is known to be finitely generated - bound on the degree in which this is generated?

# Left right action

- $\mathcal{X} = \{X_1, X_2, \ldots, X_m\}$, $X_k$, an $n \times n$ matrix with variable entries $x_{ij}^k$.
- $\mathrm{SL}_n \times \mathrm{SL}_n \curvearrowright \mathcal{X}$,
$(A, B) \cdot \{X_1, X_2, \ldots, X_m\} = \{AX_1B^t, AX_2B^t, \ldots, AX_mB^t\}$.

## Classical invariant theory questions

- What are the polynomial functions invariant under the action? - well understood characteristic zero fields,[Sch91, DZ01, ANS07], infinite fields [DZ01].
- The ring of invariants is known to be finitely generated - bound on the degree in which this is generated? characteristic zero fields, $exp(n^2)$, [Der01].

# Membership in the null cone

# Membership in the null cone

**Null cone for the left right action**

Is defined as the $m$-tuple of $n$ by $n$ matrices on which all all invariant polynomial functions vanish

# Membership in the null cone

## Null cone for the left right action

Is defined as the $m$-tuple of $n$ by $n$ matrices on which all all invariant polynomial functions vanish i.e $f(B_1, B_2, \ldots, B_m) = 0$ for all invariant polynomial functions $f$.

# Membership in the null cone

**Null cone for the left right action**

Is defined as the $m$-tuple of $n$ by $n$ matrices on which all all invariant polynomial functions vanish i.e $f(B_1, B_2, \ldots, B_m) = 0$ for all invariant polynomial functions $f$.

- Over infinite fields - an alternate characterization -

# Membership in the null cone

### Null cone for the left right action

Is defined as the $m$-tuple of $n$ by $n$ matrices on which all all invariant polynomial functions vanish i.e $f(B_1, B_2, \ldots, B_m) = 0$ for all invariant polynomial functions $f$.

- Over infinite fields - an alternate characterization - $(B_1, B_2, \ldots, B_m)$ such that $\mathcal{B}$ has a $c$-shrunk subspace for $c > 0$ [BD06, DZ01, ANS07].

# Membership in the null cone

## Null cone for the left right action

Is defined as the $m$-tuple of $n$ by $n$ matrices on which all all invariant polynomial functions vanish i.e $f(B_1, B_2, \ldots, B_m) = 0$ for all invariant polynomial functions $f$.

- Over infinite fields - an alternate characterization - $(B_1, B_2, \ldots, B_m)$ such that $\mathcal{B}$ has a $c$-shrunk subspace for $c > 0$ [BD06, DZ01, ANS07].
- A description of the invariants:
  Let $T_1, T_2, \ldots, T_m$ be matrices in $Mat(d, \mathbb{F})$. Then $det(T_1 \otimes X_1 + T_2 \otimes X_2 + \ldots + T_m \otimes X_m)$ is an invariant of degree $nd$.

# Membership in the null cone

### Null cone for the left right action

Is defined as the $m$-tuple of $n$ by $n$ matrices on which all all invariant polynomial functions vanish i.e $f(B_1, B_2, \ldots, B_m) = 0$ for all invariant polynomial functions $f$.

- Over infinite fields - an alternate characterization - $(B_1, B_2, \ldots, B_m)$ such that $\mathcal{B}$ has a $c$-shrunk subspace for $c > 0$ [BD06, DZ01, ANS07].
- A description of the invariants:
  Let $T_1, T_2, \ldots, T_m$ be matrices in $Mat(d, \mathbb{F})$. Then $det(T_1 \otimes X_1 + T_2 \otimes X_2 + \ldots + T_m \otimes X_m)$ is an invariant of degree $nd$. Over infinite fields, all invariants are obtained this way.

# Outline


1. Background and problem statement
   - Problem statement
   - Invariant theory
2. **Using Gurvits algorithm**
3. Progress via Blow-ups
   - Regularity
   - Algorithmic and degree bounds
   - Degree bounds
   - Polynomial bound - degree of generation
   - Main lemma and blow ups using division algebras
   - Proof of the main lemma

# Suggested algorithm

# Suggested algorithm

**Observation**

If $B_1$ shrinks a subspace $U \in \mathbb{F}^n$, and $T_1 \in Mat(d, \mathbb{F})$ then $T_1 \otimes B_1$ shrinks the subspace $U \otimes \mathbb{F}^d$.

# Suggested algorithm

**Observation**

If $B_1$ shrinks a subspace $U \in \mathbb{F}^n$, and $T_1 \in Mat(d, \mathbb{F})$ then $T_1 \otimes B_1$ shrinks the subspace $U \otimes \mathbb{F}^d$.

If $\mathcal{B}$ shrinks $U$, then so will its $d$-th blow-up

# Suggested algorithm

**Observation**

If $B_1$ shrinks a subspace $U \in \mathbb{F}^n$, and $T_1 \in \mathrm{Mat}(d, \mathbb{F})$ then $T_1 \otimes B_1$ shrinks the subspace $U \otimes \mathbb{F}^d$.

If $\mathcal{B}$ shrinks $U$, then so will its $d$-th blow-up $\mathcal{B}^{\{d,d\}} := \langle T_1 \otimes B_1, T_2 \otimes B_2, \ldots, T_m \otimes B_m \rangle$, $T_i \in \mathrm{Mat}(d, \mathbb{F})$.

# Suggested algorithm

**Observation**

If $B_1$ shrinks a subspace $U \in \mathbb{F}^n$, and $T_1 \in \mathrm{Mat}(d, \mathbb{F})$ then $T_1 \otimes B_1$ shrinks the subspace $U \otimes \mathbb{F}^d$.

If $\mathcal{B}$ shrinks $U$, then so will its $d$-th blow-up $\mathcal{B}^{\{d,d\}} := \langle T_1 \otimes B_1, T_2 \otimes B_2, \ldots, T_m \otimes B_m \rangle$, $T_i \in \mathrm{Mat}(d, \mathbb{F})$.

- for $i = 1, 2, \ldots,$ compute (a basis of) $\mathcal{B}^{\{i,i\}}$.

# Suggested algorithm

**Observation**

If $B_1$ shrinks a subspace $U \in \mathbb{F}^n$, and $T_1 \in \mathrm{Mat}(d, \mathbb{F})$ then $T_1 \otimes B_1$ shrinks the subspace $U \otimes \mathbb{F}^d$.

If $\mathcal{B}$ shrinks $U$, then so will its $d$-th blow-up $\mathcal{B}^{\{d,d\}} := \langle T_1 \otimes B_1, T_2 \otimes B_2, \ldots, T_m \otimes B_m \rangle$, $T_i \in \mathrm{Mat}(d, \mathbb{F})$.

- for $i = 1, 2, \ldots,$ compute (a basis of) $\mathcal{B}^{\{i,i\}}$.
- determine if there is a nonsingular matrix in the blow-up.

# Suggested algorithm

**Observation**

If $B_1$ shrinks a subspace $U \in \mathbb{F}^n$, and $T_1 \in Mat(d, \mathbb{F})$ then $T_1 \otimes B_1$ shrinks the subspace $U \otimes \mathbb{F}^d$.

If $\mathcal{B}$ shrinks $U$, then so will its $d$-th blow-up $\mathcal{B}^{\{d,d\}} := \langle T_1 \otimes B_1, T_2 \otimes B_2, \ldots, T_m \otimes B_m \rangle$, $T_i \in Mat(d, \mathbb{F})$.

- for $i = 1, 2, \ldots,$ compute (a basis of) $\mathcal{B}^{\{i,i\}}$.
- determine if there is a nonsingular matrix in the blow-up.

Question How long do we go on?

# Implications of degree bound $\sigma$

**Theorem**

[IQS15a] Over $\mathbb{Q}$, if the nullcone is defined by elements of degree $\leqslant \sigma = \sigma(n, m)$,there exists a deterministic poly$(n, m, \sigma)$ algorithm deciding if $(B_1, B_2, \ldots, B_m)$ is in the null cone.

