Computing the non-commutative rank of a matrix space

Gábor Ivanyos
HUN-REN SZTAKI

Summer School on Algorithms

23-27 June 2025, ELTE, Budapest.

Based (mostly) on joint works with Youming Qiao and K. V. Subrahmanyam

At a crossroad of

Skewfields

Invariant theory

Polynomial Invariants

$$\times$$

Combinatorial Optimization

Maximal matchings

Derandomization

Polynomial Identity Testing

$$+$$

Analysis (inequalities)

Cryptography

Commutative rank

- Matrix space $\mathcal{A} \leq M_n(F)$ F field (commutative)
- $\operatorname{rk} \mathcal{A}$: max rank from $\mathcal{A}$
- computing $\operatorname{rk} \mathcal{A}$ (Edmonds' problem 1967)
- Alt. formulation: linear matrix $A_1, \ldots, A_k$ basis for $\mathcal{A}$
  $A(x) = A(x_1, \ldots, x_k) = A_1 x_1 + \ldots + A_k x_k$
  - Find a maximal square submatrix $B(x)$ of $A(x)$ s.t. $\det(B(x))$ has a nonzero subst. from F^k
    $\sim$ Polynomial Identity Testing
- Equivalent decision problem: rank fullness
  - $\in RP$ if F is large enough (DeMillo-Lipton-)Schwartz-Zippel lemma
  - NP-complete for small F Buss, Frandsen, Shallit 1999
  - over large F not known if $\in P$
  - $\in P$ would imply circuit lower bounds for NEXP
    Kabanets, Impagliazzo 2003
- $\operatorname{rk} A(x) = \operatorname{rk}(K \otimes \mathcal{A})$ for large enough ext. K of F,
  $A(x)$ as a matrix over $F(x) = F(x_1, \ldots, x_n)$

Non-nommutative rank

- extend the base field further
- noncommutative rank: $\operatorname{ncrk}\mathcal{A} =$
  $\max\{$max rank from $\mathcal{A} \otimes_F D$: D skewfield ext. of $F\}$
  $\mathcal{A} \otimes_F D =$ "D-span" of the matrices from $\mathcal{A}$
- Gaussian elim. and consequences to rank
  remain valid over skewfields
  - independent rows/columns, full rank submatrices
    Caveat: multiply by D from the appropriate direction!

- Remark (a common interpretation):
  consider $A(x_1, \ldots, x_k)$ over a *"free skewfield"*
  a skewfield $\geq F\langle x_1, \ldots, x_k\rangle$

Commutative vs. noncommutative rank

- $\operatorname{rk} \mathcal{A} \leq \operatorname{ncrk} \mathcal{A}$
- Example for $<$: $\mathcal{A} =$ skew-symmetric 3 by 3 real matrices
  - $\operatorname{rk} \mathcal{A} = 2$. Why?
  - $\operatorname{ncrk} \mathcal{A} = 3$: over the quaternions

$$\begin{pmatrix} & -1 & -i \\ 1 & & -j \\ i & j & \end{pmatrix}$$

$$\downarrow \qquad \text{left mult by } \begin{pmatrix} 1 & & \\ & 1 & \\ j & -i & 1 \end{pmatrix}$$

$$\begin{pmatrix} & -1 & -i \\ 1 & & -j \\ & & 2k \end{pmatrix}$$

Commutative vs. noncommutative rank 2

- which one is easier to compute?
  - ncrk is a proper relaxation of rk
  - but a more difficult concept

    uses difficult objects (free skewfields)

    or a (possibly) infinite family of skewfields

    (can be "easily" pulled down to expontetial size)

    even computability in randomized poly time is not obvious
- This talk: ncrk is "easier":

  computable even in **deterministic polynomial** time!

