Noncommutative Real Algebraic Geometry and Its Friends

NC Real Algebraic Geometry

Jaka Cimpric, Igor Klep   Ljubjiana U
Eric Evert   UC San Diego
Scott McCullough, James Pascoe   University of Florida
Victor Vinnikov   Ben Gurion U of the Negev
Jurij Volčič   Texas A&M

Perfect Quantum 3 XOR games

Vern Paulsen   Waterloo
Adam Bene Watts   MIT → Waterloo

Their collaborator Bill Helton   UC San Diego

American Institute of Mathematics
June 2021

Advertisement: Try noncommutative computation

NCAlgebra   **NCSoSTools**
Helton, de Oliveira (UCSD)   Igor Klep

AIM: Noncommutative Inequalities (talk by Bill)

Huge math results of the last decade have been in these areas:

Quantum Games $MIP^* = RE$ J, N, V, W, Y 2020
The Connes Embedding Conjecture is false.

Here: Anand Natarajan, Vern Paulsen, William Sloftsra;Mon, Anna Verschynana, Adam Bene Watts

Random Matrix Theory Kadison-Singer is True M, S, S. 2015
Here: N. Srivastava; Weds, J.G. Vargas

Invariant theory- CS: G, G, O, W 2015
Given a NC rational expression, is it identically 0? This can be determined in polynomial time.

Here: Harm Derksen, Visu Makam; Tues, Raphael Oliveira

These remarkable results had strong intersection with the rapidly developing area of

Non Commutative RAG and NC Analytic Maps

Here: Meric Augat, Eric Evert, Kate Juschenko, Igor Klep, Scott McCullough, Tim Netzer, James Pascoe Tues, Eli Shamovich, Tea Strekelj, Jurij Volčič; Tues, Victor Vinnikov

Ingredients of Talk: NC polynomials

$x = (x_1, \cdots, x_g)$ $x^* = (x_1^*, \cdots, x_g^*)$ noncommuting variables

Noncommutative polynomials: $p(x)$:

$$Eg. \qquad p(x) = x_1^* x_2 + x_2^* x_1$$

An **analytic polynomial** contains no x_j^*.

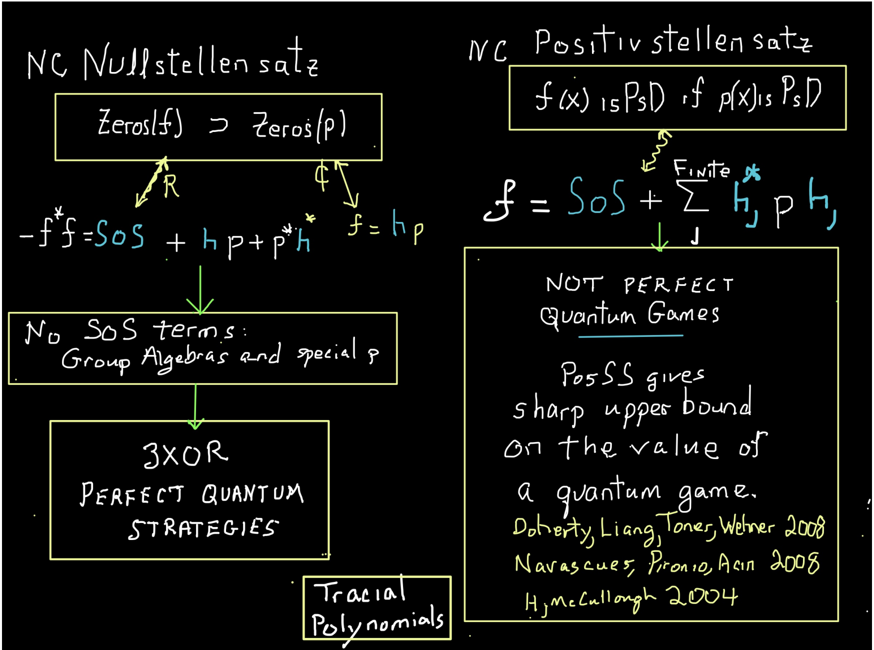
Evaluate p: on matrices $X = (X_1, \cdots, X_g)$ a tuple of matrices.

