PIT problems in the light of and the noncommutative rank algorithm

Gábor Ivanyos
MTA SZTAKI

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

(co-)PIT problems in this talk

- NONSINGULAR:

  $\det(x_0 A_0 + x_1 A_1 + \ldots + x_k A_k) \not\equiv 0$

  $\approx \exists$ a non-singular matrix in $\mathcal{A} = \langle A_0, \ldots, A_k \rangle$

  $\approx$ What is $\operatorname{rk} \mathcal{A}$, the (commutative) rank of ($=$ max rk in) $\mathcal{A}$?

  Constructive version (rank optimization):

  Find a matrix of max rank in $\mathcal{A}$
- focus on deterministic solutions
  - + interesting applications of randomized solutions
- We assume square case

  problems (mostly) reducible to that

Overview

- Common block triangular forms of matrices
- Behavior of Wong sequences
- Module problems: from easy to hard

+ If time left:

  Spaces spanned by *unknown* rank one matrices

Some notation

- $M_n(F) = M_{n\times n}(F)$
- Block matrices, ”holes” in matrices:

$$\begin{pmatrix} A & B \\ & C \end{pmatrix} = \left(\begin{array}{|c|c|}\hline A & B \\ \hline 0 & C \\ \hline \end{array}\right)$$

- Block (upper) triangular matrices: $\begin{pmatrix} A & B \\ & C \end{pmatrix}$, A and C *square*
- Matrix sets: $\begin{pmatrix} A & * \\ & * \end{pmatrix} = \left\{ \begin{pmatrix} A & B \\ & C \end{pmatrix} : B, C\text{arbitrary} \right\}$

Notation (2)

- Product of sets:

$$\mathcal{A}U = \{Au : A \in \mathcal{A}, u \in U\}$$

(subspace when either $\mathcal{A}$ or U is a subspace)

- $\mathcal{A}$-invariant ($\mathcal{A}$-closed) subspace:

$$U \text{ s.t. } U \subseteq \mathcal{A}U$$

- $\sim$ (similarity): in the same orbit of conjugation by GL, changing the basis
- $\approx$ ($\approx_{GL\times GL}$): in the same orbit of (independent) left-right multiplication by GL changing the two bases independently

Multivariate crytography

- Quantum computer (if $\exists$) factor integers,
  compute discrete log

  $\Rightarrow$ threat to present public key schemes
- Looking for "quantum-safe" primitives

  Multivariate crypto:
  based on hardness of solving polynomial systems
- 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 $P(\underline{x}) = \underline{a}$

Oil and Vinegar schemes

- Private key (hidden structure): P', A s.t.
  - $P'(\underline{y}) = \underline{a}$ "easy" to solve
  - $P = P' \circ A$, $A \in GL_n(F)$
  - a linear change of variables
- "easiness":
  - P' is linear in the first o variables:

    no terms $x_i x_j$ with $i, j \in \{1, \ldots, o\}$
  - by a random substitution for x_j ($j = o+1, \ldots, n$) we have a solvable linear system (with "good" chance)
  - $x_1, \ldots, x_o$: "*oil* variables"; $x_{o+1}, \ldots, n$ "*vinegar* variables"
- Key generation: choose *such* P' randomly, and A randomly
- Tuning: choose the parameters k, o, n:
  - P' easy to solve
  - hard to break
- *Balanced* O & V (Patarin 1997):

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

Oil and Vinegar (2)

- Balanced O & V:
  - quadratic part of the secret system: $\begin{pmatrix} & * \\ * & * \end{pmatrix}$
  - balance allows (more) algebra to act:
    hole in the sructure → hole in security
  - bad choice for practical use
  - good for publicity:)
- Breaking Balanced O & V (Kipnis & Shamir 1998)
  - $P_i = Q_i +$ linear
  - $\exists\ Q_0 = \sum \alpha_i Q_i$ invertible (for random P)
  - the hole (the "vinegar subspace") is unique (for random P)
  - divide Q_i by Q_0: reduce finding the hole to
    finding common invariant subspaces
- *Unbalanced* O & V
  (Kipnis & Patarin 1999)
  better
  "hardness": Bulygin, Petzoldt & Buchmann (2010)

Block triangular forms: the "holes"

- $G\mathcal{A}H \subseteq \begin{pmatrix} * & * \\ & * \end{pmatrix}$,

  $n - t \times t$ zero lower left block

  Remark: for O & V: $G = \begin{pmatrix} & I \\ I & \end{pmatrix} H^T$
- reduces many problems

  to the diag. blocks
- e.g, finding full rk. $A \in \mathcal{A}$;

  Find $B \in \mathcal{A}$ with invertible upper left block,

  $C \in \mathcal{A}$ with invertible lower block,

  $\lambda B + C$ will be invertible except for a few λs

Block triangular forms (2)

- The full (commutative) rank case: $A_0 \in \mathcal{A}$ invertible
- use A_0 as a bijection between the domain and range