The noncommutive rank as a rank of a block matrix

- Fact: can assume D is finite dimensional over its center K, which is a fin. gen. (possibly transcendental) extension of F
  - $\dim_K D = d^2$
  - $D \otimes_K L \cong M_d(L)$ for some field $L \geq K$
  - $M_n(K) \otimes_K M_d(L) \cong M_{nd}(L)$
- elements of $\mathcal{A} \otimes M_d(L)$:

$$\begin{pmatrix} A_{11} & \dots & A_{1d} \\ \vdots & \ddots & \vdots \\ A_{d1} & \dots & A_{dd} \end{pmatrix} \quad \text{where } A_{ij} \in \mathcal{A} \otimes L$$

- rank over D gets blown up by a factor d in $M_{nd}(L)$
- suggests that max rank in $\mathcal{A} \otimes M_d(L)$ is a multiple of d

Comment: connection to invariant theory

- determinants of matrices in $\mathcal{A} \otimes M_d(L)$
  $\sim$ invariants of $SL_n \times SL_n$ (degree dn homogeneous part)

  e.g., Domokos, Zubkov 2001

  - $(X^1, \ldots, X^m)$ tuple of formal matrices:

$$X^k = \begin{pmatrix} x_{11}^k & \dots & x_{1n}^k \\ \vdots & \ddots & \vdots \\ x_{1n}^k & \dots & x_{nn}^k \end{pmatrix}$$

  - $SL_n \times SL_n$ acts on linear matrices by left-right mult.
  - homogeneous degree nd polynomial invariants w.r.t. this action:

$$\det(X_1 \otimes B_1 + \dots X_m \otimes B_m)$$

$$(B_1, \ldots, B_m \ d \text{ by } d \text{ matrices})$$

A coefficient controlling tool

- Lemma: Given $f \in L[x_1, \ldots, x_m]$, $S \subseteq L$, $|S| > \deg_i(f)$ $(i = 1, \ldots, m)$ and $a = (a_1, \ldots, a_m) \in L^m$ s.t. $f(a) \neq 0$. Can find in det poly time $b = (b_1, \ldots, b_m) \in S^m$ s.t. $f(b) \neq 0$.
  - Algorithm: replace a_i by $b_i \in S$ one by one: e.g., $f(x_1, a_2, \ldots, a_m) \in L[x_1]$, not id. zero of degree $< |S|$. Find $b_1 \in S$ s.t. $f(b_1, a_2, \ldots, a_m) \neq 0$ by trial and error.

- Application: Given $A_1, \ldots, A_m \in M_k(L)$ and $A \in \mathcal{B} = \mathrm{span}(A_1, \ldots, A_m)$ of rank $\geq R$, $S \subseteq L$ of size $> R$, can find $c_1, \ldots, c_m \in S$ s.t. $c_1A_1 + \ldots + c_mA_m$ has rank $\geq R$.
  - choose an $R \times R$ submatrix of A of full rank
  - apply the lemma to the determinant of the corresponding submatrices from $\mathcal{B}$ (with variable coeffs)

- Useful for keeping cefficients small
and for rank rounding in the "blowup" $\mathcal{A} \otimes M_d(F)$

Rounding up the rank in $\mathcal{A} \otimes M_d(F)$

- matrix of rank $R \longrightarrow$ a matrix of rank $\geq \lceil R/d \rceil d$ (if $|F| > rd$)
- *construct* fields K, L skewfield D s.t. $F \leq K \leq L$, $K = \mathrm{centre}(D)$, $\dim_K(D) = d^2$, and a d-dim repr. of D over L:
  $D \otimes L \cong M_d(L)$.
- Example: quaternions have a 2-dimensional repr. over $\mathbb{C}$:
  $$1 \mapsto \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}, i \mapsto \begin{pmatrix} i & \\ & -i \end{pmatrix}, j \mapsto \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}, k \mapsto \begin{pmatrix} & i \\ i & \end{pmatrix}$$

Rounding up the rank II

- matrix in $\mathcal{A} \otimes M_d(F) \subseteq \mathcal{A} \otimes M_d(L)$ of rank R

  choose a K-basis of $\mathcal{A} \otimes D$, it is an L-basis of $\mathcal{A} \otimes M_d(L)$, $S \subseteq K$

- coeff. tool gives a matrix of rank $\geq R$ in $\mathcal{A} \otimes D$
  - rank $r' \geq \lceil R/d \rceil$ as a matrix over D,
  - rank $r'd$ as a matrix in $M_{nd}(L)$

  choose an F-basis of $\mathcal{A} \otimes M_d(F)$ it is an L-basis of $\mathcal{A} \otimes M_d(L)$, $S \subseteq F$

- tool gives a matrix of rank $\geq r'd = \lceil R/d \rceil d$ in $\mathcal{A} \otimes M_d(F)$.

- Corollary: r' rows and r' columns can be found together with $A \in \mathcal{A} \otimes M_d(F)$ having a submatrix of full rank $r'd$ in these.

