Algebraic algorithm for non-commutative rank.

Gábor Ivanyos, Youming Qiao,K V Subrahmanyam

Optimization, Complexity and Invariant Theory Workshop
IAS, June 4-8, 2018.

Outline

- Motivation
  - Invariant theory motivation
  - Algorithmic and complexity theoretic motivations
- Some avatars of non-commutative rank
- Augmenting sequences
- Augmenting in blow-ups and skewfields
- Constructivization, Regularity lemma, Polynomiality
  - Division algebras

Left right action

$\mathcal{X} = \{(X_1, X_2, \ldots, X_m)\}$

X_k, an $n \times n$ matrix with entries from field $\mathbb{F}$.

$\mathrm{SL}_n \times \mathrm{SL}_n \curvearrowright \mathcal{X}$,

$(A, B) \cdot (X_1, X_2, \ldots, X_m) = (AX_1B^t, AX_2B^t, \ldots, AX_mB^t)$

Classical invariant theory questions

- What are the polynomial functions invariant under the action? - well understood in characteristic zero fields, [Sch91, DW00, DZ01, ANS07], infinite fields [DW00, DZ01]
- The ring of invariants is known to be finitely generated - bound on the degree in which this is generated?, in characteristic zero fields, $exp(n^2)$, [Der01]

Membership in the nullcone

Nullcone for the left right action

Is defined as the set of all m-tuples $(A_1, A_2, \ldots, A_m)$ on which all invariant polynomial functions vanish i.e $f(A_1, A_2, \ldots, A_m) = 0$ for all invariant homogenous polynomial functions f (non-constant).

- An alternate characterization - $(A_1, A_2, \ldots, A_m)$ such that the A_i simultaneously shrink a subspace [Gur04, BD06, DZ01, ANS07].
- A description of the invariants:
  Let $T_1, T_2, \ldots, T_m$ be matrices in $\mathrm{M}at(d, \mathbb{F})$. Then $det(T_1 \otimes X_1 + T_2 \otimes X_2 + \ldots + T_m \otimes X_m)$ is an invariant of degree nd. All invariants are obtained this way.

Questions motivated from invariant theory

- Given a tuple $(A_1, \ldots, A_m)$ is it in the nullcone?

  Obvious algorithm, get a set of generators for the ring of invariants and check if all of them evaluate to zero.
- An exponential time algorithm ($exp(n^2)$) follows from Derksen[Der01]
- Given two tuples $(A_1, \ldots, A_m)$, $(B_1, \ldots, B_m)$ do their orbit closures intersect in the space of semi-stable points.

  This is an important question from the viewpoint of constructing the GIT quotient aka moduli space.

Nontrivial (lower) block triangularizations

- Minimal: 2 diagonal blocks and one below
- The **upper right** $k \times n - k$ **block** of an $n \times n$ matrix.

  zero block "touching" the diagonal
- Example:

$$\begin{pmatrix} 11 & 12 & 0 & 0 \\ 21 & 22 & 0 & 0 \\ 31 & 32 & 33 & 34 \\ 41 & 42 & 43 & 44 \end{pmatrix}, \text{ alt. notation: } \begin{pmatrix} 11 & 12 & & \\ 21 & 22 & & \\ 31 & 32 & 33 & 34 \\ 41 & 42 & 43 & 44 \end{pmatrix}$$

- Further examples:

$$\begin{pmatrix} 11 & & & \\ 21 & 22 & 23 & 24 \\ 31 & 32 & 33 & 34 \\ 41 & 42 & 43 & 44 \end{pmatrix}, \quad \begin{pmatrix} 11 & 12 & 13 & \\ 21 & 22 & 23 & \\ 22 & 32 & 33 & \\ 23 & 42 & 43 & 44 \end{pmatrix}$$

Interpretations: "reducibility"

- Adjacency matrix of a directed graph: having more that one strong (strongly connected) components E.g., Markov chains
- Bipartite graphs, a subset of size $n-k$ having at most $n-k$ neighbours
- Finite dim. modules

  Module given as the m-tuple of A_js

  Block triangularization: the last $n-k$ basis vectors span a submodule

Hall-like obstacle: zero diagonal block

- Having block triangular form with zero diag. block:

$$A = \begin{pmatrix} * & * & & & \\ * & * & & & \\ * & * & 0 & 0 & \\ * & * & 0 & 0 & \\ * & * & * & * & * \end{pmatrix} \text{ alias } \begin{pmatrix} * & * & & & \\ * & * & & & \\ * & * & & & \\ * & * & & & \\ * & * & * & * & * \end{pmatrix}$$