# Implications of degree bound $\sigma$

**Theorem**

[IQS15a] Over $\mathbb{Q}$, if the nullcone is defined by elements of degree $\leqslant \sigma = \sigma(n, m)$,there exists a deterministic poly$(n, m, \sigma)$ algorithm deciding if $(B_1, B_2, \ldots, B_m)$ is in the null cone.

- If $(B_1, \ldots, B_m)$ is in the null cone all blow-ups $\mathcal{B}^{\{d,d\}}$ shrink a subspace.

# Implications of degree bound $\sigma$

**Theorem**

[IQS15a] Over $\mathbb{Q}$, if the nullcone is defined by elements of degree $\leqslant \sigma = \sigma(n, m)$,there exists a deterministic poly$(n, m, \sigma)$ algorithm deciding if $(B_1, B_2, \ldots, B_m)$ is in the null cone.

- If $(B_1, \ldots, B_m)$ is in the null cone all blow-ups $\mathcal{B}^{\{d,d\}}$ shrink a subspace.
- Else, for some $d \leqslant \sigma$, $\exists T_i \in Mat(d, \mathbb{F}), i = 1, \ldots, m$, $det(T_1 \otimes B_1 + T_2 \otimes B_2 + \ldots + T_m \otimes B_m) \neq 0$

# Implications of degree bound $\sigma$

**Theorem**

[IQS15a] Over $\mathbb{Q}$, if the nullcone is defined by elements of degree $\leqslant \sigma = \sigma(n,m)$,there exists a deterministic poly$(n,m,\sigma)$ algorithm deciding if $(B_1, B_2, \ldots, B_m)$ is in the null cone.

- If $(B_1, \ldots, B_m)$ is in the null cone all blow-ups $\mathcal{B}^{\{d,d\}}$ shrink a subspace.
- Else, for some $d \leqslant \sigma$, $\exists T_i \in Mat(d, \mathbb{F}), i = 1, \ldots, m$, $det(T_1 \otimes B_1 + T_2 \otimes B_2 + \ldots + T_m \otimes B_m) \neq 0$ i.e. $\mathcal{B}^{\{d,d\}}$ contains a nonsingular matrix.

# Implications of degree bound $\sigma$

**Theorem**

[IQS15a] Over $\mathbb{Q}$, if the nullcone is defined by elements of degree $\leqslant \sigma = \sigma(n, m)$,there exists a deterministic poly$(n, m, \sigma)$ algorithm deciding if $(B_1, B_2, \ldots, B_m)$ is in the null cone.

- If $(B_1, \ldots, B_m)$ is in the null cone all blow-ups $\mathcal{B}^{\{d,d\}}$ shrink a subspace.
- Else, for some $d \leqslant \sigma$, $\exists T_i \in Mat(d, \mathbb{F}), i = 1, \ldots, m$, $det(T_1 \otimes B_1 + T_2 \otimes B_2 + \ldots + T_m \otimes B_m) \neq 0$ i.e. $\mathcal{B}^{\{d,d\}}$ contains a nonsingular matrix.
- Gurvits promise condition is met at stage $d$.

# Implications of degree bound $\sigma$

**Theorem**

[IQS15a] Over $\mathbb{Q}$, if the nullcone is defined by elements of degree $\leqslant \sigma = \sigma(n, m)$,there exists a deterministic poly$(n, m, \sigma)$ algorithm deciding if $(B_1, B_2, \ldots, B_m)$ is in the null cone.

- If $(B_1, \ldots, B_m)$ is in the null cone all blow-ups $\mathcal{B}^{\{d,d\}}$ shrink a subspace.
- Else, for some $d \leqslant \sigma$, $\exists T_i \in Mat(d, \mathbb{F}), i = 1, \ldots, m$, $det(T_1 \otimes B_1 + T_2 \otimes B_2 + \ldots + T_m \otimes B_m) \neq 0$ i.e. $\mathcal{B}^{\{d,d\}}$ contains a nonsingular matrix.
- Gurvits promise condition is met at stage $d$.
- For $i = 1 : \sigma$ run Gurvits' algorithm on $\mathcal{B}^{i,i}$ :

# Implications of degree bound $\sigma$

**Theorem**

[IQS15a] Over $\mathbb{Q}$, if the nullcone is defined by elements of degree $\leqslant \sigma = \sigma(n, m)$,there exists a deterministic poly$(n, m, \sigma)$ algorithm deciding if $(B_1, B_2, \ldots, B_m)$ is in the null cone.

- If $(B_1, \ldots, B_m)$ is in the null cone all blow-ups $\mathcal{B}^{\{d,d\}}$ shrink a subspace.
- Else, for some $d \leqslant \sigma$, $\exists T_i \in Mat(d, \mathbb{F}), i = 1, \ldots, m$, $det(T_1 \otimes B_1 + T_2 \otimes B_2 + \ldots + T_m \otimes B_m) \neq 0$ i.e. $\mathcal{B}^{\{d,d\}}$ contains a nonsingular matrix.
- Gurvits promise condition is met at stage $d$.
- For $i = 1 : \sigma$ run Gurvits' algorithm on $\mathcal{B}^{i,i}$ :
- If Gurvits says $Rk(\mathcal{B}^{i,i}) = i * n$, output $Rk(\mathcal{B}) = n$; exit.

# Implications of degree bound $\sigma$

**Theorem**

[IQS15a] Over $\mathbb{Q}$, if the nullcone is defined by elements of degree $\leqslant \sigma = \sigma(n, m)$,there exists a deterministic poly$(n, m, \sigma)$ algorithm deciding if $(B_1, B_2, \ldots, B_m)$ is in the null cone.

- If $(B_1, \ldots, B_m)$ is in the null cone all blow-ups $\mathcal{B}^{\{d,d\}}$ shrink a subspace.
- Else, for some $d \leqslant \sigma$, $\exists T_i \in Mat(d, \mathbb{F}), i = 1, \ldots, m$, $det(T_1 \otimes B_1 + T_2 \otimes B_2 + \ldots + T_m \otimes B_m) \neq 0$ i.e. $\mathcal{B}^{\{d,d\}}$ contains a nonsingular matrix.
- Gurvits promise condition is met at stage $d$.
- For $i = 1 : \sigma$ run Gurvits' algorithm on $\mathcal{B}^{i,i}$ :
- If Gurvits says $Rk(\mathcal{B}^{i,i}) = i * n$, output $Rk(\mathcal{B}) = n$; exit.
- Output NCrk$(\mathcal{B}) < n$.

# Suggested algorithm

# Suggested algorithm

Can we modify the suggested algorithm suitably?

# Suggested algorithm

Can we modify the suggested algorithm suitably?
Recall If $\mathcal{B}$ shrinks $U$, then so will its $d$-th blow-up.

# Suggested algorithm

Can we modify the suggested algorithm suitably?
Recall If $\mathcal{B}$ shrinks $U$, then so will its $d$-th blow-up.

- for $i = 1, 2, \ldots,$ compute (a basis of) $\langle \mathcal{B}^{\{i,i\}} \rangle$,

# Suggested algorithm

Can we modify the suggested algorithm suitably?
Recall If $\mathcal{B}$ shrinks $U$, then so will its $d$-th blow-up.

- for $i = 1, 2, \ldots,$ compute (a basis of) $\langle \mathcal{B}^{\{i,i\}} \rangle$,
- determine if there is a nonsingular matrix in the blow-up.

# Suggested algorithm

Can we modify the suggested algorithm suitably?
Recall If $\mathcal{B}$ shrinks $U$, then so will its $d$-th blow-up.

- for $i = 1, 2, \ldots,$ compute (a basis of) $\langle \mathcal{B}^{\{i,i\}} \rangle$,
- determine if there is a nonsingular matrix in the blow-up.