Substitute matrices for variables

$x_1 \mapsto X_1$, $x_2 \mapsto X_2$ $x_1^* \mapsto X_1^*$, $x_2^* \mapsto X_2^*$

$$Eg. \qquad p(X) = X_1^* X_2 + X_2^* X_1.$$

Outline of Free (Real) Algebraic Geometry



NC (FREE) ALGEBRAIC GEOMETRY

(Algebra formulas equivalent to polynomial equalities)

Let $p \in \mathbb{C}{<}\mathbf{x}, \mathbf{x}^*{>}$ - polys in nc variables.
THREE TYPES OF ZEROES of p.

1. **'Hard Zeros'** $p(X) = 0$ **for** $X = (X_1, \dots, X_g) \in (\mathbb{C}^{n\times n})^g$
   Eg. $p(x) = x_1^2 + x_2^2 - 1$ $\quad Z_{hard}(p) = \{X | \ X_1^2 + X_2^2 = I\}$
   . $Z_{hard}(p) := \bigcup_n \{X \in (\mathbb{C}^{n\times n})^g \mid \quad p(X) = 0\}$
2. **Directional Zeros**
   $Z_{dir}(p) := \bigcup_n \{(X, \psi) \in (\mathbb{C}^{n\times n})^g \times \mathbb{C}^n | \ \ p(X)\psi = 0\}$
3. **Determinantal Zeros**
   $Z_{det}(p) = \bigcup_n \{X \in (\mathbb{C}^{n\times n})^g | \ \ \det p(X) = 0\}$

GENERALITY $p = \{p_1, \cdots, p_k\}$
p_i **can be a matrix with nc poly entries**

NULLSTELLENSATZ Algebra "certificate"
$= \ Zeros(f) \supset Zeros(p)$.
"well understood" for analytic poly p
Hard Zeros: Amitsur 1957, Bresar-Klep 2011, Shamovich etal
Directional Zeros : Bergman, H-McCullough-Putinar 2007
Determinantal Zeros : H-Klep-Volcic, 2019

Directional Zeros NullSS

. $p(x)$ **analytic means: no** x_j^* **appear in** p:

. **Quiz: Is** $p(x) = x_1^4 + 3x_2^*$ **analytic?**

THM Directional Nullstellensatz (Bergman, H-McCullough-Putinar, 2007):

Suppose $p(x)$ **is nc analytic poly and** $f(x)$ **an nc poly. Then**

$$Z_{dir}(f) \supset Z_{dir}(p) \iff f \in \mathcal{LI}(p) \ \ \textit{the left ideal gen by } p$$

$$f(X)\psi = 0 \quad \textit{if} \ \ p(X)\psi = 0 \iff f = \mathbb{C}{<}\mathbf{x}, \mathbf{x}^*{>}\, p$$

Quiz: Compare to Hilbert NullSS on $\mathbb{C}^g$**. Hilbert's certificate is**

$$f^k = hp \ \ \textit{for some } k, \textit{some } h$$

Is this the "same form" as ours?

COR $\quad Z_{dir}(p) = \ \textit{empty} \iff 1 \in \mathbb{C}{<}\mathbf{x}, \mathbf{x}^*{>}\ p$

Ex: XOR 2-players, 2-variables

The basic issue is: **We are given a list of algebraic equations. Does a solution exist? Find a solution.**

Def: A selfadjoint and unitary operator M is called a signature operator, $M^2 = 1$**.**