  A has an upper right $k \times \ell$ zero block
  this block has $k + \ell - n$ diagonal entries
- A maps subspace U to subspace U'
  $\dim U - \dim U' \geq (k + \ell - n)$
  $U = \langle$last ℓ basis vectors$\rangle$, $U' = \langle$last $n - k$ basis vectors$\rangle$,
- $\mathrm{rk} A \leq n - (k + \ell - n)$

Max size zero diagonal block

Definition

We say a matrix famiy $< A_1, \ldots, A_m >$, $A_i \in Mat(n, \mathbb{F})$ c-compresses $U \in \mathbb{F}^n$ if there is a $U' \in \mathbb{F}^n$ such that $A_i U \leq U'$ with $c = \dim(U) - \dim(U')$.

- $A(X) = x_1 A_1 + \ldots x_m A_m$ as matrix over $\mathbb{F}[X] \subset \mathbb{F}(X)$.

$$\mathrm{rk} A(X) \leq n - \max \{ c : \exists a\ c\ compressed\ U\ subspace \}$$

- For large $\mathbb{F}$, $\mathrm{rk} A(X) = \max \mathrm{rk} A(\alpha_1, \ldots, \alpha_m) = \max\{\mathrm{rk} B : B \in \langle A_1, \ldots A_m \rangle\}$
- Shorthand notation

$$\mathrm{ncrk} A(X) := n - \max \left\{ \dim U - \dim U' : A_i U \leq U' \right\}$$

- $\mathrm{ncrk} A(X) < n$ if there is a compressed subspace.

Outline

- Motivation
  - Invariant theory motivation
  - Algorithmic and complexity theoretic motivations
- Some avatars of non-commutative rank
- Augmenting sequences
- Augmenting in blow-ups and skewfields
- Constructivization, Regularity lemma, Polynomiality
  - Division algebras

Term for "ncrk"?

- non-deterministically complemented rank?
- nullcone-based rank?

Recall $(A_1, A_2, \ldots, A_m)$ in the nullcone of invariants iff the A_i simultaneously shrink a subspace.

$\text{ncrk}A(X) < n$ iff $(A_1, \ldots, A_m) \in$ nullcone of invariants of $SL_n \times SL_n$.

Non-commutative rank

Another term for ncrk.

Rank of $A(X)$ in non-commutative variables

- could interpret as a "linear combination" of $A_1, \ldots, A_m$ with "non-commuting coefficients"
- Here $A(X) \in \mathbb{F}\langle X \rangle \subset$ some "enormous" skewfield[Coh85]
  $X = x_1, \ldots, x_m$
- A similar (weaker) statement (we will see this):
  $$\mathrm{ncrk} A(X) = \mathrm{rk} A(\phi(X))$$
  for some homomorphism ϕ from $\mathbb{F}\langle X \rangle$ to *some* skewfield [Coh85]
- We will use *non-injective* homomorphisms into certain "tractable" skewfields

Equality in rk $\leq$ ncrk ?

- Counterexample: skew symmetric matrices of odd degree:
  The rank of a skew-symmetric matrix is always *even*.
  The space of skew symmetric three by three matrices does not compress any subspace.
- Equality in certain special cases
  - pairs of matrices $\sim$ matrix pencils
    $$\mathrm{rk} A_1 x_1 + A_2 x_2 = \mathrm{ncrk} A_1 x_1 + A_2 x_2$$
    Probably classical, Atkinson and Stephens (1978)
  - rank one matrices: if $\mathrm{rk} A_j = 1$ then
    $$\mathrm{rk} \sum A_j x_j = \mathrm{ncrk} \sum A_j x_j$$
  - $\exists$ many other examples and counterexamples
  - Called compression spaces by Fortin and Reutenauer. [FR04]

Overview of Algorithm for NCRank

- Start with a matrix of in the span of $< A_1, \ldots, A_m >$.
- Use a matching like algorithm to augment rank, obtaining a matrix of larger rank.
- The analogue of augmenting sequences in this setting – the second Wong sequences.
- Need a stopping rule as in, no odd length alternating paths -a witnessing shrunk subspace.