However...finding a nonsingular matrix in the span will be difficult.

# Suggested algorithm

Can we modify the suggested algorithm suitably?
Recall If $\mathcal{B}$ shrinks $U$, then so will its $d$-th blow-up.

- for $i = 1, 2, \ldots,$ compute (a basis of) $\langle \mathcal{B}^{\{i,i\}} \rangle$,and a matrix $M_{i-1}$.
- ~~determine if there is a nonsingular matrix in the blow-up.~~

# Suggested algorithm

Can we modify the suggested algorithm suitably?
Recall If $\mathcal{B}$ shrinks $U$, then so will its $d$-th blow-up.

- for $i = 1, 2, \ldots,$ compute (a basis of) $\langle \mathcal{B}^{\{i,i\}} \rangle$,and a matrix $M_{i-1}$.
- ~~determine if there is a nonsingular matrix in the blow-up.~~
- Using $M_{i-1}$, update and get $M_i$, achieving some measurable progress.

# Outline

1. Background and problem statement
   - Problem statement
   - Invariant theory
2. Using Gurvits algorithm
3. Progress via Blow-ups
   - Regularity
   - Algorithmic and degree bounds
   - Degree bounds
   - Polynomial bound - degree of generation
   - Main lemma and blow ups using division algebras
   - Proof of the main lemma

# Regularity of Blow-ups

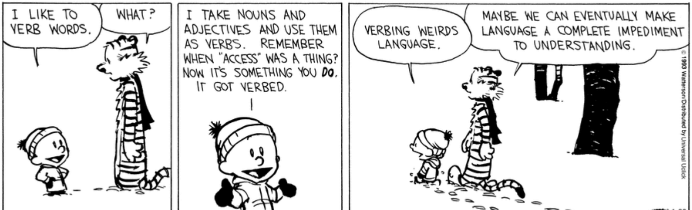
**Main Lemma**

For $\mathcal{B} \leqslant Mat(n, \mathbb{F})$ and $\mathcal{A} = \mathcal{B}^{\{d,d\}}$, assume that $|\mathbb{F}| > 2rd$. Given a matrix $A \in \mathcal{A}$ with $\mathrm{rk} A > (r-1)d$, there exists a deterministic algorithm that returns $\widetilde{A} \in \mathcal{A}$ and an $r \times r$ window $W$ in $\widetilde{A}$ s.t. $W$ is nonsingular (of rank $rd$). This algorithm uses $\mathrm{poly}(nd)$ operations and, over $\mathbb{Q}$, the algorithm runs in polynomial time.

# Regularity of Blow-ups

## Main Lemma

For $\mathcal{B} \leqslant \mathrm{Mat}(n, \mathbb{F})$ and $\mathcal{A} = \mathcal{B}^{\{d,d\}}$, assume that $|\mathbb{F}| > 2rd$. Given a matrix $A \in \mathcal{A}$ with $\mathrm{rk} A > (r-1)d$, there exists a deterministic algorithm that returns $\widetilde{A} \in \mathcal{A}$ and an $r \times r$ window $W$ in $\widetilde{A}$ s.t. $W$ is nonsingular (of rank $rd$). This algorithm uses $\mathrm{poly}(nd)$ operations and, over $\mathbb{Q}$, the algorithm runs in polynomial time.



# Regularity of Blow-ups

**Main Lemma**

For $\mathcal{B} \leqslant Mat(n, \mathbb{F})$ and $\mathcal{A} = \mathcal{B}^{\{d,d\}}$, assume that $|\mathbb{F}| > 2rd$. Given a matrix $A \in \mathcal{A}$ with $\mathrm{rk}A > (r-1)d$, there exists a deterministic algorithm that returns $\tilde{A} \in \mathcal{A}$ and an $r \times r$ window $W$ in $\tilde{A}$ s.t. $W$ is nonsingular (of rank $rd$). This algorithm uses $\mathrm{poly}(nd)$ operations and, over $\mathbb{Q}$, the algorithm runs in polynomial time.

The matrix with maximum rank in the $d$-th blow-up has rank a multiple of $d$.

# Regularity of Blow-ups

**Main Lemma**

For $\mathcal{B} \leqslant Mat(n, \mathbb{F})$ and $\mathcal{A} = \mathcal{B}^{\{d,d\}}$, assume that $|\mathbb{F}| > 2rd$. Given a matrix $A \in \mathcal{A}$ with $\mathrm{rk} A > (r-1)d$, there exists a deterministic algorithm that returns $\tilde{A} \in \mathcal{A}$ and an $r \times r$ window $W$ in $\tilde{A}$ s.t. $W$ is nonsingular (of rank $rd$). This algorithm uses $\mathrm{poly}(nd)$ operations and, over $\mathbb{Q}$, the algorithm runs in polynomial time.

The matrix with maximum rank in the $d$-th blow-up has rank a multiple of $d$.

Starting with a matrix of rank $(r-1)d + 1$ in $\mathcal{A}$, we construct a matrix of rank $rd$ in $\mathcal{A}$ - a constructive proof.

# Regularity of Blow-ups

**Main Lemma**

For $\mathcal{B} \leqslant Mat(n, \mathbb{F})$ and $\mathcal{A} = \mathcal{B}^{\{d,d\}}$, assume that $|\mathbb{F}| > 2rd$. Given a matrix $A \in \mathcal{A}$ with $\mathrm{rk} A > (r-1)d$, there exists a deterministic algorithm that returns $\tilde{A} \in \mathcal{A}$ and an $r \times r$ window $W$ in $\tilde{A}$ s.t. $W$ is nonsingular (of rank $rd$). This algorithm uses $\mathrm{poly}(nd)$ operations and, over $\mathbb{Q}$, the algorithm runs in polynomial time.

The matrix with maximum rank in the $d$-th blow-up has rank a multiple of $d$.

Starting with a matrix of rank $(r-1)d + 1$ in $\mathcal{A}$, we construct a matrix of rank $rd$ in $\mathcal{A}$ - a constructive proof.

Central division algebras almost do our job.

# Suggested algorithm

# Suggested algorithm

1. Start with a matrix in the given family $\mathcal{B}$ of rank $r$.

# Suggested algorithm

1. Start with a matrix in the given family $\mathcal{B}$ of rank $r$.
2. Determine if this is the matrix with largest rank in the family.

# Suggested algorithm

1. Start with a matrix in the given family $\mathcal{B}$ of rank $r$.
2. Determine if this is the matrix with largest rank in the family.
3. If not, consider the $r+1$-th blow blow up $\mathcal{A} = \mathcal{B}^{r+1,r+1}$.

# Suggested algorithm

1. Start with a matrix in the given family $\mathcal{B}$ of rank $r$.
2. Determine if this is the matrix with largest rank in the family.
3. If not, consider the $r+1$-th blow blow up $\mathcal{A} = \mathcal{B}^{r+1,r+1}$.
4. Starting with a rank $r$ matrix in this blow up, find a matrix of rank at least $r(r+1)+1$.

# Suggested algorithm

1. Start with a matrix in the given family $\mathcal{B}$ of rank $r$.
2. Determine if this is the matrix with largest rank in the family.
3. If not, consider the $r+1$-th blow blow up $\mathcal{A} = \mathcal{B}^{r+1,r+1}$.
4. Starting with a rank $r$ matrix in this blow up, find a matrix of rank at least $r(r+1)+1$.
5. Use regularity of blow-ups to get a matrix of rank $(r+1)*(r+1)$ in the blow up.

# Suggested algorithm

1. Start with a matrix in the given family $\mathcal{B}$ of rank $r$.
2. Determine if this is the matrix with largest rank in the family.
3. If not, consider the $r+1$-th blow blow up $\mathcal{A} = \mathcal{B}^{r+1,r+1}$.
4. Starting with a rank $r$ matrix in this blow up, find a matrix of rank at least $r(r+1)+1$.
5. Use regularity of blow-ups to get a matrix of rank $(r+1)*(r+1)$ in the blow up.
6. Loop back to step 2 with $\mathcal{B} = \mathcal{A}$ and $r = r+1$.