  $\sim$ a prefect matchings: bipartite graphs → digraphs
- "Fractional" matrix space: $A_0^{-1}\mathcal{A}$
- $A_0^{-1}\mathcal{A} = A_0^{-1}\mathcal{A}I \approx_{GL\times GL} \mathcal{A}$, inherits block triang.
- $(GA_0H)^{-1}G\mathcal{A}H = H^{-1}A_0^{-1}G^{-1}G\mathcal{A}H = H^{-1}A_0^{-1}\mathcal{A}H$

  New action: conjugation $X \mapsto H^{-1}XH$

  $=$ two-sided action of $GL \times GL$ preserving I

Block triangular forms (3)

- $H^{-1}\mathcal{A}H \subseteq \begin{pmatrix} * & * \\ & * \end{pmatrix}$, $n-t \times t$ zero block
- First t basis vectors span an $H^{-1}\mathcal{A}H$-invariant subspace U'
  - $U = H^{-1}U'$ t-dim $\mathcal{A}$-invariant subspace

  $\sim$ nontrivial strong components in digraphs
- Env($\mathcal{A}$) *enveloping (matrix) algebra*

  closure of $\mathcal{A}$ w.r.t. lin. comb. and multiplications

  $\sim$ transitive closure of digraphs
- $\mathcal{A}$-invariant subspace:

  submodule for Env($\mathcal{A}$) (or for the free algebra)

Finding common invariant subspaces

- Quite well studied/understood
- Many of the methods: based on structure of $\mathrm{Env}(\mathcal{A})$

  one-sided ideals, zero divisors

  - for $\mathcal{A} = \langle I, A_0 \rangle$: factors of the minimum polynomials of A_0
  - general $\mathcal{A}$: zero div. ← factoring min. pol. of "good" $A \in \mathrm{Env}(\mathcal{A})$
- over algebraically closed fields: "almost" easy
  - Depends on the computational model
  - Representation size explosion? E.g. "huge" (composite) extensions
    - $M_{2n}(\mathbb{Q}) \ni A \sim \begin{pmatrix} \sqrt{2} & & & & \\ & -\sqrt{2} & & & \\ & & \ddots & & \\ & & & \sqrt{p_n} & \\ & & & & -\sqrt{p_n} \end{pmatrix}$

Finding invariant subspaces - ”rationality” issues

- over non-closed base fields (extensions not allowed)
- over finite fields: only randomized methods (in large char),

  equivalent to factoring polynomials

  tool: *MeatAxe*

  standard, polished package for group representations
- over $\mathbb{Q}$ only a partial decompositions
  - Hardness of distinguishing full matrix algebras from division algebras over $\mathbb{Q}$ (Rónyai 1987):

    in some generalizations of the quaternions

    existence of zero divisors $\gtrapprox$ quadratic residuousity
    mod composite numbers

    finding zero divisors: $\gtrapprox$ factoring integers
  - the source of regularity of blowups

From hardness to regularity

- Assume $\mathcal{A} \leq M_n(F)$ violates regularity for some d:
- $r = \operatorname{rk}(\mathcal{A} \otimes M_d(F)$ is nor divisible by d
- Algorithm

  Input: $\mathcal{D} \cong M_d(F)$ (unkown iso)

  - take $C \in \mathcal{A} \otimes \mathcal{D}$ random
  - consider C a matrix with entries from $\mathcal{D}$
  - try right Gaussian elimation
  - succeeds: only if $\operatorname{rk} C$ is divisible by d
  - fails: zero divisor found in $\mathcal{D}$

    ↑ this is the case for random C

  Output: the zero divisor

Using blowups for block triangularization

- $\mathcal{A}' = \mathcal{A} \otimes M_d(F)$ (on $F^n \otimes F^d$).
  Property $\mathcal{A}' = (I_n \otimes M_d(F))\mathcal{A}') = \mathcal{A}'(I_n \otimes M_d(F))$
  (this *characterizes* blowups)
- $\mathcal{A}'U' \leq V' \Longrightarrow \mathcal{A}'(I_n \otimes M_d(F))U'$ is an
  $I_n \otimes M_d(F)$-invariant subsp. of V'
- $I_n \otimes M_d(F)$-invariant subspaces of $F^n \otimes F^d$:
  - $(I \otimes M_d(F))U' = U' \Longleftrightarrow U' = U \otimes F^d$
    $U = \{u \in F^n : u \otimes v \in U' \text{ for some } 0 \neq v \in F^d\}$
    Computing U:
    - $v_1, \ldots, v_d$: basis for F^d, $u'_1, \ldots, u'_k$: basis for U'
    - $u'_i = \sum u_{ij} \otimes v_j \quad u_{ij} \in F^n$
    - U is spanned by u_{ij} $(i = 1, \ldots, k\ j = 1, \ldots, d)$

Using blowups (2)