Outline

Testing $\mathrm{rk}A(X) = \mathrm{ncrk}A(X)$

- proposed by Fortin, Reutenauer [FR04]
  a critical part rediscovered by Ivanyos, Qiao, Karpinski, Santha, [IKQS15]
- Reduce to testing $\mathrm{rk}A_1 = \mathrm{ncrk}A(X)$:
  replace A_1 with $A(\underline{\alpha})$ for random $\underline{\alpha}$
- Assume $\mathrm{rk}A_1 = \mathrm{ncrk}A(X)$. Then try to find U, U' s.t.:
  - $U \geq \ker A_1$
  - $A_j U \leq U'$ $(j = 1, \ldots, k)$
  - $\dim U - \dim U' = n - \mathrm{rk}A_1$ $\quad (\mathrm{rk}A_1 = n - (\dim U - \dim U'))$
- $U \geq \ker A_1$ and **two equations**:
  - $\sum A_j U = U'$
    $\leq$: ✓; $\quad \geq$: $\sum_j A_j U \geq A_1 U = U'$
  - $U = A_1^{-1}(U')$
    $\leq$: ✓; $\quad \geq$: $\dim A_1^{-1} U' = \dim U' + \dim \ker A_1$

The second Wong sequence

- $U \geq \ker A_1$ and two equations:

$$U' = \sum A_j U \text{ and } U = A_1^{-1}(U')$$

- Resolve by recursion (find smallest possible U'):
  - $U'_0 = (0),\ U_1 = A_1^{-1}(0) = \ker A_1$
  - $U'_i = \sum_j A_j U_i,\ U_{i+1} = A_1^{-1}(U'_i)$
  - monotone non-decreasing sequences, $U'_i \subseteq U'_{i+1}$.
  - stabilize at repetition

    can stop if $U'_{i+1} = U'_i$ (then $U_n = U_i,\ U'_n = U'_i$)
  - if $U'_n \leq \mathrm{im} A_1$ then $U = U_n, U' = U'_n$ are good
  - otherwise $\nexists$ good U, U'

    can also stop if $U'_{i+1} \not\leq \mathrm{im} A_1$
  - analogue of DFS-ing "alternating forests" in bipartite graphs

Augmenting sequence

- If $U_n \leq \mathrm{im} A_1$ then done.
- otherwise find $i_1, \ldots i_\ell$, (smallest ℓ) such that

  $A_{i_\ell} A_1^{-1} \ldots A_{i_2} A_1^{-1} A_{i_1} \ker A_1 \not\leq \mathrm{im} A_1$
- simplification: multiply A_i by matrices such that

  A_1 block diagonal with diag block I_r and 0_{n-r}:

$$A_1 = \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \\ \end{pmatrix} \text{ alias } \begin{pmatrix} I & \\ & \end{pmatrix}$$

(already useful in computing the Wong sequence)

Augmenting sequence

- Further simplification: we can assume $A_1 = \begin{pmatrix} I_{n-1} & \\ & \end{pmatrix}$

  Find $v \in \ker A_1$ s.t. $w = A_{i_\ell} A_1^{-1} \ldots A_{i_2} A_1^{-1} A_{i_1} v \not\leq \mathrm{im} A_1$
  first n column indices: $\mathrm{im} A_1 + \langle v \rangle$
  first n row indices: $\mathrm{im} A_1 + \langle w \rangle$
- Then $\{i_1, \ldots, i_\ell\} \subseteq \{2, \ldots, m\}$ and A_1^{-1} can be omitted.
- $A_{i_\ell} \ldots A_{i_2} A_{i_1}$ is a shortest product with nonzero lower right diagonal block: $\begin{pmatrix} * & * \\ * & b \end{pmatrix}, \quad b \neq 0$
- Easiest case $\ell = 1$: $\det(XA_1 + A_{i_1}) =$

  $$\det\left(\begin{pmatrix} xI & \\ & \end{pmatrix} + \begin{pmatrix} * & * \\ * & b \end{pmatrix}\right) = bx^{n-1} + \text{lower degree terms}$$

  try $\lambda A_1 + A_j$ for n different λs and for $j = 2, \ldots, m$.
  works for some interesting instances.

Augmenting sequences for matrix pencils

- A_1, A_2, find λ s.t. $\mathrm{rk}(A_1 + \lambda A_2) > \mathrm{rk} A_1$.
- Basis case: $A_1 = \begin{pmatrix} I_{n-1} & \\ & 0 \end{pmatrix}$
- Augmenting sequence: $A_2^\ell = \begin{pmatrix} * & * \\ * & b \end{pmatrix}$, $b \neq 0$, ℓ smallest possible. Suppose $\ell > 1$.
- $\ker A_1 = \langle u_1 \rangle$.
- $u_i = A_2^{i-1} u_1$ $(i = 2, \ldots \ell)$
- $u_2, \ldots, u_\ell \in \mathrm{im} A_1$
- extend to a basis $u_2, \ldots, u_{\ell-1}, u_\ell, u_{\ell+1}, \ldots, u_n$ of $\mathrm{im} A_1$.
- in basis $u_2, \ldots, u_n, u_1$ (this order!)