Blowups of matrix spaces

- $\mathcal{A} \otimes M_d(F)$: *"blown up"* matrix space (d: blowup factor)
  n by n matrices with entries from $F^{d\times d}$
- using divisibility, Derksen-Makam 2015-2017:

  reduce the blowup factor d to $d-1$ if $d \geq n$

  preserving the "relative rank":

  $\exists$ matrix of rank $d \cdot \mathrm{ncrk}$ in $\mathcal{A} \otimes M_d(F)$

  $\Downarrow$

  $\exists$ matrix of rank $(d-1) \cdot \mathrm{ncrk}$ in $\mathcal{A} \otimes M_{d-1}(F)$

- Corollary:
  $\mathrm{ncrk}\,\mathcal{A} = \frac{1}{d}\max$ rank in $\mathcal{A} \otimes M_d(F)$ for some $d \leq n-1$.

  $\Rightarrow$ ncrk computable in randomized poly time

A simple constructive blowup reduction

- start from $A \in \mathcal{A} \otimes M_d(F)$ of rank rd
- reducing d to $d-1$ if $d > r+1$ (Derksen-Makam $d > r-1$)
- Can assume that $n = r$ (find r rows and colums and $A' \in \mathcal{A} \otimes M_d(F)$ with submatrix of rank rd)
- Consider elements of $\mathcal{A} \otimes M_d(F)$ as $d \times d$ block matrices (blocks of size $n \times n$)
- delete the last row and column of blocks of A
- $(d-1) \times (d-1)$ block matrix of rank $\geq$ $\operatorname{rk} A - 2n = nd - 2n > nd - n - (d-1) = (n-1)(d-1)$
- round up to rank divisible by $d-1$: full rank $n(d-1)$

- Remark: IQS implement Derksen-Makam in det poly time

A simple blowup reduction - illustration

- $$\begin{pmatrix} A_{1,1} & \cdots & A_{1,d-1} & A_{1,d} \\ \vdots & \ddots & \vdots & \vdots \\ A_{d-1,1} & \cdots & A_{d-1,d-1} & A_{d-1,d} \\ A_{d,1} & \cdots & A_{d,d-1} & A_{d,d} \end{pmatrix}$$ of rank nd

- $$\begin{pmatrix} A_{1,1} & \cdots & A_{1,d-1} & \\ \vdots & \ddots & \vdots & \\ A_{d-1,1} & \cdots & A_{d-1,d-1} & \end{pmatrix}$$ of rank

  $$\geq nd - 2n > nd - n - (d-1) = (n-1)(d-1)$$

Deterministic polynomial time algorithms

- Garg, Gurvits, Oliveira, Wigderson 2015-2016:

  operator scaling for over fields of zero characteristic
- IQS 2015-2018: a constructive algorithm
  - computes a matrix of rank $d \cdot \operatorname{ncrk} \mathcal{A}$ in $\mathcal{A} \otimes F^{d \times d}$

    $d \leq n - 1$ (or $d \leq n \log n$ if F is too small)
  - computes an ("upper") witness for that ncrk cannot be larger
  - uses analogues of the alternating paths for matchings if graphs + efficient implementation of the DM reduction tool
- Franks, Soma, Goemans 2023:

  a version of GGOW that also finds an upper witness
- Hamada, Hirai 2021:

  convex optimization (based on finding an upper witness)

The upper witnesses: shrunk subspaces (Hall-like obstacles)

- ℓ-shrunk subspace: $U \le F^n$ mapped to a subspace of dimension $\dim U - \ell$ by $\mathcal{A}$

$$\mathcal{A} \le \begin{pmatrix} * & * & * & * & * \\ & & & * & * \\ & & & * & * \\ & & & * & * \end{pmatrix}; \text{ del. } \dim U - \ell \text{ rows and } n - \dim U \text{ cols} \to 0$$

$\exists$ ℓ-shrunk subsp. $\Rightarrow$ the max rank in $\mathcal{A}$ is at most $n - \ell$

- Inheritance: $U \otimes M_d(F)$ mapped to a subspace of dim less by $\ell \cdot d$ $\Rightarrow$ max rank in $\mathcal{A} \otimes F^{d \times d}$ is at most $nd - \ell d$.
- $\Rightarrow$ ncrk $\le n - \ell$
- $\sim$ a characterization of the nullcone of invariants $SL_n \times SL_n$ (by Hilbert-Mumford)