- Holes (lower left zero blocks) in blowups:
- $\mathcal{A}' = \mathcal{A} \otimes M_d(F)$
  - U', V' $(I \otimes M_d(F))$-invariant subsp.
  - $U' = U \otimes M_d(F)$, $V = V \otimes M_d(F)$
  - $\mathcal{A}'U' \leq V' \iff \mathcal{A}U \leq \mathcal{A}V$
  - "holes" in $\mathcal{A}'$ $\longleftrightarrow$ "holes" in $\mathcal{A}$
  - block triang forms of $\mathcal{A}'$ $\longleftrightarrow$ block triang forms of $\mathcal{A}$
- Application of constructive ncrank:find
  - "singular" block triang of *some* blowup $\mathcal{A}'$

    $\longrightarrow$ block triang of $\mathcal{A}$
  - or an invertible element in *some* blowup $\mathcal{A}'$

    $\longrightarrow$ block triang $\mathcal{A}'$

    $\longrightarrow$ a block triang of $\mathcal{A}'$
- More serious applications in the next talk

The Wong sequence

- Given $A_0, A_1, \ldots, A_k \in M_n(F)$
  - $\mathcal{A} = \langle A_0, \ldots, A_k \rangle$
  - $\operatorname{rk} A_0 = r < n$, $c = n - r$ (co-rank of A_0)
- Idealistic goal: find

  case (1) $A' \in \mathcal{A}$ s.t. $\operatorname{rk} A' > r$ or
  case (2) $U \leq F^n$ s.t. $\dim \mathcal{A}U \leq \dim U - c$
- $U'_0 = (0)$, $U_j = A_0^{-1} U'_j$, $U'_{j+1} = \mathcal{A}U_j$

  ($A_0^{-1}W$: full inverse image of W at A_0)
  - $U'_0 \leq U'_1 \leq \ldots \leq U'_\ell$, $U_0 \leq U_1 \leq \ldots \leq U_\ell$
  - $\ldots, U'_j, \ldots$ stops inside $\operatorname{im} A_0 \Leftrightarrow$ case (2)
  - otherwise *escapes* from $\operatorname{im} A_0$: $\mathcal{A}U_j \not\subseteq \operatorname{im} A_0$ for some j
- *length of the (escaping) Wong sequence*

  $\ell = \min\{j : \mathcal{A}U_{j-1} \not\subseteq \operatorname{im} A_0\}$

Length 1 Wong sequence

- $\ell = 1$; basic case $n = r + 1$, $A_0 = \begin{pmatrix} I_r & \\ & \end{pmatrix}$, $r > 0$
- $\mathcal{A} \ker A_0 \not\leq \operatorname{im} A_0$
- $\exists i$: $A_i \ker A_0 \not\subseteq \operatorname{im} A_0$ (lower right entry of A_i is $b \neq 0$)
- $A_i + \lambda A_0 \approx \begin{pmatrix} B' + \lambda I & * \\ * & b \end{pmatrix} \approx \begin{pmatrix} B'' + \lambda I & * \\ & b \end{pmatrix}$ $(b \neq 0)$
- has rank $> r$ if λ and is not an eigenvalue of B''

  (F large enough)
- "Blind" algorithm

  compute $\operatorname{rk}(A_i + \lambda A_0)$

  $(i = 1, \ldots, k,\ \lambda = \lambda_1, \ldots, \lambda_{r+1})$

Length 1 - some examples

- Examples (long Wong sequences):

$$A_0 = \begin{pmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ & & & \end{pmatrix},$$

  - $k = 1$, $A_1 = I$: $\operatorname{rk}(A_0 + A_1) > \operatorname{rk} A_0$
  - $k = n > 1$, $A_i = E_{ii}$: $\operatorname{rk}(A_0 + A_i) = \operatorname{rk} A_0$
- Length one — a "nice" property:
  - independent of the basis for $\mathcal{A}$
  - preserved by $\approx_{GL_n \times GL_n}$
  - preserved by base field extension
- $F = \mathbb{R}$; A_0, A_i pos. semidef.
  - $v \in \ker A_0 \setminus \ker A_i = (\operatorname{im} A_0)^{\perp} \setminus \ker A_i$
  - $0 \neq v^T A_i v$, but $v^T A_0 w = 0$ for every w

Length 1 - examples (2)

- A_i diagonal ($i = 0, \ldots, k$)
  - $\exists i, v$: $\operatorname{im} A_0 \cap \ker A_0 = (0)$
  - $\ker A_0$, A_i-invariant (because $A_i A_0 = A_0 A_i$)
  - $A_i \ker A_0 \leq \operatorname{im} A_0 \Leftrightarrow \ker A_0 \subseteq \ker A_i$
- Application of diag case: simplicity of finite extensions of $\mathbb{Q}$:
- the above examples are trivial:

  $\exists A \in \mathcal{A}$ s.t. $\ker A \subseteq \ker B$ for every $B \in \mathcal{A}$
- Remark: $\exists$ less trivial examples:

  homomorphisms between modules of special type
  (special: semisimple)