$$xA_1 + A_2 = \begin{pmatrix} x & & & & & * & \cdots & * & 1 \\ 1 & x & & & & * & \cdots & * & \\ & 1 & x & & & * & \cdots & * & \\ & & \ddots & \ddots & & \vdots & \ddots & \vdots & \\ & & & 1 & x & * & * & & \\ & & & & & y & \cdots & * & \\ & & & & & * & \ddots & * & \\ & & & & & * & \cdots & z & \\ & & & & 1 & * & \cdots & * & \end{pmatrix}$$

$y = x + c, \ldots, z = x + d$
Move last column to the first, last row to the ℓth

$$
xA_1 + A_2 = \begin{pmatrix}
1 & x & & & & & * & \cdots & * \\
 & 1 & x & & & & * & \cdots & * \\
 & & 1 & x & & & * & \cdots & * \\
 & & & \ddots & \ddots & & \vdots & \ddots & \vdots \\
 & & & & 1 & x & * & * & \\
 & & & & & 1 & * & \cdots & * \\
 & & & & & & y & \cdots & * \\
 & & & & & & * & \ddots & * \\
 & & & & & & * & \cdots & z
\end{pmatrix}
$$

Block upper triangular with upper triangular upper left block
$\det(xA_1 + A_2) = x^{n-\ell} +$ lower degree terms
Try $n - \ell + 1$ different substitutions for x

Attempt to reduce to pairs

- Our tool: $A_1 = \begin{pmatrix} I_r & \\ & \end{pmatrix}$ is max rank in $\langle A_1, B\rangle$ if and only if lower right $n-r \times n-r$ block of $B, B^2, \ldots, B^{r+1} = 0$.
- basic case $r = n-1$ can be supposed
- Assume: lower right entry of $A_{i\ell} \ldots A_{i1}$: $b \neq 0$, (ℓ smallest).
- Put $B = x_1 A_{i_1} + \ldots + x_\ell A_{i\ell}$
- Lower right entry of B^ℓ: $bx_1 \ldots x_\ell +$other degree ℓ summands.
  homogeneous poly of degree ℓ
  or zero: "interference"
- $\approx$ a hard instance of PIT
  - $\approx$: the assumption "ℓ smallest" may help , without that would "solve" the PIT.
    Indeed helps for rank one A_js

A counterexample for triples

- Skew symmetric matrices have even rank

$$A_1 = \begin{pmatrix} & 1 & \\ -1 & & \\ & & \end{pmatrix}, A_2 = \begin{pmatrix} & & \\ & & 1 \\ & -1 & \end{pmatrix}, A_3 = \begin{pmatrix} & & 1 \\ & & \\ -1 & & \end{pmatrix}$$

$$\Big\downarrow \quad \text{multiply from the left by by} \quad \begin{pmatrix} & -1 & \\ 1 & & \\ & & 1 \end{pmatrix}$$

$$A_1 = \begin{pmatrix} 1 & & \\ & 1 & \\ & & \end{pmatrix}, A_2 = \begin{pmatrix} & & -1 \\ & & \\ & -1 & \end{pmatrix}, A_3 = \begin{pmatrix} & & \\ & & 1 \\ -1 & & \end{pmatrix}$$

A counterexample for triples (2)

- $A_2^2 = \begin{pmatrix} & 1 & \\ & & \\ & & \end{pmatrix}, A_3^2 = \begin{pmatrix} & & \\ -1 & & \\ & & \end{pmatrix},$

  $A_2A_3 = \begin{pmatrix} 1 & & \\ & & \\ & & -1 \end{pmatrix}, A_3A_2 = \begin{pmatrix} & & \\ & -1 & \\ & & 1 \end{pmatrix}$
- Lower right entry of $(xA_2 + yA_3)^2$ is $xy - yx = 0$.
- $(xA_2 + yA_3)^2 = \begin{pmatrix} xy & x^2 & \\ -y^2 & -yx & \\ & & \end{pmatrix}$
- $(xA_2 + yA_3)^t$: zero last row and last column for $t > 1$

NCRK of skew-symmetric matrices?

- Skew-symmetric matrices do not shrink a subspace.
- So the rank of $< A_1, A_2, A_3 >$ over the free-skew field is 3.
- For some d there exist $M_1, M_2, M_3 \in M_d(\mathbb{F})$ with $A_1 \otimes M_1 + A_2 \otimes M_2 + A_3 \otimes M_3$ having rank $3d$.
- Can we work with non-commuting variables and increase rank using augmenting paths?
- Can we go to a larger tensor space and increase rank using augmenting paths?
- Reduction to matrix pencils?