Main tool: the Wong sequence

- Idea: attempt to find a "maximally" shrunk subspace

  (used in spec. commutative cases: Fortin, Reutenauer 2004; I., Karpinski, Saxena 2010; I., Karpinski, Qiao, Santha 2015)

- Observation: Assume we have $B \in \mathcal{A}$ with $\mathrm{rk}\, B = \mathrm{ncrk}$, $\ell = n - \mathrm{ncrk}$, U ℓ-shrunk. Then

$$U \geq \ker B \text{ and } \mathcal{A}U = BU.$$

  - Proof: If $U \not\geq \ker B$ then $\dim U - \dim BU < \ell$;
  - $\dim BU = \dim U - \dim \ker B = \dim U - \ell$.

- $U = B^{-1}(AU)$ ($B^{-1}\cdot$: inverse image under B)

- Expand into iteration: Wong sequence

  ($\sim$ alternating forest in bipartite graph matching):

$$U_1 = \ker B;\ U_{j+1} = B^{-1}(\mathcal{A}U_j)$$

Wong sequence II

- Wong sequence (∼ alternating forest in bipartite graph matching):

  $U_1 = \ker B;\ U_{j+1} = B^{-1}(\mathcal{A}U_j)$
- Make B idempotent ($B^2 = B$)
  - multiply $\mathcal{A}$ by a pseudoinverse of B
- then $U_{j+1} = U_j + \mathcal{A}U_j$ if $U_j \leq \operatorname{Im} B$
- Either stabilizes inside $\operatorname{Im} B$: gives an ℓ-shrunk subspace

  $\longrightarrow$"done"
- or "escapes" : $\mathcal{A}U_j \not\subseteq \operatorname{Im} B$: (∼ $\exists$ augmenting path)

  How to exploit it?

Escaping Wong sequence $\sim$ augmenting path

- Key fact: ncrk $=$ rk if $\dim \mathcal{A} \leq 2$ (Atkinson, Stephens 1978)
  If $B^2 = B$ and $A^j \ker B \not\subseteq \mathrm{Im}\, B$ $A^j \ker B \not\subseteq \mathrm{Im}\, B$ for some j,
  then rk $(B + \lambda A) >$ rk B for some λ (if F is large enough)

  Proof: Take smallest j s.t. $A^j v \notin \mathrm{Im}\, B$ for some $v \in \ker B$
  $1, \ldots, u_r$ basis of $\mathrm{Im}\, B$ with "tail" $Av, \ldots, A^{j-1}v$.
  two lin. indep. systems: $u_1, \ldots, u_{r-j+1}, v, Av, \ldots, A_{j-1}v$ and
  $u_1, \ldots, u_{r-j+1}, Av, \ldots, A_{j-1}v, A^j v$
  $B + \lambda A$ has $r+1$ by $r+1$ block

$$
\begin{pmatrix}
* & * & * & & & & \\
* & \ddots & * & & & & \\
* & * & * & & & & \\
* & * & * & \lambda & 1 & & \\
\vdots & \vdots & \vdots & & \ddots & \ddots & \\
* & * & * & & & \lambda & 1 \\
* & * & * & & & & \lambda
\end{pmatrix}
\quad \text{upper left block: } I + \lambda A_0
$$

Escaping Wong sequence II

- $B^2 = B$, smallest s such that for some $A_1, \dots A_s \in \mathcal{A}$

$$A_s A_{s-1} \dots A_1 \ker B \not\subseteq \operatorname{Im} B$$

  (e.g., choose A_j from a basis of $\mathcal{A}$)
- Idea: try $B + \lambda A$ where $A = \sum \lambda_i A_i$
- Why ncrk $\neq$ rk in general: escaping "paths" may cancel out
  Example: 3×3 skew symmetric matrices

Cancel out ...