# Realizing the algorithm

# Realizing the algorithm

Issues to be addressed:

# Realizing the algorithm

Issues to be addressed:

- Finding if a matrix in a given family has the largest rank.

# Realizing the algorithm

Issues to be addressed:

- Finding if a matrix in a given family has the largest rank.
- Incrementing rank otherwise.

# Realizing the algorithm

Issues to be addressed:

- Finding if a matrix in a given family has the largest rank.
- Incrementing rank otherwise.
- Finding a matrix with rank a multiple of the blow-up factor.

# Realizing the algorithm

Issues to be addressed:

- Finding if a matrix in a given family has the largest rank.
- Incrementing rank otherwise.
- Finding a matrix with rank a multiple of the blow-up factor.
- Keeping the size of matrix entries polynomial.

# Realizing the algorithm

Issues to be addressed:

- Finding if a matrix in a given family has the largest rank.
- Incrementing rank otherwise.
- Finding a matrix with rank a multiple of the blow-up factor.
- Keeping the size of matrix entries polynomial.
- Blowing down matrices to keep matrix size polynomial.

# Realizing the algorithm

Issues to be addressed:

- Finding if a matrix in a given family has the largest rank.
- Incrementing rank otherwise.
- Finding a matrix with rank a multiple of the blow-up factor.
- Keeping the size of matrix entries polynomial.
- Blowing down matrices to keep matrix size polynomial.

- Knowing when to stop.

# Realizing the algorithm

Issues to be addressed:

- Finding if a matrix in a given family has the largest rank.
- Incrementing rank otherwise.
- Finding a matrix with rank a multiple of the blow-up factor.
- Keeping the size of matrix entries polynomial.
- Blowing down matrices to keep matrix size polynomial.
- Identifying the shrunk subspace, if any.
- Knowing when to stop.

# Upper bounds

# Upper bounds

- [Der01] Over algebraically closed fields of characteristic zero, $\sigma = O(n^2 4^{n^2})$. The invariant ring is generated in degree $\beta = O(n^2\sigma^2)$.

# Upper bounds

- [Der01] Over algebraically closed fields of characteristic zero, $\sigma = O(n^2 4^{n^2})$. The invariant ring is generated in degree $\beta = O(n^2 \sigma^2)$.
- [IQS15a] When $\mathbb{F}$ is large, a $poly(n+1!)$ algorithm for computing $Rk(\mathcal{B})$ so $\sigma \leqslant n+1!$. Over algebraically closed fields of char 0, $\beta = O(n^4 (n+1!)^2)$.

# Upper bounds

- [Der01] Over algebraically closed fields of characteristic zero, $\sigma = O(n^2 4^{n^2})$. The invariant ring is generated in degree $\beta = O(n^2\sigma^2)$.
- [IQS15a] When $\mathbb{F}$ is large, a $poly(n+1!)$ algorithm for computing $Rk(\mathcal{B})$ so $\sigma \leqslant n+1!$. Over algebraically closed fields of char 0, $\beta = O(n^4(n+1!)^2)$.
- [GGOW15] used the degree bound from [IQS15a] - give a polynomial time algorithm for the nullcone membership over fields of characteristic zero.

# Upper bounds

- [Der01] Over algebraically closed fields of characteristic zero, $\sigma = O(n^2 4^{n^2})$. The invariant ring is generated in degree $\beta = O(n^2\sigma^2)$.
- [IQS15a] When $\mathbb{F}$ is large, a $poly(n+1!)$ algorithm for computing $Rk(\mathcal{B})$ so $\sigma \leqslant n+1!$. Over algebraically closed fields of char 0, $\beta = O(n^4(n+1!)^2)$.
- [GGOW15] used the degree bound from [IQS15a] - give a polynomial time algorithm for the nullcone membership over fields of characteristic zero.
- [DM15] use the regularity under blow-up lemma of [IQS15a], and a convexity argument - $\sigma \leqslant O(n^2)$, over algebraically closed fields, $\beta = O(n^6)$.

# Upper bounds

- [Der01] Over algebraically closed fields of characteristic zero, $\sigma = O(n^2 4^{n^2})$. The invariant ring is generated in degree $\beta = O(n^2\sigma^2)$.
- [IQS15a] When $\mathbb{F}$ is large, a $poly(n+1!)$ algorithm for computing $Rk(\mathcal{B})$ so $\sigma \leqslant n+1!$. Over algebraically closed fields of char 0, $\beta = O(n^4(n+1!)^2)$.
- [GGOW15] used the degree bound from [IQS15a] - give a polynomial time algorithm for the nullcone membership over fields of characteristic zero.
- [DM15] use the regularity under blow-up lemma of [IQS15a], and a convexity argument - $\sigma \leqslant O(n^2)$, over algebraically closed fields, $\beta = O(n^6)$.
- [IQS15b] Show $\sigma \leqslant O(n^2)$ over all large fields. Two proofs - a constructive version of [DM15] and a simple proof based on regularity under blow-up. Get the above results.

# Blow-up upper bound of $n + 1$

# Blow-up upper bound of $n+1$

## Generation of the invariant ring in poly($n$)-degree

[DM15]. If there is no nonsingular matrix in $\mathcal{B}^{n+1,n+1}$, then there is no nonsingular matrix in $\mathcal{B}^{d,d}$, for all $d \geqslant n+1$. Over infinite fields the null cone is cut by invariants of degree $O(n^2)$. Over $\overline{\mathbb{Q}}$ the ring of invariants is generated in degree $O(n^6)$.

# Blow-up upper bound of $n + 1$

**Generation of the invariant ring in poly($n$)-degree**

[DM15]. If there is no nonsingular matrix in $\mathcal{B}^{n+1,n+1}$, then there is no nonsingular matrix in $\mathcal{B}^{d,d}$, for all $d \geqslant n + 1$. Over infinite fields the null cone is cut by invariants of degree $O(n^2)$. Over $\overline{\mathbb{Q}}$ the ring of invariants is generated in degree $O(n^6)$.

Proof [IQS15b]

# Blow-up upper bound of $n+1$

## Generation of the invariant ring in poly($n$)-degree

[DM15]. If there is no nonsingular matrix in $\mathcal{B}^{n+1,n+1}$, then there is no nonsingular matrix in $\mathcal{B}^{d,d}$, for all $d \geqslant n+1$. Over infinite fields the null cone is cut by invariants of degree $O(n^2)$. Over $\overline{\mathbb{Q}}$ the ring of invariants is generated in degree $O(n^6)$.

Proof [IQS15b]

- Take $d = n+2$.

# Blow-up upper bound of $n + 1$

## Generation of the invariant ring in poly($n$)-degree

[DM15]. If there is no nonsingular matrix in $\mathcal{B}^{n+1,n+1}$, then there is no nonsingular matrix in $\mathcal{B}^{d,d}$, for all $d \geqslant n + 1$. Over infinite fields the null cone is cut by invariants of degree $O(n^2)$. Over $\overline{\mathbb{Q}}$ the ring of invariants is generated in degree $O(n^6)$.

Proof [IQS15b]

- Take $d = n + 2$.
- So the largest ranked matrix in a $n + 1 \times n + 1$ window is $(n + 1) * (n - 1) = n^2 - 1$.

# Blow-up upper bound of $n + 1$

## Generation of the invariant ring in poly($n$)-degree

[DM15]. If there is no nonsingular matrix in $\mathcal{B}^{n+1,n+1}$, then there is no nonsingular matrix in $\mathcal{B}^{d,d}$, for all $d \geqslant n + 1$. Over infinite fields the null cone is cut by invariants of degree $O(n^2)$. Over $\overline{\mathbb{Q}}$ the ring of invariants is generated in degree $O(n^6)$.