Short Wong sequences

- Key observation of Bläser, Jindal & Pandey (2017)

$$\mathcal{A} = \langle A_0, A_1, \ldots, A_k \rangle$$
$$\mathcal{A}' = \langle A_0, A_1' \rangle \text{ (over } F(x_1, \ldots, x_k))$$
$$A_1' = x_1 A_1 + \ldots, x_k A_k$$

A_0 not of max rank in $\mathcal{A}$

$\Updownarrow$ (F sufficiently large)

A_0 not of max rank in $\mathcal{A}'$

$\Updownarrow$ (rk $=$ ncrk for pair $\mathcal{A}'$)

$A_1' U_{\ell-1} \not\leq \operatorname{im} A_0$

$U_1, \ldots, U_{\ell-1}$ Wong sequence for A_0 in $\mathcal{A}'$

Short Wong sequences (2)

- Assume basic case $A_0 = \begin{pmatrix} I_r & \\ & \end{pmatrix}$, $n = r + 1$
- $A_1' U_{\ell-1} = {A_1'}^{\ell} \ker A_0$
- lower right entry of ${A_1'}^{\ell}$:
  - nonzero degree ℓ polynomial in $x_1, \ldots, x_k$
  - has term $a \cdot x_{i_1} \ldots x_{i_\ell}$
  - A_0 is not of max rank in $\mathcal{A}'' = \langle A_0, x_{i_1} A_{i_1} + \ldots + x_{i_\ell} A_{i_\ell} \rangle$
  - A_0 is not of max rank in $\mathcal{A}''' = \langle A_0, A_{i_1}, \ldots, A_{i_\ell} \rangle$.
- Assume $\ell' \geq$ length of Wong seq. for $\mathcal{A}'$. Then

  A_0 is of max rank in $\langle A_0, A_1, \ldots, A_k \rangle$

  $\Updownarrow$

  A_0 is of max rank in $\langle A_0, A_{i_1}, \ldots, A_{i_{\ell'}} \rangle$

  for every subset $\{i_1, \ldots, i_{\ell'}\} \subseteq \{1, \ldots, k\}$
- a simpe algorithm of complexity $(kn)^{\ell'} \cdot poly$

Short Wong sequences (3)

Algorithm (Bläser, Jindal & Pandey (2017))

- Input: $A_0, A_1, \ldots, A_k$ and $\ell \leq k$
- Output: $A_0' \in \mathcal{A}$ of rank $> \operatorname{rk} A_0$

  or: "ℓ IS TOO SMALL"
- for every subset $\{i_1, \ldots, i_\ell\} \subseteq \{1, \ldots, k\}$

  try $A_0 + \sum_{t=1}^{\ell} \omega_t A_{i_t}$

  for all $(\omega_1, \ldots, \omega_\ell) \in \Omega^\ell$ $(|\Omega| = n)$
- complexity $(kn)^\ell \cdot \mathit{poly}$

Progress of Wong sequences

- Wong sequence $U'_0 = (0)$, $U'_j = \mathcal{A}A_0^{-1}A_0$
- $U'_j \subseteq \operatorname{im} A_0$ $(j = 0, \ldots, \ell - 1)$
- Lemma (BJP17 for case $k = 2$) Assume that $\operatorname{rk} A_0 = r < \operatorname{ncrk} \mathcal{A}$. Then for every $1 \leq j < \ell$, $\dim U'_j \geq \dim U'_{j-1} + \operatorname{ncrk} \mathcal{A} - r$.
  - sufficient to prove for $n = \operatorname{ncrk} \mathcal{A}$ ("basic case")
    $A_0 = \begin{pmatrix} I_r & \\ & \end{pmatrix}$; $s = \operatorname{ncrk} \mathcal{A}$,
    take an $s \times s$ "window" of full ncrk
    containing the upper left r by r

Progress of Wong (2)

$A_0 = \begin{pmatrix} I_r & \\ & \end{pmatrix}$ $F^n = \operatorname{im} A_0 \oplus \ker A_0$, block structure using

$(0) = U'_0 < U'_1 < \ldots < U'_{\ell-1} \leq \operatorname{im} A_0$

$$\mathcal{A} \ni A = \begin{pmatrix} \boxed{B_1} & B_{12} & \cdots & B_{17} & B_{18} & B_{19} \\ B_{21} & \boxed{B_2} & \cdots & B_{27} & B_{28} & \\ & \ddots & \ddots & \vdots & \vdots & \\ & & B_{76} & \boxed{B_7} & B_{78} & \\ & & & B_{87} & \boxed{B_8} & \\ & & & B_{97} & B_{98} & \end{pmatrix} \qquad (7 = \ell)$$