- Example: $\mathcal{A} = \mathrm{span}(A_1, A_2, A_3)$

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

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

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

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

Cancel out ... II

- $B^2 = B$, $A_2^2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $A_3^2 = \begin{pmatrix} 0 & 0 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$,

  $A_2 A_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$, $A_3 A_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$
- Lower right entry of $(xA_2 + yA_3)^2$ is $xy - yx = 0$.
- $(xA_2 + yA_3)^2 = \begin{pmatrix} xy & x^2 & 0 \\ -y^2 & -yx & 0 \\ 0 & 0 & 0 \end{pmatrix}$
- $(xA_2 + yA_3)^t$: zero last row and last column for $t > 1$

Escaping Wong sequence III

- Idea: try $B + \lambda A$ where $A = \sum \lambda_i A_i$
- Escaping "paths" may cancel out
- Workaround let $d > s$;
  - $A_j \otimes E_{j,j+1} \in \mathcal{A} \otimes M_d(F)$
    give a nonzero product in exactly one order
  - Put $A_1' = B' = B \otimes I_d$, $A_2' = \sum A_{i_j} \otimes E_{j,j+1}$; $\mathcal{A}' = \langle A_1', A_2' \rangle$
  - Then the Wong seq. escapes $\operatorname{Im} B'$ and
    $C' = B' + \lambda A_2'$ has rank $> d \cdot \operatorname{rk} B$ for some λ
  - Round up the rank of C' in $\mathcal{A} \otimes F^{d \times d}$ to a multiple of d

A high-level description of the algorithm

- iterate the above "scaled" rank incrementation procedure (with iteratively blowing up $\mathcal{A}$)
- combine with the reduction tool to control blowup factor
- Result: $A \in \mathcal{A} \otimes F^{d \times d}$ of rank $d \cdot \text{ncrk}$; and a maximally (by $(n - \text{ncrk})d$) shrunk subspace (of F^{nd}) for $\mathcal{A} \otimes F^{d \times d}$
- Use converse of inheritance to obtain a maximally (by $n - \text{ncrk}$) shrunk subspace of F^n for $\mathcal{A}$.
- Remarks:

  (1) Actually, *the smallest* maximally shrunk subspace found. ((0) if $\text{ncrk} = n$.)

  (2) The largest one can also be found (duality)

Reverse inheritence:

Maximal zero blocks in $\mathcal{A} \otimes M_d(F)$ are blowups of zero block in $\mathcal{A}$.

- $\mathcal{A} \otimes M_d(F)$ invariant under left-right multiplication by matrices from $I \otimes M_d(F)$
- $(\mathcal{A} \otimes M_d(F))U \leq U' \implies \mathcal{A} \otimes M_d(F)W \leq W'$, where $W = (1 \otimes M_d(F))U$, $W' = \bigcap_{B \in M_d(F)} (1 \otimes B)U'$
- $W = W_0 \otimes M_d(F)$, $W' = W_0' \otimes M_d(F)$
- Computation: first tensor components of basis elements for W, W' span W_0, W_0'

Skewfield construction: cyclic algebras

when d is not a multiple of char(F)

- $F' = F[\omega]$, $\omega = \sqrt[d]{1}$, $\qquad K = F'(x,y)$, $L = K[\sqrt[d]{y}]$
- $D = K\langle X, U\rangle/(X^d - x, U^d - y, UX - \omega XU)$

  K-basis of D: $X^i U^j$ $(i,j = 0, \dots d-1)$
- $U_0 = U \otimes 1/\sqrt[d]{y} \in D \otimes_K L$
- $E = U_0 + U_0^2 + \ldots + U_0^{d-1} + U_0^d \neq 0$
- $(U \otimes 1)^j E = \sqrt[d]{y}^j E$, so $\qquad (X^i \otimes 1)E \;\; (i = 1, \dots, d)$

  are a basis of the left ideal $J = (D \otimes L)E$ of $D \otimes L$.
- left multilication on J gives d-dim repr. of D over L: $D \otimes L \cong M_d(L)$

Skewfield construction - issues

- When d is a multiple of char(F):
  - $\nexists$ primitive $\sqrt[d]{1}$
  - $K\langle X\rangle \cong K[\sqrt[d]{x}]$ is replaced by a more complicated extension
    Artin–Schreier–Witt extensions involved
  - Alternatively, use rounding only for "good" blowups:
    reduce blowup factor d to $d-2$ if char$(F)|(d-1)$
    works when $d > 2\mathrm{ncrk}\,\mathcal{A}+2$
- Even when char$(F) \not| d$:
  - F can already contain "hidden" (part of) $\sqrt[d]{1}$
  - work with the ring $F' = F[\omega]/(1+\omega+\ldots\omega^d-1)$ as if it were a field
  - if a zero divisor emerges, replace F' with an ideal and restart