Proof [IQS15b]

- Take $d = n + 2$.
- So the largest ranked matrix in a $n + 1 \times n + 1$ window is $(n + 1) * (n - 1) = n^2 - 1$.
- But we add to such a matrix at most $2n$ linearly independent rows and columns.

# Blow-up upper bound of $n+1$

## Generation of the invariant ring in poly($n$)-degree

[DM15]. If there is no nonsingular matrix in $\mathcal{B}^{n+1,n+1}$, then there is no nonsingular matrix in $\mathcal{B}^{d,d}$, for all $d \geqslant n+1$. Over infinite fields the null cone is cut by invariants of degree $O(n^2)$. Over $\overline{\mathbb{Q}}$ the ring of invariants is generated in degree $O(n^6)$.

Proof [IQS15b]

- Take $d = n+2$.
- So the largest ranked matrix in a $n+1 \times n+1$ window is $(n+1)*(n-1) = n^2 - 1$.
- But we add to such a matrix at most $2n$ linearly independent rows and columns.
- So rank is upper bounded by $n^2 - 1 + 2n$,

.

# Blow-up upper bound of $n+1$

## Generation of the invariant ring in poly($n$)-degree

[DM15]. If there is no nonsingular matrix in $\mathcal{B}^{n+1,n+1}$, then there is no nonsingular matrix in $\mathcal{B}^{d,d}$, for all $d \geqslant n+1$. Over infinite fields the null cone is cut by invariants of degree $O(n^2)$. Over $\overline{\mathbb{Q}}$ the ring of invariants is generated in degree $O(n^6)$.

Proof [IQS15b]

- Take $d = n+2$.
- So the largest ranked matrix in a $n+1 \times n+1$ window is $(n+1)*(n-1) = n^2 - 1$.
- But we add to such a matrix at most $2n$ linearly independent rows and columns.
- So rank is upper bounded by $n^2 - 1 + 2n$, cannot be $(n+2)*n$.

# Blow-up upper bound of $n+1$

## Generation of the invariant ring in poly($n$)-degree

[DM15]. If there is no nonsingular matrix in $\mathcal{B}^{n+1,n+1}$, then there is no nonsingular matrix in $\mathcal{B}^{d,d}$, for all $d \geqslant n+1$. Over infinite fields the null cone is cut by invariants of degree $O(n^2)$. Over $\overline{\mathbb{Q}}$ the ring of invariants is generated in degree $O(n^6)$.

Proof [IQS15b]

- Take $d = n+2$.
- So the largest ranked matrix in a $n+1 \times n+1$ window is $(n+1)*(n-1) = n^2-1$.
- But we add to such a matrix at most $2n$ linearly independent rows and columns.
- So rank is upper bounded by $n^2-1+2n$, cannot be $(n+2)*n$. Regularity says rank is at most $(n+2)*(n-1) = n^2+n-2$. QED

# Blowing-up using a division algebra.

# Blowing-up using a division algebra.

## Claim

Let $\mathbb{F}'$ be an extension field of $\mathbb{F}$, and Let $D$ be a central division algebra over $\mathbb{F}'$ of dimension $d^2$ over $\mathbb{F}'$, and let $\mathbb{K}$ be a maximal field in $D$ with extension degree $d$ over $\mathbb{F}'$. Let $\rho : D \to Mat(d, \mathbb{K})$ be a representation of $D$ over $\mathbb{K}$. Then every matrix in $Mat(n, \mathbb{F}) \otimes_{\mathbb{F}} \rho(D)$ has rank divisible by $d$ over $\mathbb{K}$.

# Blowing-up using a division algebra.

**Claim**

Let $\mathbb{F}'$ be an extension field of $\mathbb{F}$, and Let $D$ be a central division algebra over $\mathbb{F}'$ of dimension $d^2$ over $\mathbb{F}'$, and let $\mathbb{K}$ be a maximal field in $D$ with extension degree $d$ over $\mathbb{F}'$. Let $\rho : D \to Mat(d, \mathbb{K})$ be a representation of $D$ over $\mathbb{K}$. Then every matrix in $Mat(n, \mathbb{F}) \otimes_{\mathbb{F}} \rho(D)$ has rank divisible by $d$ over $\mathbb{K}$.

- $D \otimes \mathbb{K} \cong Mat(\mathbb{K})$. Explicit matrices describing the $\mathbb{F}'$-algebra $D \cong D \otimes 1$ can be written down easily.

# Blowing-up using a division algebra.

**Claim**

Let $\mathbb{F}'$ be an extension field of $\mathbb{F}$, and Let $D$ be a central division algebra over $\mathbb{F}'$ of dimension $d^2$ over $\mathbb{F}'$, and let $\mathbb{K}$ be a maximal field in $D$ with extension degree $d$ over $\mathbb{F}'$. Let $\rho : D \to Mat(d, \mathbb{K})$ be a representation of $D$ over $\mathbb{K}$. Then every matrix in $Mat(n, \mathbb{F}) \otimes_{\mathbb{F}} \rho(D)$ has rank divisible by $d$ over $\mathbb{K}$.

- $D \otimes \mathbb{K} \cong Mat(\mathbb{K})$. Explicit matrices describing the $\mathbb{F}'$-algebra $D \cong D \otimes 1$ can be written down easily.
- Regard $\mathbb{K}^{dn} \cong \mathbb{F}'^{d^2 n}$ as a module over $Mat(n, \mathbb{F}) \otimes_{\mathbb{F}} \rho(D)$.

# Blowing-up using a division algebra.

## Claim

Let $\mathbb{F}'$ be an extension field of $\mathbb{F}$, and Let $D$ be a central division algebra over $\mathbb{F}'$ of dimension $d^2$ over $\mathbb{F}'$, and let $\mathbb{K}$ be a maximal field in $D$ with extension degree $d$ over $\mathbb{F}'$. Let $\rho : D \to \mathrm{Mat}(d, \mathbb{K})$ be a representation of $D$ over $\mathbb{K}$. Then every matrix in $\mathrm{Mat}(n, \mathbb{F}) \otimes_{\mathbb{F}} \rho(D)$ has rank divisible by $d$ over $\mathbb{K}$.

- $D \otimes \mathbb{K} \cong \mathrm{Mat}(\mathbb{K})$. Explicit matrices describing the $\mathbb{F}'$-algebra $D \cong D \otimes 1$ can be written down easily.
- Regard $\mathbb{K}^{dn} \cong \mathbb{F}'^{d^2 n}$ as a module over $\mathrm{Mat}(n, \mathbb{F}) \otimes_{\mathbb{F}} \rho(D)$.
- Since $D \otimes D^{op} \cong \mathrm{Mat}(d, \mathbb{F}') \subset \mathrm{Mat}(\mathbb{K})$, the centralizer of the action of $\mathrm{Mat}(n, \mathbb{F}) \otimes_{\mathbb{F}} \rho(D)$ is $\mathrm{id} \otimes D^{op} \cong D^{op}$.

# Blowing-up using a division algebra.

## Claim

Let $\mathbb{F}'$ be an extension field of $\mathbb{F}$, and Let $D$ be a central division algebra over $\mathbb{F}'$ of dimension $d^2$ over $\mathbb{F}'$, and let $\mathbb{K}$ be a maximal field in $D$ with extension degree $d$ over $\mathbb{F}'$. Let $\rho : D \to Mat(d, \mathbb{K})$ be a representation of $D$ over $\mathbb{K}$. Then every matrix in $Mat(n, \mathbb{F}) \otimes_{\mathbb{F}} \rho(D)$ has rank divisible by $d$ over $\mathbb{K}$.