$B_{jj} = B_j$ square (I for A_0); $B_{\ell+2,\ell} \neq 0$

cyclically shift by $n - r$

Progress of Wong (3)

diagonal shifted by $n - r$ to the right

$$A \approx \begin{pmatrix} B_{19} & \boxed{B_1} & B_{12} & \cdots & B_{17} & B_{18} \\ & B_{21} & \boxed{B_2} & \cdots & B_{27} & B_{28} \\ & & \ddots & \ddots & \vdots & \vdots \\ & & & B_{76} & \boxed{B_7} & B_{78} \\ & & & & B_{87} & \boxed{B_8} \\ & & & & B_{97} & B_{98} \end{pmatrix}$$

$B_{jj} = B_j$ has $\geq n - r$ columns

otherwise a $t \times t'$ "hole" with $t + t' > n$

Progress of Wong (3)

- A "formal" proof the lemma

  for $1 \leq j < \ell$:

  $$U_{j-1} = A_0^{-1} U'_{j-1} = U'_{j-1} \oplus \ker A_0 \qquad \text{for } A_0 = \begin{pmatrix} I_r & \\ & \end{pmatrix};$$

  $$\begin{aligned} \dim U'_j = \dim \mathcal{A} U_{j-1} &\geq \dim U_{j-1} \quad \text{(full ncrank)} \\ &= \dim U'_{j-1} + \dim \ker A_0 \\ &= \dim U'_{j-1} + n - r \end{aligned}$$

Approximating the commutative rank

- Bläser, Jindal & Pandey (2017)
- $r = \text{max. rk in } \mathcal{A} = \langle A_1, \ldots, A_k \rangle$
- goal: find $A \in \mathcal{A}$: $\operatorname{rk} A \geq (1-\epsilon)r)$
- $\ell = \min(k, \lfloor 1/\epsilon \rfloor)$
- Iteration
  - if $\operatorname{rk} A_0 \leq (1-\epsilon r)$ then:
    length of Wong seq. for A_0 and $x_1 A_1 + \ldots + x_k A_k$
    $\leq \operatorname{rk} A_0 / (r - \operatorname{rk} A_0) \leq (1-\epsilon)/\epsilon = 1/\epsilon - 1$
- try $A_0' = A_0 + \omega_1 A_{i_1} + \ldots + \omega_\ell A_{i\ell}$
- replace A_0 with A_0' if better
- terminate if no improvement
- Cost: $(kn)^{1/\epsilon} \cdot \mathit{poly}$

Thin Wong sequences

- $\dim U_{j+1} = \dim U_j + 1$ $(j = 0, \ldots, \ell - 1)$
- basic case $n = \operatorname{rk} A_0 + 1$

$$\begin{pmatrix} b_{11} & b_{12} & \cdots & b_{17} & B_{18} & b_{19} \\ b_{21} & b_{22} & \cdots & b_{27} & B_{28} & \\ & \ddots & \ddots & \vdots & \vdots & \\ & & b_{76} & b_{77} & B_{78} & \\ & & & B_{87} & B_{88} & \\ & & & b_{97} & B_{98} & \end{pmatrix} \approx \begin{pmatrix} b_{19} & b_{11} & b_{12} & \cdots & b_{17} & B_{18} \\ & b_{21} & b_{22} & \cdots & b_{27} & B_{28} \\ & & \ddots & \ddots & \vdots & \vdots \\ & & & b_{76} & b_{77} & B_{78} \\ & & & & b_{97} & B_{98} \\ & & & & B_{87} & B_{88} \end{pmatrix}$$

$(7 = \ell + 1)$

- find $A' \in \mathcal{A}$ with no zero diag entry in the big upper left part
- find $A' + \lambda A_0$ with invertible lower right diag block (B_{88})

Thin Wong sequences (2)

- Remark: rank of diagonal A_i is hard over F of constant size $q \geq 3$:

  reduction from coloring with q colors:

  vertices: $v_1, \ldots, v_k$, edges $e_1, \ldots, e_n$

  $$(A_i)_{tt} = \begin{cases} +1 & \text{if } e_t = \{v_i, v_j\},\ j > i \\ -1 & \text{if } e_t = \{v_i, v_j\},\ j < i \quad (i = 1, \ldots, k) \\ 0 & \text{otherwise.} \end{cases}$$

- special instances:
  - pencils: $\mathcal{A} = \langle A_0, A_1 \rangle$
  - $A_1, \ldots, A_k$ of rank one:

    find smallest ℓ, $A_{i_\ell} \ldots A_{i_1} \ker A_0 \not\subseteq \operatorname{im} A_0$

    $\mathcal{A} \leftarrow \langle A_0, A_{i_1}, \ldots, A_{i_\ell} \rangle$
  - $\exists$ poly method for $\mathcal{A}$ spanned by A_0 and unknown rank one matrices

Wong sequences - remarks & problems

- Triangularizable spaces of full rank:

$$\mathcal{A} \lessapprox_{GL\times GL} \begin{pmatrix} * & \cdots & * \\ & \ddots & \vdots \\ & & * \end{pmatrix}$$

  - Would be "length 1" for $\operatorname{rk} A^n$

    rank of the "diagonal part"

    triangularization by *conjugation*
  - Dual Wong sequence could recover part of triang structure
- Shortening Wong with $A_0 \leftarrow A_0 + \lambda A_i$?
  - Example: A_0 triangular, $A_1, \ldots, A_k$ diagonal
  - Nicer classes?
- Nice classes for length ≤ 2?