Outline

- Motivation
  - Invariant theory motivation
  - Algorithmic and complexity theoretic motivations
- Some avatars of non-commutative rank
- Augmenting sequences
- Augmenting in blow-ups and skewfields
- Constructivization, Regularity lemma, Polynomiality
  - Division algebras

Over the quaternions

- $\mathbb{H} = \mathbb{R}\langle x, y, z\rangle/(x^2+1, y^2+1, xy-z, yx+z)$
- Lower right entry of $(xA_2 + yA_3)^2$ is $xy - yx = 2z$.
- $(xA_2 + yA_3)^2 = \begin{pmatrix} z & -1 & \\ 1 & z & \\ & & 2z \end{pmatrix}$
- $A_1 + xA_2 + yA_3 = \begin{pmatrix} 1 & & -x \\ & 1 & y \\ -y & -x & \end{pmatrix}$
- Gaussian elimination: left multiply by $\begin{pmatrix} 1 & & \\ & 1 & \\ y & x & 1 \end{pmatrix}$, get

$\begin{pmatrix} 1 & & -x \\ & 1 & y \\ & & 2z \end{pmatrix}$: full rank over $\mathbb{H}$

As block matrices over $\mathbb{C}$

- Matrix representation of $\mathbb{H}$ (over $\mathbb{C}$): $1 \mapsto I = \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$
  $x \mapsto X = \begin{pmatrix} i & \\ & -i \end{pmatrix}$ $y \mapsto Y = \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$ $z \mapsto Z = \begin{pmatrix} & i \\ -i & \end{pmatrix}$
- extend to representation of $M_3(\mathbb{H})$ in $M_6(\mathbb{C})$:
  $A_1 \mapsto \begin{pmatrix} I & & \\ & I & \\ & & \end{pmatrix}$, $(xA_2 + yA_3)^2 \mapsto \begin{pmatrix} Z & -I & \\ I & Z & \\ & & 2Z \end{pmatrix}$,
  $(A_1 + xA_2 + yA_3) \mapsto \begin{pmatrix} I & & -X \\ & I & Y \\ -Y & -X & \end{pmatrix}$, after elimination:
  $\begin{pmatrix} I & & -X \\ & I & Y \\ & & 2Z \end{pmatrix}$

Augmenting in blow-ups

Given $\mathcal{A} = \langle A_1, \ldots, A_m \rangle$ the d-th blow up of $\mathcal{A}^d \triangleq \mathcal{A} \otimes Mat(d, \mathbb{F})$.

- Recall $v_1 \in ker(A_1)$, $rk(A_1) = r$.
  $A_{i_\ell} \cdots A_{i_1}(v_1) \notin Im(A_1)$
- $B = x_1 A_{i_1} + \cdots + x_{i_\ell} A_{i_\ell}$
  B^ℓ has a term $x_{i_\ell} \ldots x_{i_1} A_{i_\ell} \cdots A_{i_1}$.
- Let $d = \ell + 1$ (can improve this to $d = (\ell + 1)/2$)
- Let u_i be a basis of $\mathbb{F}^d$. Let E_{ij} be the elementary $d \times d$ matrix with the non-zero entry 1 at position (i, j) and zero elsewhere.
- Set $A' = A_1 \otimes Id_d$
  $B = A_{i_1} \otimes E_{21} + A_{i_2} \otimes E_{32} + A_{i_3} \otimes E_{43} + \ldots A_{i_\ell} \otimes E_{\ell+1\ell}$.

Augmenting in blow-ups(2)

- $(v_1 \otimes u_1) \in ker(A')$
- $B^\ell(v_1 \otimes u_1)$ contains a term
  $A_{i_\ell} \otimes E_{\ell+1\ell} \cdot A_{i_\ell-1} \otimes E_{\ell\ell-1} \cdots\cdots A_{i_1} \otimes E_{21}$,
  $= A_{i_\ell} A_{i_\ell-1} \ldots A_{i_1}(v_1) \otimes u_d \neq 0$,
  and terms linearly independent of this.
- For the second Wong sequence starting with the pencil $\langle A', B\rangle$, the limiting sequence is not in $Im(A')$.
- There exists λ in a set of size $rd+1$, with $\lambda A' + B$ having rank more than $rd+1$.
- $A', B, \lambda A' + B \in \mathcal{A}^d$.

