Trading Determinism for Noncommutativity in SINGULARITY Testing

(Joint work with V. Arvind and Abhranil Chatterjee)
(FOCS 2024)

Edmonds' Problem (1967)

$X = \{x_1, \cdots, x_n\}$ $\mathbb{F}$: Field

$T = A_0 + A_1 x_1 + \cdots + A_n x_n$

$A_i \in M_s(\mathbb{F})$

Problem: Check if T is invertible over $\mathbb{F}(x_1, \cdots, x_n) \to$ SINGULAR

Motivation: Matching, Matroids (Lovász)

- — Randomized Polynomial-time (PIT)

Open Q: Deterministic Algorithm?

$\hookrightarrow$ Ckt Lower Bound (KI'04)

NSINGULAR PROBLEM

$X = \{x_1, \dots, x_n\} \longrightarrow$ Noncommuting variables

$$x_i x_j \neq x_j x_i$$

- Rank in Free Skew Field $\longrightarrow \mathbb{F}(\!\langle x_1, \dots, x_n \rangle\!)$

$$\begin{array}{c} \mathbb{F}(\!\langle x_1, \dots, x_n \rangle\!) \\ \uparrow \\ \mathbb{F}\langle x_1, \dots, x_n \rangle \end{array}$$

[Cohn, Amitsur]

C- Rank / NC- Rank

$$M = \begin{bmatrix} 0 & 1 & x_1 \\ -1 & 0 & x_2 \\ -x_1 & -x_2 & 0 \end{bmatrix} \xRightarrow{\text{y.E}} \begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & x_2x_1 - x_1x_2 \end{bmatrix}$$

$\Rightarrow$ C- Rank $= 2$, NC- Rank $= 3$

Known Theorem

Thm [GGOW'16, IQS'18, HH'21]:

$$\text{NSINGULAR} \in P$$

- No direct connection with standard PIT

Key Concepts

- Inner Rank:

$$\text{nc-rank}(T) = \min r \text{ s.t.}$$
$$T = [P]_{s\times r}[Q]_{r\times s}$$

- Blow-up spaces

$$T = A_0 + \sum_{i=1}^{n} A_i x_i$$

$$\underline{p} = (p_1, \dots, p_n) \in M_d(\mathbb{F})^n$$

$$T(\underline{p}) = A_0 \otimes I_d + \sum_{i=1}^{n} A_i \otimes p_i$$

Blow up space: $T^{\{d\}} = \left\{ T(\underline{p}) : \underline{p} \in M_d(\mathbb{F})^n \right\}$

Key Fact (DM, IQS)

[Regularity Lemma]: The maximum rank in $T^{\{d\}}$ is a multiple of d.

Def^n: $$\text{nc-rank}(T) = \lim_{d\to\infty} \frac{\text{rank}(T^{\{d\}})}{d}$$

$= \text{Inner Rank}$

<u>Concept of Witness</u>:

$\underline{p} = (p_1, \ldots, p_n) \in M_d^n(\mathbb{F})$ is witness of $\text{ncrank}(T) \geq r$ if $\text{rank}(T(\underline{p})) \geq rd$.

Key Idea: Find better and better witness.

[Sketch] : NSINGULAR $\in$ P

Input: $T = A_0 + \sum_{i=1}^{n} A_i x_i$

Output: ncrank(T)

→ Suppose already have witness $\underline{p}$ of rank $= r$ in d-dimension.