Wong sequences - remarks & problems (2)

- Length and blowup size
  - length $\geq 2\times$ "*current*" blowup size
    (sufficient to increase rk A_0)
  - thinness at a single step → block triang
  - $\Rightarrow$ "current" blowup size $\lesssim \text{rk}\, A_0/4$
  - relation with "final" blowup size?
  - computing commutative rank for bounded blowup size?
- Rank of generators
  - rank one: blowup size 1
  - rank ≤ 2: *current* blowup size ≤ 2 (looks so)
    final blowup size????
    in special cases, e.g., (skew) symmetric?
  - rank $\leq c$: bound on *current* blowup size?

Modules

- modules for the free algebra $\widetilde{\mathcal{B}} = F\langle X_1, \ldots, X_t \rangle$
- n-dimensional (left) $\widetilde{\mathcal{B}}$-module:
    - $V \cong F^n$, $\cdot : \widetilde{\mathcal{B}} \times V \to V$

      bilinear

      commutes with $\cdot$ of $\widetilde{\mathcal{B}}$: $(a \cdot b) \cdot v = a \cdot (b \cdot v)$

      Notation: $av = a \cdot v$
    - input data: linear maps $L_1, \ldots, L_t : V \to V$ ($n \times n$ matrices)

      action of $X_1 \cdot, \ldots, X_t \cdot$

      $\sim$ multiplication tables in groups
    - could take smaller (finite dim.) $\widetilde{\mathcal{B}}$
- Isomorphisms
    - V, V', given by $L_1, \ldots, L_t \in M_n(F)$, $L'_1, \ldots, L'_t \in M_n(F)$
    - $\phi : V \to V'$ bijective linear
    - $X_i \cdot \phi(v) = \phi(X_i \cdot v)$
    - $L'_i \circ \phi = \phi \circ L_i$

Module morphisms (2)

- Homomorphisms
  - V, V', given by $L_1, \ldots, L_t \in M_n(F)$, $L'_1, \ldots, L'_t \in M_{n'}(F)$

  $\mathrm{Hom}(V, V') := \{\phi : V \to V' \text{ lin. } : \quad \phi \circ L_i = L'_i \circ \phi\}$

  subspace of $\mathrm{Lin}_{n' \times n}(F)$

  solutions of the lin. constraints $\phi \circ L_i = L'_i \circ \phi$
- Isomorphism: a full rank matrix $\in \mathrm{Hom}(V, V')$ $(n' = n)$
- In $\mathcal{P}$:
  - Chistov, I & Karpinski (1997) over many fields;
  - Brooksbank & Luks (08); I, Karpinski & Saxena (010) all fields
- Length 1 Wong sequence in a special case ....

Module morphisms (3)

- submodule

  Common invariant subspaces for L_i
  Block triangular form of L_i
  simple (irreducible) modules: no proper submodules

- direct sum

  "external": space $V \oplus V'$; action $\begin{pmatrix} L_i & \\ & L_i' \end{pmatrix}$
  "internal": $V = V_1 \oplus V_2$ (of subspaces), V_1, V_2 submodule
  block diagonal form for L_i
  indecomposable modules: no such decomp.

- Krull-Schmidt:

  "uniqueness" of decomposition into indecomposables:
  isomorphism types and multiplicities
  $\sim$ factorization of numbers

Module isomorphism - the decision version

- A "simple" ncrank-based method
- Key observation:

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

- Consequence: (assume $\dim V = \dim V' = n$):

$$V \cong V' \Leftrightarrow \mathrm{ncrk}\,(\mathrm{Hom}(V, V') = n$$

Proof.

$$\begin{aligned} V \cong V' \ &\Rightarrow \ \mathrm{rk}\,\mathrm{Hom}(V, V') = n \ \Rightarrow \ \mathrm{ncrk}\,\mathrm{Hom}(V, V') = n \\ &\Rightarrow \ V^{\oplus d} \cong {V'}^{\oplus d} \text{ for some } d \\ &\Rightarrow \quad V \cong V' \text{ by (Krull-Schmidt)} \end{aligned}$$

Hardness of injectivity

- Are spaces $\mathrm{Hom}(V, V')$ special?