Matrix skewfields

- D: sub-skewfield of $Mat(d, \mathbb{L})$ ($\mathbb{L}$ extension of $\mathbb{F}$)
  D spans $Mat(d, \mathbb{L})$ over $\mathbb{L}$, Then
  $\mathbb{K} = \{x \in D : xy = yx \text{ for every } y \in D\} = D \cap \mathbb{L}$
  ($\mathbb{L} \subset Mat(d, \mathbb{L})$ as scalar matrices)
  $\dim_{\mathbb{K}} D = d^2$
  D and $Mat(d, \mathbb{L})$ satisfy the same polynomial identities in $\mathbb{K}\langle x_1, \ldots, x_k\rangle$
- d: large enough to avoid (homogeneous) polynomial identities of degree ℓ
- $Mat(d, \mathbb{L})$ has a degree $2d$ polynomial identity

  called the standard identity

  Fact: $Mat(d, \mathbb{L})$ satisfies no PI of degree $< 2d$:

Augmenting using Skewfields

- We have $\widetilde{A_\lambda} = \lambda A_1 \otimes I + \sum A_{i_j} \otimes E_{j+1,j}$ of rank $> rd + 1$
- Find $\widetilde{B} = \lambda A_1 \otimes I + \sum A_{i_j} \otimes \delta_j$ with $\delta_j \in D$ of rank $> rd + 1$ (as a matrix over $\mathbb{L}$)
  - Express $E_{j+1,j}$s in terms of a basis for D with coefficients from $\mathbb{L}$
  - use a coordinate reduction tool (deGraaf, Ivanyos, Rónyai)
  - to replace these by coefficients from $\mathbb{K}$ (or even from $\mathbb{F}$)
- $\widetilde{B}$ must have rank divisible by d (The regularity lemma.)

  Proof: Gaussian elimination over D
- Find $\widetilde{C} = \lambda A_1 + \otimes I + \sum A_{i_j} \otimes \mu_j$ with $\mu_j \in Mat(d, \mathbb{F})$ ($\mathbb{F}$ large enough)
  - Express δ_j in terms of E_{uv} with
  - coefficients from $\mathbb{L}$
  - coordinate reduction from $\mathbb{L}$ to $\mathbb{F}$ (if $\mathbb{F}$ is large enough)

Outline

- Motivation
  - Invariant theory motivation
  - Algorithmic and complexity theoretic motivations
- Some avatars of non-commutative rank
- Augmenting sequences
- Augmenting in blow-ups and skewfields
- Constructivization, Regularity lemma, Polynomiality
  - Division algebras

A coordinate reduction tool

- simple but useful
- $f = f(y_1, \ldots, y_N) \in \mathbb{L}[y_1, \ldots, y_N]$
- $\Omega \subseteq L$, $|\Omega| \geq \max_i \deg_{y_i} f + 1$
- Given $\underline{\alpha} \in \mathbb{L}^N$ s.t. $f(\underline{\alpha}) \neq 0$;
- Find $\underline{\beta} \in \Omega^N$ s.t. $f(\underline{\beta}) \neq 0$;
    - $f(y_1, \alpha_2, \ldots, \alpha_N) \in F[y_1]$ nonzero of degree at most $\deg_{y_1} f$. Find $\beta_1 \in \Omega$ by exhaustive search s.t. $f(\beta_1, \alpha_2, \ldots, \alpha_N) \neq 0$.
    - and so on to find $\beta_2, \ldots$
- Variant: $B(\underline{y}) = y_1 B_1 + \ldots, y_N B_N$ lin. matrix. Given $\underline{\alpha} \in \mathbb{L}^N$ s.t. $\mathrm{rk} B(\underline{\alpha}) \geq r$; find $\underline{\beta} \in \Omega^N$ s.t. $\mathrm{rk} B(\underline{\beta}) \geq r$;
- Allows us to go from $\mathcal{A} \otimes Mat(d, \mathbb{F})$ to $\mathcal{A} \otimes D$ and back.

Regularity of blowups

Theorem

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

- Follows from Gaussian eliminations in D; another proof in the Appendix
- Requirements:
  - D spanning $Mat(d, \mathbb{L})$ given by a basis over some subfield of $\mathbb{L}$.

    A non-tractable D: $UT(d)$ (Amitsur, used by Derksen and Makam)
  - Can "quickly" compute ranks of matrices in $Mat(dn, \mathbb{L})$.