1. Is r the maximum rank?
   If "YES" → NCRANK$(T) = r$ [STOP]

2. Otherwise: Use a "rank increment" step to produce witness of rank $> r$

3. [Rounding]: Another witness of rank $\geq r+1$

4. [Blow-up Control]: Keep the dimension small

IQS: Finite dimensional division algebra

A new PIT insight

(nc)-PIT-based "rank increment"

- Let $(p_1, \dots, p_n)$ be a rank witness ρ of dimension $= d$

Shift

$z_1, \dots, z_n$: generic matrices

$$T_d(z_1 + p_1, \dots, z_n + p_n)$$

$$\to U \left[\begin{array}{c|c} I_{rd} - L & 0 \\ \hline 0 & C - B(I_{rd} - L)^{-1} A \end{array}\right] V$$

- Key (simple) Observation

rank can be increased

$$\iff C - B(I_{rd} - L)^{-1} A \not\equiv 0$$

$$\iff C - B\Big(\sum_{k \le rd} L^k\Big) A \not\equiv 0$$

[Schützenberger]

nc-ABP PIT $\in$ P
[Raz-Shpilka '05]

Trade-off Result

$$X = X_1 \sqcup X_2 \sqcup \cdots \sqcup X_k$$

X_i : Noncommuting

$i \neq j$: $[X_i, X_j] = 0$

Main Question:

- Given a linear matrix T over X compute the rank of T

$$\mathbb{F}\langle X_1 \sqcup X_2 \sqcup \cdots \sqcup X_k \rangle \hookrightarrow \mathcal{U}_{[k]}$$

[KVV'20]

generalization of rational function field and Skew field

Main Theorem

A polynomial-time algorithm for the [PC]-SING problem for $k = O(1)$, $\mathbb{F} = \mathbb{Q}$.

- [En-route] (Key algebraic question)

Let T_1, T_2 are Linear matrices defined over

$X = X_1 \sqcup X_2 \sqcup \cdots \sqcup X_k$, $k = O(1)$.

u_1, v_1, u_2, v_2 : vectors

Check : $\vec{u}_1 \left(\sum_{i \geq 0} T_1^i \right) v_1 \stackrel{?}{=} \vec{u}_2 \left(\sum_{i \geq 0} T_2^i \right) v_2$

A central problem in algebraic automata theory

Solution : In deterministic polynomial-time.

Example: $X_1 = \{x_1, x_2\}$ $X_2 = \{x_1', x_2'\}$

$\Rightarrow x_1 x_2' x_2 x_1' \sim x_1 x_2 x_2' x_1'$

History:

- Rabin & Scott — 1959
- Griffiths — 1968
- Bird — 1973
- Valiant — 1974
- Friedman – Greibach – 1982
- Harju – Karhumäki – 1991
- Worrell – 2013 ⟵ Randomized poly-time.

A Finite Truncation: [Worrell, Schützenberger]

$\Downarrow$

An ABP identity testing problem over X

algebraic branching program.

Glimpse of the Proof Idea

Main Point: The new NSINGULAR algorithm can be lifted in this setting (modulo a lot of work!)

PIT · connection

Two Recursive Subroutines

PC-PIT[k]

Finds nonzero for a PC-ABP

PC-RANK[k]

Find rank witness Matrices

Sketch

$$x_1 \longrightarrow M_1 \otimes I_{d_2} \otimes I_{d_3} \otimes \cdots \otimes I_{d_k}$$

$$x_2 \longrightarrow I_{d_1} \otimes M_2 \otimes I_{d_3} \otimes \cdots \otimes I_{d_k}$$

$$\vdots$$

$$x_k \longrightarrow I_{d_1} \otimes I_{d_2} \otimes \cdots \cdots \otimes M_k$$

Partially commutative structure

$$\left.\begin{array}{c} \text{PC-RANK}(k) \\ \Downarrow \\ \text{PC-PIT}(k) \\ \Downarrow \\ \text{PC-RANK}(k-1) \end{array}\right\} \text{very high level}$$

Some Remarks

- Runtime $\to$ $s^{2^{O(k\log k)}}$ ← s: size of the matrix

- (Worrel) : Randomized: $s^{O(k)}$

- For non constant k: No known progress
  (For series equivalent problem)

- Find new Invariant theory connection
  [Makam, Wigderson '20]

- Develop Black-box algorithms.

Thank You!