  NO: every matrix space is essentially $\mathrm{Hom}(V, V')$
  Construction: I, Karpinski & Saxena (2010)

- $A_1, \ldots, A_k$ arbitrary $n \times n$
- V, V' modules for $F\langle x_1, \ldots, x_n, x_{n+1}\rangle$
- $\dim V = n + 1$, $\dim V' = n + k$
- $L_j = \begin{pmatrix} & e_j \\ & \end{pmatrix}$ $n+1 \times n+1$ $\quad e_j = \begin{pmatrix} \\ 1 \\ \\ \end{pmatrix} \leftarrow j \quad (j \leq n)$
- $L_j' = \begin{pmatrix} & \widehat{\mathcal{A}}_j \\ & \end{pmatrix}$, $n+k \times n+k$

  $\widehat{\mathcal{A}}_j = \begin{pmatrix} A_1^{(j)} & \cdots & A_k^{(j)} \end{pmatrix}$: jth columns of $A_1, \ldots, A_k$ $(j \leq n)$

  Another "slicing" of the 3-tensor $\mathcal{A}$: $(\widehat{\mathcal{A}}_j)_{i\ell} = (A_\ell)_{ij}$

- $L_{n+1} = \begin{pmatrix} I_{n\times n} & \\ & 0 \end{pmatrix}$, $L'_{n+1} = \begin{pmatrix} I_{n\times n} & \\ & 0_{k\times k} \end{pmatrix}$

Hardness of injectivity (2)

- Hom(V, V'): $n + k \times n + 1$-matrices $C = \begin{pmatrix} B & \\ & \underline{\alpha} \end{pmatrix}$

  $B \in M_n(F)$, $\underline{\alpha} = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_k \end{pmatrix} \in F^n$ s.t.:

  $$CL_j = L'_j C \ (j = 1, \ldots, n)$$
  $$\Updownarrow$$
  $$B = A_{\underline{\alpha}}, \text{ where } A_{\underline{\alpha}} = \alpha_1 A_1 + \ldots + \alpha_k A_k$$

  Proof.

  $$\begin{aligned} CL_j &= \begin{pmatrix} & B^{(j)} \\ & \end{pmatrix} \\ L'_j C &= \begin{pmatrix} & \alpha_1 A_1^{(j)} + \ldots + \alpha_k A_k^{(j)}) \\ & \end{pmatrix} = \begin{pmatrix} & A_{\underline{\alpha}}^{(j)} \\ & \end{pmatrix} \end{aligned}$$

- Hom$(V, V') \ni C_{\underline{\alpha}} = \begin{pmatrix} A_{\underline{\alpha}} & \\ & \underline{\alpha} \end{pmatrix}$ injective $\Leftrightarrow$ $A_{\underline{\alpha}}$ nonsingular

Module isomorphism - the semisimple case

- $V \cong V'$ semisimple (the indecomposable components are simple)
- important property: every submodule is a direct summand
- Assume $\phi : \mathrm{Hom}(V, V')$ not invertible.
- Let $V_0 \leq \ker \phi$ simple, let $V = V_0 \oplus W_0$.
- Let $V' = V'_1 \oplus \cdots \oplus V'_t$, V'_i irreducible
- By Krull-Schmidt, $\exists\ i$ s.t. $V'_i \notin \mathrm{im}\,\phi$ and $V'_i \cong V_0$.
- $\psi_0 : V_0 \to V'_i$ isomorphism
- extend to $V \to V'_i \leq V'$: $\psi(v + w) := \psi_0(v)$ $(v \in V_0, w \in W)$
- $\psi \ker \phi = V_0 \notin \mathrm{im}\,\phi \qquad \Rightarrow$ length 1 Wong

Semisimple module algorithm - remarks

- Actually, finds max rank morphisms between semisimple module
- An application to decrease dimension of representation of simple algebras (Babai & Rónyai 1990, revised presentation):

  $\mathcal{B} \cong M_n(F)$, (unknown isomorphism)

  Every (unital) module is a direct sum of copies of F^n

  - V $\mathcal{B}$-module of dimension nr,
    $r' = \text{g.c.d}(n, r)$, $sr = tn + r'$, $U = \mathcal{B}$ by left mult.
    find injective $\phi \in \text{Hom}(U^t, V^s)$, $W = \text{im}\,\phi$
    V^s/W is a $\mathcal{B}$-module of dim. nr'.
  - Example: n prime, z *any* zero divisor in $\mathcal{B}$
    - $V = \mathcal{B}z$ left ideal as module of dimension nr
    - $r' = 1$, construct n-dimensional module
      $\longrightarrow$ isomorphism with $M_n(F)$.