- $D \otimes \mathbb{K} \simeq Mat(\mathbb{K})$. Explicit matrices describing the $\mathbb{F}'$-algebra $D \simeq D \otimes 1$ can be written down easily.
- Regard $\mathbb{K}^{dn} \simeq \mathbb{F}'^{d^2 n}$ as a module over $Mat(n, \mathbb{F}) \otimes_{\mathbb{F}} \rho(D)$.
- Since $D \otimes D^{op} \simeq Mat(d, \mathbb{F}') \subset Mat(\mathbb{K})$, the centralizer of the action of $Mat(n, \mathbb{F}) \otimes_{\mathbb{F}} \rho(D)$ is $id \otimes D^{op} \simeq D^{op}$.
- For all $A$ in $Mat(n, \mathbb{F}) \otimes_{\mathbb{F}} \rho(D)$, $A\mathbb{F}'^{d^2 n}$ is a $D^{op}$-submodule, and so its dimension over $\mathbb{F}'$ is divisible by $d^2$, so dimension over $\mathbb{K}$ is divisible by $d$. But this is the rank of $A'$.

# Recap

**Main Lemma**

For $\mathcal{B} \leqslant Mat(n, \mathbb{F})$ and $\mathcal{A} = \mathcal{B}^{\{d,d\}}$, assume that $|\mathbb{F}| > 2rd$. Given a matrix $A \in \mathcal{A}$ with $\mathrm{rk} A > (r-1)d$, there exists a deterministic algorithm that returns $\widetilde{A} \in \mathcal{A}$ and an $r \times r$ window $W$ in $\widetilde{A}$ s.t. $W$ is nonsingular (of rank $rd$). This algorithm uses $\mathrm{poly}(nd)$ operations and, over $\mathbb{Q}$, the algorithm runs in polynomial time.

# Proof

# Proof

- Assuming we have a division algebra and a representation of it.

# Proof

- Assuming we have a division algebra and a representation of it.
- Induction on $r$: Base case: $r = 1$ - there is at least one nonzero matrix $B$ in $\mathcal{B}$; $(i, j)$-th entry is nonzero then we have a $d \times d$ block in $B \otimes I$ which is non zero, of rank $d$.

# Proof

- Assuming we have a division algebra and a representation of it.
- Induction on $r$: Base case: $r = 1$ - there is at least one nonzero matrix $B$ in $\mathcal{B}$; $(i, j)$-th entry is nonzero then we have a $d \times d$ block in $B \otimes I$ which is non zero, of rank $d$.
- By induction, the principal $(r - 1)$ window of $A' \in \mathcal{A} = \mathcal{B}^{\{d,d\}}$ has non-zero determinant.

# Proof

- Assuming we have a division algebra and a representation of it.
- Induction on $r$: Base case: $r = 1$ - there is at least one nonzero matrix $B$ in $\mathcal{B}$; $(i, j)$-th entry is nonzero then we have a $d \times d$ block in $B \otimes I$ which is non zero, of rank $d$.
- By induction, the principal $(r-1)$ window of $A' \in \mathcal{A} = \mathcal{B}^{\{d,d\}}$ has non-zero determinant. $\exists \lambda, \mu$, with the principal $r-1$ window of $\lambda * A + \mu A'$ having non-zero determinant and the principal $r$-window having rank at least $(r-1)d + 1$.

# Proof

- Assuming we have a division algebra and a representation of it.
- Induction on $r$: Base case: $r = 1$ - there is at least one nonzero matrix $B$ in $\mathcal{B}$; $(i, j)$-th entry is nonzero then we have a $d \times d$ block in $B \otimes I$ which is non zero, of rank $d$.
- By induction, the principal $(r - 1)$ window of $A' \in \mathcal{A} = \mathcal{B}^{\{d,d\}}$ has non-zero determinant. $\exists \lambda, \mu$, with the principal $r - 1$ window of $\lambda * A + \mu A'$ having non-zero determinant and the principal $r$-window having rank at least $(r - 1)d + 1$.
- Wlog we have matrix of rank at least $(n - 1)d + 1$ with the principal $n - 1$ window having a nonsingular matrix.

# Proof of main lemma .....

# Proof of main lemma .....

- Let $\rho : D \to Mat(d, \mathbb{K})$, be a representation of $D$.

# Proof of main lemma .....

- Let $\rho : D \to Mat(d, \mathbb{K})$, be a representation of $D$.
- $\mathcal{A}' := \mathcal{A} \otimes Mat(d, \mathbb{K})$. Then $\mathcal{A}' = \mathcal{B} \otimes Mat(d, \mathbb{K})$ is a $\mathbb{K}$-linear subspace of $Mat(n, \mathbb{K}) \otimes Mat(d, \mathbb{K})$.

# Proof of main lemma .....

- Let $\rho : D \to Mat(d, \mathbb{K})$, be a representation of $D$.
- $\mathcal{A}' := \mathcal{A} \otimes Mat(d, \mathbb{K})$. Then $\mathcal{A}' = \mathcal{B} \otimes Mat(d, \mathbb{K})$ is a $\mathbb{K}$-linear subspace of $Mat(n, \mathbb{K}) \otimes Mat(d, \mathbb{K})$.
- $\mathcal{B} \otimes_{\mathbb{F}} \rho(D)$ is an $\mathbb{F}'$ linear space. Its $\mathbb{K}$ linear span is $\mathcal{A}'$.

# Proof of main lemma .....

- Let $\rho : D \rightarrow Mat(d, \mathbb{K})$, be a representation of $D$.
- $\mathcal{A}' := \mathcal{A} \otimes Mat(d, \mathbb{K})$. Then $\mathcal{A}' = \mathcal{B} \otimes Mat(d, \mathbb{K})$ is a $\mathbb{K}$-linear subspace of $Mat(n, \mathbb{K}) \otimes Mat(d, \mathbb{K})$.
- $\mathcal{B} \otimes_{\mathbb{F}} \rho(D)$ is an $\mathbb{F}'$ linear space. Its $\mathbb{K}$ linear span is $\mathcal{A}'$.
- Starting with the matrix $A$, get a matrix $\tilde{A}$ in $\mathcal{B} \otimes_{\mathbb{F}} \rho(D)$ of the same rank, so rank is at least $(n-1)d + 1$.

# Proof of main lemma .....

- Let $\rho : D \to Mat(d, \mathbb{K})$, be a representation of $D$.
- $\mathcal{A}' := \mathcal{A} \otimes Mat(d, \mathbb{K})$. Then $\mathcal{A}' = \mathcal{B} \otimes Mat(d, \mathbb{K})$ is a $\mathbb{K}$-linear subspace of $Mat(n, \mathbb{K}) \otimes Mat(d, \mathbb{K})$.
- $\mathcal{B} \otimes_{\mathbb{F}} \rho(D)$ is an $\mathbb{F}'$ linear space. Its $\mathbb{K}$ linear span is $\mathcal{A}'$.
- Starting with the matrix $A$, get a matrix $\tilde{A}$ in $\mathcal{B} \otimes_{\mathbb{F}} \rho(D)$ of the same rank, so rank is at least $(n-1)d + 1$.
- All matrices in $\mathcal{B} \otimes_{\mathbb{F}} \rho(D)$ have rank $nd$ (over $\mathbb{K}$) so $\tilde{A}$ has rank $nd$

# Proof of main lemma .....

- Let $\rho : D \to Mat(d, \mathbb{K})$, be a representation of $D$.
- $\mathcal{A}' := \mathcal{A} \otimes Mat(d, \mathbb{K})$. Then $\mathcal{A}' = \mathcal{B} \otimes Mat(d, \mathbb{K})$ is a $\mathbb{K}$-linear subspace of $Mat(n, \mathbb{K}) \otimes Mat(d, \mathbb{K})$.
- $\mathcal{B} \otimes_{\mathbb{F}} \rho(D)$ is an $\mathbb{F}'$ linear space. Its $\mathbb{K}$ linear span is $\mathcal{A}'$.
- Starting with the matrix $A$, get a matrix $\tilde{A}$ in $\mathcal{B} \otimes_{\mathbb{F}} \rho(D)$ of the same rank, so rank is at least $(n-1)d + 1$.
- All matrices in $\mathcal{B} \otimes_{\mathbb{F}} \rho(D)$ have rank $nd$ (over $\mathbb{K}$) so $\tilde{A}$ has rank $nd$
- Because $\mathbb{F} \geqslant 2nd$, we can find a matrix in $\mathcal{A}$ of rank $nd$ using ideas from [dGIR96].