QUANTUM XOR : **Do there exist signature matrices A_0, A_1 and B_0, B_1 and a vector $\psi \neq 0$, with all A_i commuting with all B_j which solve the equations (left sides called clauses):**

$$A_0 B_0 \psi = \psi \qquad A_1 B_0 \psi = \psi$$

$$A_0 B_1 \psi = \psi \qquad -A_1 B_1 \psi = \psi.$$

To use NullSS set $p := \{A_0 B_0 - 1, \ldots, A_j^2 - 1, \ldots\}$**.**
$\exists\ p(A,B)\psi = 0$ **IFF** $Z_{dir}(p) \neq$ **empty** **IFF** $I \notin \mathcal{LI}(p)$
CAN NOT USE NullSS, since $A_J = A_J^*$ **ETC. The polynomials 'p' are NOT analytic. They contain *.**

NONCOMMUTATIVE REAL ALGEBRAIC GEOMETRY

(Needed for self adjoint variables)

Classical RAG: compare zeros in $\mathbb{R}^g$ of polynomials f and p.
Hilbert 17^{th} 1890's Tarski-Seidenberg 1920s Dubois, Risler 1970ish

NC REAL DIRECTIONAL NULLSTELLENSATZ

Let $\mathcal{A}$ be a pre C^* algebra (eg. a group C^* algebra) containing I.

Exanple: $\mathcal{A} := \mathbb{C}<\mathbf{x}, \mathbf{x}^*>$ **- polys in g nc variables.**

Def: NC Directional Real Zeroes

Fix $X \in B(H)^g$ selfadjt.

Then $\pi(p) := p(X)$ is a C^*-algebra representation of $\mathcal{A}$ into $B(H)$.

General def.

$$Z^{re}_{dir}(p) := \{(\pi, \psi) \mid \ \pi(p)\psi = 0 \quad \textit{some } C^* \textit{ representation } \pi : \mathcal{A} \to B(H), \ \ \psi \in H, \ \textit{all } H\}$$

Let $\mathcal{I}$ (resp. $\mathcal{LI}$) denote a two sided ideal (resp. left ideal) in $\mathcal{A}$.

$$Z^{re}_{dir}(\mathcal{LI}(p)) = Z^{re}_{dir}(p) \qquad\qquad Z^{re}_{hard}(\mathcal{I}(p)) = Z^{re}_{hard}(p)$$

NC Real NulSS

THM - Dir Zeroes: $Z^{re}_{dir}(\mathcal{LI})$ **[Cimpric,H, McCul, Nelson 2013]**
$Z^{re}_{dir}(f) \supset Z^{re}_{dir}(\mathcal{LI})$ **IFF**

$$-f^*f \in closure[SOS_{\mathcal{A}} + \mathcal{LI} + \mathcal{LI}^*] \tag{1}$$

Special case $f = 1$. For $\mathcal{A}$ associated to a quantum game:
$Z^{re}_{dir}(\mathcal{LI})$ **is empty IFF**

$$-1 \in SOS_{\mathcal{A}} + \mathcal{LI} + \mathcal{LI}^* \tag{2}$$

Ex: Applies to any game to tell if is perfect (quantum solvable).

THM - Hard Zeroes: $Z^{re}_{hard}(\mathcal{I})$ **For $\mathcal{A} \sim$ to a quantum game:**
Suppose $\mathcal{I}$ is a *-closed 2 sided ideal.

$$Z^{re}_{hard}(\mathcal{I}) \text{ is empty} \quad \mathit{IFF} \quad -1 \in SOS_{\mathcal{A}} + \mathcal{I}.$$

Ex: Applies to all synchronous games– Vern Paulsen etal

NC Real NulSS with no SOS

Special with **no SOS** **(Groups, groups, groups)**
Cleve Liu Slofstra Mon -Two sided ideals

THM[Watts-Harrow-Kanwar-Natarajan 2018, Watts-H-Klep]
$\mathcal{G} :=$ **cntable group.** $\mathcal{A} = \mathbb{C}[Z_2 \times \mathcal{G}] :=$ **group algebra.**
$Z_2 := \{-1, 1\}$
$\mathcal{C} :=$ **elements of** $Z_2 \times \mathcal{G}$ **(** **think** $c_i \in \mathcal{C}$ **has form** $c_i = \pm g_i$ **for** $g_i \in \mathcal{G}$**).**