Module isomorphism - the general case

- Reduction to finding minimum size sets of module generators ($\sim$ surjective morphisms from free modules)
  - $\mathcal{H} = \mathrm{Hom}(V, V)$ closed under multiplication: a matrix algebra
  - $\mathrm{Hom}(V, V')$ left $\mathcal{H}$-module
  - if $V' \cong V$: isomorphism $\leftrightarrow$ $\mathcal{H}$-mod. generator of $\mathrm{Hom}(V, V')$
- the "length 1" property of the semisimple case

  can be exploited to finding min. size sets of generators

  (I, Karpinski & Saxena (2010))
  - Surjectivity from free modules
  - Remark: "free" can be weakened to "projective"

Hidden rank one generators

- I, Karpinski, Qiao, Santha & Saxena (2014)
- $\mathcal{A} = \langle A_0, A_1, \ldots, A_k \rangle$ rk $A_i = 1$, but A_i unknown $(i = 1, \ldots, k)$
- Assume $A_0 = \begin{pmatrix} I_r & \\ & \end{pmatrix}$,
- ℓ: smallest s.t. $\mathcal{A}^\ell \ker A_0 \not\subseteq \operatorname{im} A_0$
- $\exists\ i_1, \ldots, i_\ell$: $A_{i_\ell} \ldots A_{i_1} \ker A_0 \not\subseteq \operatorname{im} A_0$
- $\mathcal{A}^{\ell-s} A_{i_j} \mathcal{A}^{s-1} \ker A_0 \in \operatorname{im} A_0$ when $s \neq j$
  - For $s < j$: $A_{i_j} \mathcal{A}^{s-1} \ker A_0 = (0)$,
    (otherwise $\mathcal{A}^{\ell-j-s} \ker A_0 \supseteq A_{i\ell} \ldots A_{i_j} \mathcal{A}^{s-1} \ker A_0 = \operatorname{im} A_{i\ell} \not\subseteq \operatorname{im} A_0$)
  - For $j > s$: $\mathcal{A}^{\ell-s} \operatorname{im} A_j \subseteq \operatorname{im} A_0$,   similarly
- $\mathcal{A}_j$: space of solutions for

$$\mathcal{A}^{\ell-s} X \mathcal{A}^{s-1} \ker A_0 \in \operatorname{im} A_0 \quad (s \in \{1, \ldots, \ell\} \setminus \{j\})$$

system of lin eq.

Hidden rank one generators (2)

- Compute bases for $\mathcal{A}_1, \ldots, \mathcal{A}_\ell$
- $\mathcal{A}_\ell \cdots \mathcal{A}_1 \ker A_0 \supseteq A_\ell \cdots A_1 \ker A_0 \not\subseteq \operatorname{im} A_0$
- key property: $\mathcal{A}_{i_\ell} \ldots \mathcal{A}_{i_1} \subseteq \operatorname{im} A_0$ if $i_j \neq j$ for some j
- Find $B_i \in \mathcal{A}_i$: $B_\ell \cdots B_1 \ker A_0 \not\subseteq \operatorname{im} A_0$
  - Pick a basis element B_1 for $\mathcal{A}_1$ s.t. $\mathcal{A}_\ell \cdots \mathcal{A}_2 B_1 \ker A_0 \not\subseteq \operatorname{im} A_0$;
  - Then B_2 from basis for $\mathcal{A}_2$ s.t. $\mathcal{A}_\ell \cdots \mathcal{A}_3 B_2 B_1 \ker A_0 \not\subseteq \operatorname{im} A_0$; etc. ...
- $(B_1 + \ldots + B_\ell)^\ell \ker A_0 = B_\ell \ldots B_1 \ker A_0$ modulo $\operatorname{im} A_0$
- Find λ: $\lambda A_0 + B_1 + \ldots B_\ell$ has rank $\operatorname{rk} A_0$.
- rationality issues:
  - rank one generators do not need to be rational
    example: field extension
  - known rank one generators: over F, even if small

Length 1 - application

- already know: A_i diagonal $(i = 0, \dots, k) \Rightarrow$ length one Wong
- Application: simplicity of finite extensions of $\mathbb{Q}$:
  - L: field extension of $F = \mathbb{Q}$, $|L : F| = n$
  - $a \in L$: $F[a] =$ subring (=subfield) generated by F and a
  - Task: find a s.t. $L = F[a]$
- Matrix representation of L

  $a \mapsto M_a =$ matrix of $x \mapsto ax$ on L $(n \times n)$
  identify a with M_a;
- Facts:
  - M_a are simultaneously diagonalizable over $\mathbb{C}$
  - $|F[a] : F| = \#$distinct eigenvalues of a

Lenght one: application (2)

- $a \mapsto \mathrm{Ad}_{M_a} =$ matrix of $X \mapsto M_a X - X M_a$
- $\mathcal{A} := \{\mathrm{Ad}_{M_a} : a \in L\}$ n-dim subspace of $M_{n^2}(F)$
- $\Delta = \begin{pmatrix} \delta_1 & & \\ & \ddots & \\ & & \delta_n \end{pmatrix} \Rightarrow \mathrm{Ad}_\Delta$ diagonal in M_{n^2}:
  - $\mathrm{Ad}_\Delta E_{ij} = \Delta E_{ij} - E_{ij}\Delta = (\delta_i - \delta_j) E_{ij}$
  - max. rank is $n^2 - n$
    when $\delta_i \neq \delta_j$ for $i \neq j$
- generalizes to direct sums of field extensions (over perfect base fields)