Tractable matrix skewfields

- D: $\mathbb{F}$-subalgebra spanning $\mathrm{M}at(d, \mathbb{L})$, $D \otimes_{\mathbb{K}} \mathbb{L} \cong \mathrm{M}at(d, \mathbb{L})$.
  given by a basis over $K = D \cap \mathbb{L}$
- need to compute rank of matrices in $\mathrm{M}at(dn, \mathbb{L})$ in poly time
- d should be $n^{O(1)}$
- $\mathbb{L}$ algebraic of degree $n^{O(1)}$ over $\mathbb{F}(t_1, \ldots, t_s)$,
- We use transcendence degree 2
- Construction: cyclic division algebras. Appendix

The (almost) final algorithm

1. Input: $\mathcal{A} = \{A_1, \ldots, A_m\}$. Set $d = 1$. Find a matrix of rank say, r.
2. Start with a matrix in $A \in \mathcal{A}^d$ of rank rd.
3. Compute the second Wong sequence with this A, get $\ell \leq rd + 1$ and matrices $A_{i_\ell}, \ldots, A_{i_1}$ with $A_\ell \ldots A_{i_1}(ker(A)) \not\leq im(A)$.
4. For $d' = \ell + 1$ find a matrix in $\mathcal{A}^{dd'}$ with rank $rdd' + 1$.
5. For large $\mathbb{F}$ using constructive division algebras of degree d'^2 and coordinate reduction tools find a matrix in $\mathcal{A}^{dd'}$ with rank $(r+1)dd'$. Set $r = r + 1$, $d = dd'$, compute a basis of $\mathcal{A}^d$, go back to step 2.

Developments since 2015

- Garg, Gurvits, Oliveira, Wigderson [GGOW16], gave a polynomial time algorithm for non-commutative rank in characteristic zero. No witnessing shrunk subspace.
- Derksen, Makam [DM17], showed that blow-up need only be by $n-1$. Nullcone is cut by polynomials of degree $poly(m,n)$, and $poly(n)$ in characteristic 0.
- IQS[IQS18], showed polynomiality over all reasonably sized fields and construct a shrunk subspace.
- Recently, Allen-Zhu, Garg, Li, Oliveira, Wigderson [AZGL$^+$18], solved the orbit closure problem over $\mathbb{C}$.
- Soon, Derksen and Makam [DM18], solved the orbit closure problem over all large enough fields using results from [IQS18]. Recently [DM18b] showed that the null cone is cut by polynomials of degree $poly(n)$.

Blowing down

Reducing the size of blow-ups

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

- Tighter theorem proved first by Derksen, Makam (for $d > n - 1$).
- Gives a polynomial bound on the degree in which the ring of invariants is generated.
- A convexity argument uses even rectangular blow-ups.

Blowing down(2)

- Take an appropriate $(d-1)n \times (d-1)n$ submatrix A'' of A in $\mathcal{A}^{d-1}$.
- Rank of A" is more than $(d-1)(n-1)$.
- We have added at most n rows and n columns to get to A from A", so rank A is otherwise at most $nd - d - n + 1 + 2n = nd + (n+1) - d$, a contradiction!.
- Use regularity to get A' of rank $(d-1)n$.
- $\Longrightarrow$ Never need to consider blow-ups of size more than $n+1$.

Cyclic algebras and the construction of Dickson

- Let $\mathbb{L}/\mathbb{K}$ be a Galois extension with cyclic Galois. Let σ be a generator of the Galois group and $d = dim_{\mathbb{K}}(\mathbb{L})$.
- Take $f \in \mathbb{K}$ and a symbol x, and consider $D = \mathbb{L} \oplus \mathbb{L} \cdot x \oplus \mathbb{L} \cdot x^2 + \ldots \mathbb{L} \cdot x^{d-1}$.
- Multiply elements in D using the distributive law and using $x^d = f$ and $x \cdot b = \sigma(b)x$ for all $b \in L$.
- $\mathbb{K}$ is the center of D and D is an $\mathbb{K}$-algebra. Dimension over $\mathbb{K}$ is d^2.
- Wedderburn - if f is choosen carefully, then D is a division algebra, and in this case $D \otimes_{\mathbb{K}} \mathbb{L} \cong Mat(d, \mathbb{L})$.

Construction of division algebras of degree d

- p be the characteristic of $\mathbb{F}$. And ler $d = d_1 p^s$.
- Will construct the division algebra by constructing a cyclic Galos extension of degree d, as a product of two extensions of degree d_1 and degree p^s.
- Assume the characteristic of $\mathbb{F}$ does not divide d_1. Start with $\mathbb{F}'$ containing a d_1-th root of unity ζ.
- Take $\mathbb{K} = \mathbb{F}'(X)$ for an indeterminate X.
- Extend $\mathbb{K}$ by appending Y with $Y^d = X$, to get $\mathbb{L}_1$, a Galois extension of $\mathbb{K}$. $Y^i Y^j = Y^{i+j}$ if $i + j \leq d$, otherwise $Y^i Y^j = XY^{i+j-d}$. Can construct a generator for the Galois group sending Y^j to $\zeta^j Y^j$.
- Construct a cyclic extension L_2 of $\mathbb{F}_p(X)$ of degree p^s and a generator (Artin-Schrier extension).