Let $\mathcal{LI}(\mathcal{C} - 1)$ **be the left ideal generated by** $\{c - 1 \mid c \in \mathcal{C}\}$**.**
Then the following are equivalent:

1. $Z^{re}_{dir}(\mathcal{C} - 1)$ **is empty.**
2. $1 \in \mathcal{LI}(\mathcal{C} - 1) + \mathcal{LI}(\mathcal{C} - 1)^*$
3. $1 \in \mathcal{LI}(\mathcal{C} - 1)$
4. $-1 \in \langle \mathcal{C} \rangle :=$ **the group generated by** $\mathcal{C}$

Example: 2XOR game revisited; CHSH

Do there exist signature matrices A_0, A_1 and B_0, B_1 and vector $\psi \neq 0$ with all A_i commuting with all B_j which solve the equations.

$$A_0 B_0 \psi = \psi \qquad A_1 B_0 \psi = \psi$$
$$A_0 B_1 \psi = \psi \qquad -A_1 B_1 \psi = \psi.$$

These equations have no matrix or operator soln (Bell 1960's)

Real NC NullSS applies directly.

$$\mathcal{A} := \mathbb{C} < x, x^* > /\mathcal{I} \ \mathit{where}\ \mathcal{I} := \mathit{ideal}\{A_i^2 - 1, \ldots A_i B_j - B_j A_i = 0\}$$

The issue is $1 \in \mathcal{LI}_{\mathcal{A}}(\mathcal{C} - 1)$?

$$\mathcal{C} := \{a_0 b_0,\ a_1 b_0,\ a_0 b_1,\ -a_1 b_1\}$$

This is easy to test, say, using a noncommutative (left) Groebner Basis type algorithm.
Advertisement: Use NCAlgebra

Not solvable (not perfect) games.

A measure b of how close to solvable a game Γ is: the average of its (signed) clauses. Eg for CHSH

$$b(A, B) := \frac{1}{4}(+A_0B_0 + A_1B_0 + A_0B_1 - A_1B_1)$$

Then the quantum value of the game Γ is

$$Val(\Gamma) := \max_{A,B,|u|=1} u^* b(A, B)u$$

1. $Val(\Gamma) = 1 \iff$ **the eqs have a solution (perfect),, since for all words $\|A_iB_j\| \leq 1$ and b averages them.**

2. Games with (robustly) unique solutions are important, called self testing games. Key in Connes Counter example.

CLASSICAL: **Find a 1 dim soln. Same as**

$$A_i = \pm 1, \quad B_j = \pm 1 \quad \psi = 1.$$

This example is a classic: the CHSH game

ANS: (CHSH) (Bell 1964)

1. $Val(CHSH) = \frac{\sqrt{2}}{2}$ **and soln matrices are** 4×4
2. **ClassicalVal(CHSH)** $= \frac{1}{2}$

Quantum Advantage $:= \frac{Val(CHSH)}{ClassicalVal(CHSH)} = \sqrt{2}$

Historically super important: An experiment violated the Bell inequality thus validating quantum entanglement.

Outline of talk

NC (Free) Algebraic Geometry

NC Nullstellensatze

NC Real Nullstellensatze

A certificate without SOSs

XOR games

2 Player XOR games

3 Player XOR Games

NC RAG Positivstellensatz: Convexity

NC Convexity and LMIs

Enginering Motivation

NC (Free) Extreme Points

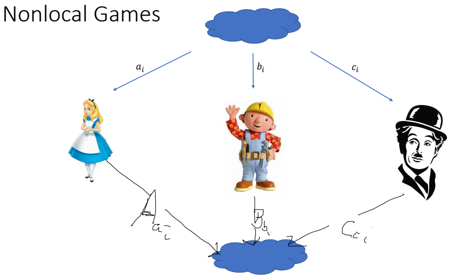
NC Positivstellensatz

. 3 XOR GAMES

Advertisement: XOR games package for quantum games
Needs Mathematica

Igor Klep, Zehong Zhao, Zinan Hu, Bill Helton
Mauricio de Oliveira

write Bill at
helton at ucsd dot edu



3XOR Setting

Group $\mathcal{G}$ with generators::
Selfadjoint $A_i, B_j, C_k \quad i, j, k = 1, \ldots, m$ **and** σ
and defining relations:

$$A_i^2 = B_j^2 = C_k^2 = I$$

Players commute eg. $\quad A_i B_j A_i^{-1} B_j^{-1} = I$

$\sigma^2 = 1$ **and** σ **commutes everything** *think* $\sigma = \pm 1$

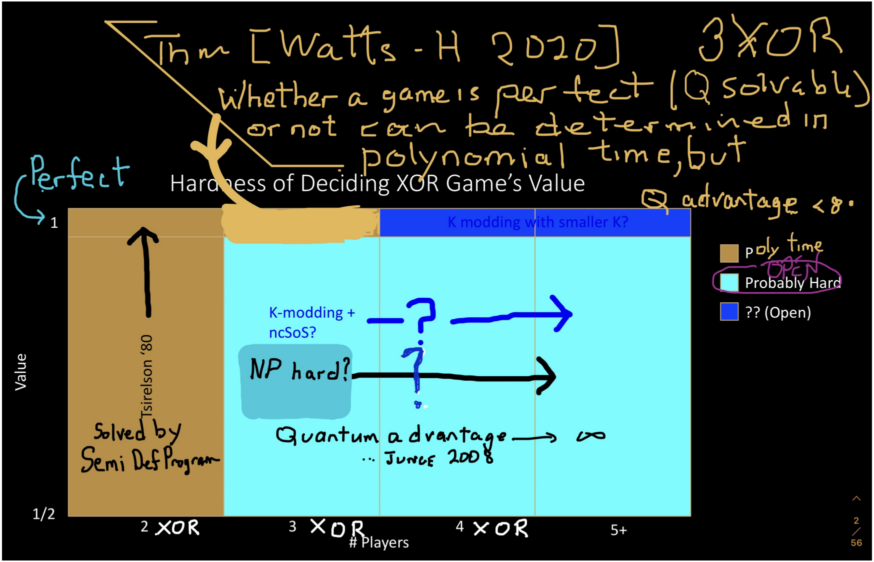
A particular game is defined by a set $\mathcal{C}$ of signed words (called clauses)

$$c_1 := \sigma^{t_1} A_{a_1} B_{b_1} C_{c_1}, \quad \ldots, \quad c_e := \sigma^{t_e} A_{a_e} B_{b_e} C_{c_e}?$$

The point is we are given words with signs. Can we solve the corresponding matrix (or operator) equations:

$$(-1)^{t_1} A_{a_1} B_{b_1} C_{c_1} \psi = \psi, \quad \ldots \quad (-1)^{t_e} A_{a_e} B_{b_e} C_{c_e} \psi = \psi$$

3XOR perfection in polynomial time



Proof: Tricky long algebraic

HISTORICAL LANDMARKS FOR XOR games

1. **Bell 1964 CHSH game, by another name**
2. **Two player XOR games are 'completely' understood by Tsierlson 1987:**
   - 2.1 **Finding value of a 2 player game can be done by solving a Linear Matrix Inequality, (Its an SDP)**
   - 2.2 **Quantum advantage $\leq$ real Grothendieck constant ≤ 2**
   - 2.3 **Whether or not a game is solvable (aka. perfect) can be decided in polynomial time.(do not need SDP)**
   - 2.4 **This study originated the famous Tsierlson Conjecture, later proved equivalent to Connes Embedding Conjecture.**

1. **Three player not perfect games, 3 XOR**

   1.1 **Determining the optimal value of a not perfect 3 player game is "thought" to be NP hard to approximate. Vidick 2013. But is OPEN.**

   1.2 **The quantum advantage can go to ∞ as the number of variables m and dimension of the matrices A_i, B_j, C_ℓ go to ∞. Briet and Vidick 2012, Pérez-Garcia ... Junge 2008 respectively.**

Perfect 3 player XOR games.