# Proof of main lemma .....

- Let $\rho : D \to Mat(d, \mathbb{K})$, be a representation of $D$.
- $\mathcal{A}' := \mathcal{A} \otimes Mat(d, \mathbb{K})$. Then $\mathcal{A}' = \mathcal{B} \otimes Mat(d, \mathbb{K})$ is a $\mathbb{K}$-linear subspace of $Mat(n, \mathbb{K}) \otimes Mat(d, \mathbb{K})$.
- $\mathcal{B} \otimes_{\mathbb{F}} \rho(D)$ is an $\mathbb{F}'$ linear space. Its $\mathbb{K}$ linear span is $\mathcal{A}'$.
- Starting with the matrix $A$, get a matrix $\tilde{A}$ in $\mathcal{B} \otimes_{\mathbb{F}} \rho(D)$ of the same rank, so rank is at least $(n-1)d + 1$.
- All matrices in $\mathcal{B} \otimes_{\mathbb{F}} \rho(D)$ have rank $nd$ (over $\mathbb{K}$) so $\tilde{A}$ has rank $nd$
- Because $\mathbb{F} \geqslant 2nd$, we can find a matrix in $\mathcal{A}$ of rank $nd$ using ideas from [dGIR96].
- We need to construct division algebras, and be able to compute with them, at each stage

# Using extension fields [dGIR96].

# Using extension fields [dGIR96].

- Assume $\mathbb{K}$ is an extension of $\mathbb{F}$ and you have a matrix in $\mathcal{B} \otimes Mat(d, \mathbb{K})$ of rank $r$. Let $S \subset \mathbb{F}$ of size at least $r$.

# Using extension fields [dGIR96].

- Assume $\mathbb{K}$ is an extension of $\mathbb{F}$ and you have a matrix in $\mathcal{B} \otimes Mat(d, \mathbb{K})$ of rank $r$. Let $S \subset \mathbb{F}$ of size at least $r$.
- Let $B_1, \ldots, B_l$ be a $\mathbb{F}$ basis of $\mathcal{B}$. Then $A = a_1' B_1 + a_2' B_2 + \ldots + a_l' B_l$, and there is a $r \times r$ window in $A$ with nonzero determinant, say the principal $r$ window.

# Using extension fields [dGIR96].

- Assume $\mathbb{K}$ is an extension of $\mathbb{F}$ and you have a matrix in $\mathcal{B} \otimes Mat(d, \mathbb{K})$ of rank $r$. Let $S \subset \mathbb{F}$ of size at least $r$.
- Let $B_1, \ldots, B_l$ be a $\mathbb{F}$ basis of $\mathcal{B}$. Then $A = a'_1 B_1 + a'_2 B_2 + \ldots + a'_l B_l$, and there is a $r \times r$ window in $A$ with nonzero determinant, say the principal $r$ window.
- As a polynomial in $x$, the determinant of the principal $r$ window $xB_1 + a'_2 B_2 + \ldots + a'_l B_l$ is non zero. This is of degree $r$. Since $S$ has more than $r$ elements there is an $a_1 \in S \subset \mathbb{F}$ such that the determinant $a_1 B_1 + a'_2 B_2 + \ldots + a'_l B_l$ is non zero.

# Using extension fields [dGIR96].

- Assume $\mathbb{K}$ is an extension of $\mathbb{F}$ and you have a matrix in $\mathcal{B} \otimes Mat(d, \mathbb{K})$ of rank $r$. Let $S \subset \mathbb{F}$ of size at least $r$.
- Let $B_1, \ldots, B_l$ be a $\mathbb{F}$ basis of $\mathcal{B}$. Then $A = a'_1 B_1 + a'_2 B_2 + \ldots + a'_l B_l$, and there is a $r \times r$ window in $A$ with nonzero determinant, say the principal $r$ window.
- As a polynomial in $x$, the determinant of the principal $r$ window $xB_1 + a'_2 B_2 + \ldots + a'_l B_l$ is non zero. This is of degree $r$. Since $S$ has more than $r$ elements there is an $a_1 \in S \subset \mathbb{F}$ such that the determinant $a_1 B_1 + a'_2 B_2 + \ldots + a'_l B_l$ is non zero.
- Complete the proof by recursion, substituting values for $a'_2, a'_3, \ldots, a'_l$.

# Second Wong sequence [IKQS14]

# Second Wong sequence [IKQS14]

**Definition**

Given $(A, \mathcal{B})$, $A \in \mathrm{Mat}(n, \mathbb{F})$ and $\mathcal{B} \leqslant \mathrm{Mat}(n, \mathbb{F})$, the second Wong sequence of $(A, \mathcal{B})$ is the following sequence of subspaces in $\mathbb{F}^n$: $W_0 = 0$, $W_1 = \mathcal{B}(A^{-1}(W_0))$, ..., $W_i = \mathcal{B}(A^{-1}(W_{i-1}))$, ....

# Second Wong sequence [IKQS14]

**Definition**

Given $(A, \mathcal{B})$, $A \in \mathrm{Mat}(n, \mathbb{F})$ and $\mathcal{B} \leqslant \mathrm{Mat}(n, \mathbb{F})$, the second Wong sequence of $(A, \mathcal{B})$ is the following sequence of subspaces in $\mathbb{F}^n$: $W_0 = 0$, $W_1 = \mathcal{B}(A^{-1}(W_0)), \ldots,$ $W_i = \mathcal{B}(A^{-1}(W_{i-1})), \ldots.$

- $W_0 < W_1 < W_2 < \cdots < W_\ell = W_{\ell+1} = \ldots$ for some $\ell \in \{0, 1, \ldots, n\}$. $W_\ell$ is then called the limit of this sequence, denoted as $W^*$.

# Second Wong sequence [IKQS14]

**Definition**

Given $(A, \mathcal{B})$, $A \in \mathrm{Mat}(n, \mathbb{F})$ and $\mathcal{B} \leqslant \mathrm{Mat}(n, \mathbb{F})$, the second Wong sequence of $(A, \mathcal{B})$ is the following sequence of subspaces in $\mathbb{F}^n$: $W_0 = 0$, $W_1 = \mathcal{B}(A^{-1}(W_0)), \ldots,$ $W_i = \mathcal{B}(A^{-1}(W_{i-1})), \ldots$.

- $W_0 < W_1 < W_2 < \cdots < W_\ell = W_{\ell+1} = \ldots$ for some $\ell \in \{0, 1, \ldots, n\}$. $W_\ell$ is then called the limit of this sequence, denoted as $W^*$.
- When $A \in \mathcal{B}$, $W^* \leqslant \mathrm{im}(A)$ if and only if there exists a corank$(A)$-shrunk subspace

# Second Wong sequence [IKQS14]

**Definition**

Given $(A, \mathcal{B})$, $A \in \mathrm{Mat}(n, \mathbb{F})$ and $\mathcal{B} \leqslant \mathrm{Mat}(n, \mathbb{F})$, the second Wong sequence of $(A, \mathcal{B})$ is the following sequence of subspaces in $\mathbb{F}^n$: $W_0 = 0$, $W_1 = \mathcal{B}(A^{-1}(W_0))$, ..., $W_i = \mathcal{B}(A^{-1}(W_{i-1}))$, ....

- $W_0 < W_1 < W_2 < \cdots < W_\ell = W_{\ell+1} = \ldots$ for some $\ell \in \{0, 1, \ldots, n\}$. $W_\ell$ is then called the limit of this sequence, denoted as $W^*$.
- When $A \in \mathcal{B}$, $W^* \leqslant \mathrm{im}(A)$ if and only if there exists a corank$(A)$-shrunk subspace
- $A$ is of maximum rank and $A^{-1}(W^*)$ is a corank($A$)-shrunk subspace.