Applications I.: Module isomorphism (unpublished)

- Module data (over m-generated algebras)

  $B_1, \ldots, B_m \in M_n(F) \sim$ action of generators

- Space of homomorphisms

  V, V' with data $B_1, \ldots, B_m, B'_1, \ldots, B'_m$

$$\mathrm{Hom}(V, V') = \{A \in M_n(F) : AB_i = B'_i A\}$$

  Isomorphism: nonsingular element

- Blowups of Hom-spaces

$$\mathrm{Hom}(V, V') \otimes M_d(F) = \mathrm{Hom}(V^{\oplus d}, V'^{\oplus d})$$

Module isomorphism II.

- Krull-Schmidt
  - Unique direct decomposition into indecomposables
  - $V^{\oplus d} \cong V'^{\oplus d} \iff V \cong V'$
  - $V \cong V' \iff \operatorname{ncrk} \operatorname{Hom}(V, V') = n$
- deciding $\cong$: a simple application of ncrank computation
- can be made constructive

  using a "lazy" constructive Krull-Schmidt
- $\exists$ several more direct approaches, e.g.,
  - Brooksbank, Luks (2008)
  - I., Karpinski, Saxena (2010)

    based on Chistov, I., Karpinski (1997) (for the semisimple case)
  - Ciocănea-Teodorescu (2015)

Applications II. (Invariant theory and related)

- Orbit closure separation for left-right action of SL
  - Derksen, Makam 2018
    Compute a separating invariant (if $\exists$)
- Brascamp-Lieb inequalities

$$\int_{x\in\mathbb{R}^n} \prod_i (f_i(B_i x))^{p_i}\, dx \le C \prod_i \left(\int_{y_i \in \mathbb{R}^{n_i}\, f_i(y_i} dy_i \right)^{p_i}$$

  $\forall\ 0 \le f_i :\in L^1(\mathbb{R}^{n_i})$
  $0 < C \le \infty$ (the BL-constant)
  depending on $B_i \in \mathbb{R}^{n_i \times n}$, $p_i \ge 0$.
  - capture many known inequalities, e.g., Hölder's
  - Garg, Gurvits, Oliveira, Wigderson 2018
    Operator scaling for a related matrix space computes C
  - $C < \infty$ iff full ncrk

Applications III: Block triangularization

in the full ncrk case

- $\sim$ finding flag of 0-shrunk subspaces U ($\dim \mathcal{A}U = \dim U$)
- If $I \in \mathcal{A}$ then (as $\mathcal{A}W \geq W$) equivalent to $\mathcal{A}U = U$.
  - U: a submodule for the enveloping algebra of $\mathcal{A}$,
  - over many F, $\exists$ good algorithms
- If $A \in \mathcal{A}$ of full rank found, $I \in A^{-1}\mathcal{A}$

$$\mathcal{A} \leftarrow A^{-1}\mathcal{A}$$

More generally:

- Find $A \in \mathcal{A} \otimes M_d(F)$ of full rank,
- Block triangularize $\mathcal{A} \otimes M_d(F)$ as above
- Pull back by "reverse inheritance"

  Blowup as a "magnifier"

Applications of block triangularization

- Effective orbit closure intersection
  - I., Qiao 2023
  - Compute one-parameter subgroups driving from orbits to the intersection of orbit closures
- In multivariate cryptography
  - based on hardness of solving polynomial systems
  - Sometimes: secret $\sim$ block triang. strucure
  - e.g, Patarin's balanced Oil and Vinegar scheme

Oil and Vinegar singature schemes

- Oil and Vinegar signature schemes – Patarin (1997), ...
- Public key: $P = (P_1, \dots, P_k) \in F[\underline{x}]^k$ $\underline{x} = (x_1, \dots, x_n)$, $\deg P = 2$
  - Message: $\underline{a} \in F^k$
  - Valid signature: a solution of $P(\underline{x}) = \underline{a}$
- Private key (hidden structure): P', B s.t.
  - $P'(\underline{y}) = \underline{a}$ "easy" to solve
  - $P = P' \circ B$, $B \in GL_n(F)$
  - a linear change of variables
- "easiness":
  - P' is linear in the first o variables:

    no terms $x_i x_j$ with $i, j \in \{1, \dots, o\}$
  - by a random substitution for x_j ($j = o + 1, \dots, n$) we have a solvable linear system (with "good" chance)
  - $x_1, \dots, x_o$: "*oil* variables"; $x_{o+1}, \dots, n$ "*vinegar* variables"
- Key generation: choose *such* P' randomly, and B randomly
- Tuning: choose the parameters k, o, n:
  - P' easy to solve
  - hard to break

Oil and Vinegar II.