Construction of division algebras of degree d (2)

- $\mathbb{L} = L_1 \otimes_{\mathbb{F}_p(X)} L_2$ is a cyclic Galois extension of degree d of $\mathbb{K} \otimes_{\mathbb{F}_p(X)} F_p(X)$. Can compute a generator of the Galois group.
- For Z^d transcendental over L, $\mathbb{L}(Z^d)$ is a Galois extension of $[\mathbb{K} \otimes_{\mathbb{F}_p(X)} F_p(X)](Z^d)$.
- $L \oplus L \cdot Z \oplus L \cdot Z^2 \oplus \ldots L \cdot Z^{d-1}$ is a division algebra over $K(Z^d)$ and can realized in $\mathrm{M}at(d, \mathbb{F}'(X, Z))$.
- Can construct a basis for the division algebra, a generator for the Galois group. All this in polynomial time.

Proof of regularity lemma

- $D \otimes_{\mathbb{K}} \mathbb{L} \cong Mat(d, \mathbb{L})$. Explicit matrices describing the $\mathbb{K}$-algebra $D \cong D \otimes 1$ can be written down easily.
- $D \otimes_{\mathbb{K}} D^{op} \cong Mat(d^2, \mathbb{K})$, with D embedded as $D \otimes_{\mathbb{K}} Id$ and D^{op} as $Id \otimes_{\mathbb{K}} D^{op}$ - Inside $Mat(d^2, \mathbb{K})$, the images commute.
- Regard $\mathbb{K}^n \otimes_{\mathbb{K}} L^d (\cong \mathbb{K}^{d^2 n})$ as a module over $Mat(n, \mathbb{K}) \otimes_{\mathbb{F}} D$. $(A \otimes d) \cdot [v \otimes \ell] = Av \otimes d \cdot \ell$
- The action of $id \otimes D^{op}$ on $\mathbb{K}^n \otimes_{\mathbb{K}} L^d$ commutes with the action of $Mat(n, \mathbb{F}) \otimes_{\mathbb{F}} D$.
- For all A in $Mat(n, \mathbb{F}) \otimes_{\mathbb{F}} D$, $A\mathbb{K}^{d^2 n}$ is a D^{op}-submodule, and so its dimension over $\mathbb{K}$ is divisible by d^2, so dimension over $\mathbb{L}$ is divisible by d. But this is the rank of A.

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.

Zeyuan Allen-Zhu, Ankit Garg, Yuanzhi Li, Rafael Oliveira, and Avi Wigderson.
Operator scaling via geodesically convex optimization, invariant theory and polynomial identity testing.
arXiv preprint arXiv:1804.01076, 2018.

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

References II

P. M. Cohn.
Free Rings and Their Relations.
L.M.S. Monographs. Acad. Press, 1985.
First edition 1971.

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

Harm Derksen and Visu Makam.
Polynomial degree bounds for matrix semi-invariants.
Advances in Mathematics, 310:44–63, 2017.

References III

Harm Derksen and Visu Makam.
Algorithms for orbit closure separation for invariants and semi-invariants of matrices.
arXiv preprint arXiv:1801.02043, 2018.

Harm Derksen and Jerzy Weyman.
Semi-invariants of quivers and saturation for littlewood-richardson coefficients.
Journal of the American Mathematical Society, 13(3):467–479, 2000.

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

References IV

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.
In *Foundations of Computer Science (FOCS), 2016 IEEE 57th Annual Symposium on*, pages 109–117. IEEE, 2016.

References V

Leonid Gurvits.
Classical complexity and quantum entanglement.
J. Comput. Syst. Sci., 69(3):448–484, 2004.

Gábor Ivanyos, Marek Karpinski, Youming Qiao, and Miklos Santha.
Generalized wong sequences and their applications to edmonds' problems.
J. Comput. Syst. Sci., 81(7):1373–1386, 2015.

References VI

Gábor Ivanyos, Youming Qiao, and KV Subrahmanyam.
Constructive noncommutative rank computation in deterministic polynomial time over fields of arbitrary characteristics.
computational complexity, 2018.

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