# Using the second Wong sequence

# Using the second Wong sequence

- What if $A$ is not of maximum rank in $\mathcal{B}^{\{d,d\}}$?

# Using the second Wong sequence

- What if $A$ is not of maximum rank in $\mathcal{B}^{\{d,d\}}$?

## Incrementing rank

Let $\mathcal{B} \leqslant \mathrm{Mat}(n, \mathbb{F})$ and let $\mathcal{A} = \mathcal{B}^{\{d,d\}}$. Assume that we are given a matrix $A \in \mathcal{A}$ with $\mathrm{rk}(A) = rd$, and $|\mathbb{F}|$ is $\Omega(ndd')$, where $d' > r$ is any positive integer. There exists a deterministic algorithm that returns either an $(n-r)d$-shrunk subspace for $\mathcal{A}$ (equivalently, an $(n-r)$-shrunk subspace for $\mathcal{B}$), or a matrix $B \in \mathcal{A} \otimes \mathrm{Mat}(d', \mathbb{F})$ of rank at least $(r+1)dd'$.

# Cyclic algebras and the construction of Dickson

- Let $\mathbb{K}/\mathbb{F}$ be a Galois extension with cyclic Galois group. Let $\sigma$ be a generator of the Galois group and $s = dim_{\mathbb{F}}(\mathbb{K})$.
- Take $f \in \mathbb{F}$ and a symbol $x$, and consider $D = \mathbb{K} \bigoplus \mathbb{K} \cdot x \bigoplus \mathbb{K} \cdot x^2 + \ldots \mathbb{K} \cdot x^{s-1}$.
- Multiply elements in $D$ using the distributive law and using $x^s = f$ and $x \cdot b = \sigma(b)x$ for all $b \in K$.
- $\mathbb{F}$ i in the center of $D$ and so $D$ is an $\mathbb{F}$-algebra. Dimension over $\mathbb{F}$ is $s^2$.
- Wedderburn - if $f, f^2, \ldots, f^{s-1}$ are not in Norm$(\mathbb{K})$, then $D$ is a division algebra, and in this case $D \otimes_{\mathbb{F}} \mathbb{K} \cong Mat(\mathbb{K})$.

# Blowing-down a shrunk subspace

# Blowing-down a shrunk subspace

## Shrinking by a factor of $d$

If $\mathcal{A} = \mathcal{B}^{\{d,d\}}$ has an $s$-shrunk subspace, then $\mathcal{A}$ has an $s'$-shrunk subspace with $s' \geqslant s$ and s.t. $d$ divides $s'$. $\mathcal{B}$ has an $s'/d$-shrunk subspace.

# Blowing-down a shrunk subspace

**Shrinking by a factor of $d$**

If $\mathcal{A} = \mathcal{B}^{\{d,d\}}$ has an $s$-shrunk subspace, then $\mathcal{A}$ has an $s'$-shrunk subspace with $s' \geqslant s$ and s.t. $d$ divides $s'$. $\mathcal{B}$ has an $s'/d$-shrunk subspace.

Idea Maximal shrunk subspaces are of the form $U_o \otimes \mathbb{F}^d$ and their image under $\mathcal{A}$ is of the form $W_o \otimes \mathbb{F}^d$.

# Blowing-down

# Blowing-down

### Reducing the size of blow-ups

Let $\mathcal{B} \leqslant \mathrm{Mat}(n, \mathbb{F})$, and $d > n+1$. Assume we are given a matrix $A \in \mathcal{B}^{\{d,d\}}$ of rank $dn$. Then there exists a deterministic polynomial-time procedure that constructs $A' \in \mathcal{B}^{\{d-1,d-1\}}$ of rank $(d-1)n$.

## Construction of division algebras

Let $L$ be a cyclic extension of degree $d$ of a field $K'$. Let $\sigma$ be a generator of the Galois group. Consider the transcendental extension $L(Z)$ of $L$. Then $\sigma$ extends to an automorphism (denoted again by $\sigma$) of $L(Z)$ such that the fixed field of $\sigma$ is $K'(Z)$. Thus $L(Z)$ is a cyclic extension of $K'(Z)$. Consider the $K'(Z)$-algebra $D$ generated by (a basis for) $L$ and by an element $U$ with relations $U^d = Z$ and $Ua = a^\sigma U$ ($\forall a \in L(Z)$, or, equivalently $\forall a \in$ the basis for $L$). Then $D$ is a central division algebra of index $d$ over $K'(Z)$.

# Open problems

# Open problems

- Get a combinatorial algorithm in characteristic zero.

# Open problems

- Get a combinatorial algorithm in characteristic zero.
- Is there an augmenting path algorithm?

# Open problems

- Get a combinatorial algorithm in characteristic zero.
- Is there an augmenting path algorithm?
- For the GCT programme, desingularizing the null cone may be important - this may help isolate points which are in the border.

# Open problems

- Get a combinatorial algorithm in characteristic zero.
- Is there an augmenting path algorithm?
- For the GCT programme, desingularizing the null cone may be important - this may help isolate points which are in the border.
- Orbit closure problem for the left right action

# Open problems

- Get a combinatorial algorithm in characteristic zero.
- Is there an augmenting path algorithm?
- For the GCT programme, desingularizing the null cone may be important - this may help isolate points which are in the border.
- Orbit closure problem for the left right action .. NNL for this invariant ring.

# References I


- B. Adsul, S. Nayak, and K. V. Subrahmanyam.
  A geometric approach to the Kronecker problem II: rectangular shapes, invariants of matrices and the Artin–Procesi theorem.
  preprint, 2007.

- M. Bürgin and J. Draisma.
  The Hilbert null-cone on tuples of matrices and bilinear forms.
  Mathematische Zeitschrift, 254(4):785–809, 2006.

- Harm Derksen.
  Polynomial bounds for rings of invariants.
  Proceedings of the American Mathematical Society, 129(4):955–964, 2001.

# References II

Willem A. de Graaf, Gábor Ivanyos, and Lajos Rónyai.
Computing Cartan subalgebras of Lie algebras.
Applicable Algebra in Engineering, Communication and Computing, 7(5):339–349, 1996.

Harm Derksen and Visu Makam.
Polynomial degree bounds for matrix semi-invariants.
preprint, 2015.

M. Domokos and A. N. Zubkov.
Semi-invariants of quivers as determinants.
Transformation groups, 6(1):9–24, 2001.

Jack Edmonds.
Systems of distinct representatives and linear algebra.
J. Res. Nat. Bur. Standards Sect. B, 71:241–245, 1967.

# References III


M. Fortin and C. Reutenauer.
Commutative/noncommutative rank of linear matrices and subspaces of matrices of low rank.
Séminaire Lotharingien de Combinatoire, 52:B52f, 2004.

Ankit Garg, Leonid Gurvits, Rafael Oliveira, and Avi Wigderson.
A deterministic polynomial time algorithm for non-commutative rational identity testing.
preprint ArXiv:1511.03730, 2015.

# References IV


- Gábor Ivanyos, Marek Karpinski, Youming Qiao, and Miklos Santha.
  Generalized Wong sequences and their applications to Edmonds' problems.
  In STACS, pages 397–408, 2014.

- Gábor Ivanyos, Youming Qiao, and K. V. Subrahmanyam.
  Non-commutative Edmonds' problem and matrix semi-invariants.
  preprint arXiv:1508.00690, 2015.

- Gábor Ivanyos, Youming Qiao, and K. V. Subrahmanyam.
  On generating the ring of matrix semi-invariants.
  preprint, 2015.

# References V

Aidan Schofield.
Semi-invariants of quivers.
Journal of the London Mathematical Society, 2(3):385–395, 1991.