- *Balanced* O & V (Patarin 1997):

  $n = 2o$ (and $k \approx o$)

  - quadratic part of the secret system: $\begin{pmatrix} & * \\ * & * \end{pmatrix}$

  $\Rightarrow$ bad choice
- Breaking Balanced O & V (Kipnis, Shamir 1998)
  - $P_i = Q_i +$ linear
  - $\mathrm{span}(Q_1, \ldots, Q_k)$ has full rank (for random P)
  - the hole (the "vinegar subspace") is unique (for random P)
- *Unbalanced* O & V (Kipnis, Patarin 1999)
  - better

    "hardness": Bulygin, Petzoldt, Buchmann (2010)

On Wong sequences and the commutative rank

Wong sequence: $U_1 = \ker B$; $U_{i+1} = B^{-1}(\mathcal{A}U_i)$.

- Progress of the seq. ($\approx$ Bläser, Jindal, Pandey 2017) If $\mathcal{A}U_i \leq \operatorname{Im} B$ then $\dim U_{i+1} \geq \dim \mathcal{A}U_i + \operatorname{ncrk} \mathcal{A} - \operatorname{rk} B$
  - Proof:
  - $\dim U_{i+1} = \dim \mathcal{A}U_i + \dim \ker B = \dim \mathcal{A}U_i + n - \operatorname{rk} B$
  - $\dim \mathcal{A}U_i \geq \dim U_i - (n - \operatorname{ncrk} \mathcal{A})$
- Interpretation: Far from the ncrk , the Wong sequence expands quickly $\Longrightarrow$ is short
- Bläser, Jindal, Pandey 2017: deterministic commutative rank approximation scheme based on the above
  - Key observation: Assume B idempotent, $(\sum_{i=1}^{k} x_i A_i)^s v \notin \operatorname{Im} B \Longrightarrow (\sum_{i \in I}^{k} x_i A_i)^s v \notin \operatorname{Im} B$ for some at most s-element subset I of $\{1, \ldots, k\}$

Wong sequences and the commutative rank II

In extreme cases, ncrk $=$ rk

- Immediately escaping case: length 1
  - $\mathrm{rk}\,(B+\lambda A_i) > \mathrm{rk}\,B$ for some i and λ:
    $\longrightarrow$ "blind" rank incrementing algorithm
    Notable cases:
  - when $\mathcal{A} = \mathrm{Hom}(V_1, V_2)$ where V_1, V_2 semisimple modules
  - when $\mathcal{A}$ simultaneously diagonalizable
- Slim Wong sequence: $\dim U_{j+1} = \dim U_j + 1$
  - can be enforced if $\mathcal{A}$ spanned by rank 1 matrices
    I., Karpinski, Saxena (2010)
    even if they are not given explicitly
    I., Karpinski, Qiao, Santha (2014)
  - Proof/algorithm: similar to the 2-dimensional $\mathcal{A}$ case

Slim Wong sequence: $\dim U_{j+1} = \dim U_j + 1$

- again, make B idempotent
- $v \in \ker B$ s.t. $\mathcal{A}v \neq 0$.
- $v_1 \in \mathcal{A}v \setminus \{0\}$, $v_{j+1} \in U_{j+1} \setminus U_j$
- $u_1, \ldots, u_r$: basis of $\operatorname{Im} B$ with tail $v_1, \ldots, v_{s-1}$
- two systems: $u_1, \ldots, u_{r-s+1}, v, v_1, \ldots v_{s-1}$ and $u_1, \ldots, u_{r-s+1}, v_1, \ldots v_{s-1}, v_s$
- $\mathcal{A}$ has block triangular $r+1$ by $r+1$ block $\begin{pmatrix} \mathcal{B} & \\ \mathcal{C} & \mathcal{D} \end{pmatrix}$, u-left-block of B: I, $\mathcal{D}$ non-singular upper triangular,
- find $A \in \mathcal{A}$ non-singular in $\mathcal{D}$
- $B + \lambda A$ has rank $\geq r+1$ for some λ