THM [Watts + H; arXiv 2020]

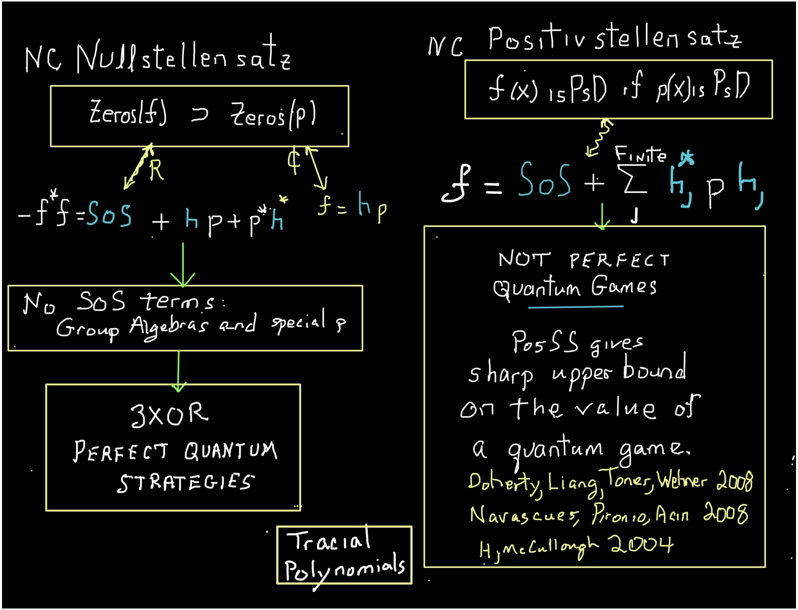
1. **Given any 3XOR game, whether or not a (perfect) quantum solution exists can be decided in polynomial time. (Previously this problem was not known to be decidable.)**

2. **If there is a solution, then there is a "fairly explicit" solution with A_i, B_j, C_ℓ which are 8×8 matrices.**

3. **The quantum advantage of a perfect quantum solution is ≤ 8**

Proof: Tricky (long) calculation on top of previous NullSS.

Our path


NC Nullstellensatz
Zeros(f) ⊃ Zeros(p)
R
⊄
$-f^*f = SoS + hp + p^*h$
$f = hp$
No SoS terms:
Group Algebras and special p
3XOR
PERFECT QUANTUM
STRATEGIES
Tracial
Polynomials
NC Positivstellensatz
f(x) is PsD if p(x) is PsD
Finite
$f = SoS + \sum_j h_j^* p h_j$
NOT PERFECT
Quantum Games
PosSS gives
sharp upper bound
on the value of
a quantum game.
Doherty, Liang, Toner, Wehner 2008
Navascues, Pironio, Acin 2008
H, McCullough 2004

NC RAG and Convexity

NC Linear Matrix Inequalities

NC LINEAR MATRIX INEQUALITIES LMIs
GIVEN a monic symmetric linear pencil

$$L(x) := I + L_1 x_1 + \cdots + L_g x_g$$

Recall evaluation on $X = (X_1, \ldots, X)$

$$L(X) := I + L_1 \otimes X_1 + \cdots + L_g \otimes X_g$$

Example

$$\begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix} \otimes X = \begin{pmatrix} 1X & 2X \\ 3X & 5X \end{pmatrix}$$

CONVEX SETS: have LMI representations

THM: [McCullough-H 2012, Kriel 2017]
SUPPOSE p **is an nc symmetric poly,** $p(0) \succ 0$ **and** $\mathcal{D}_p$ **bounded.**

THEN
$\mathcal{D}_p^n := compt_0 \{X \in (R^{n\times n})^g : \ p(X) \succ 0\}$ **is a convex set for each** n

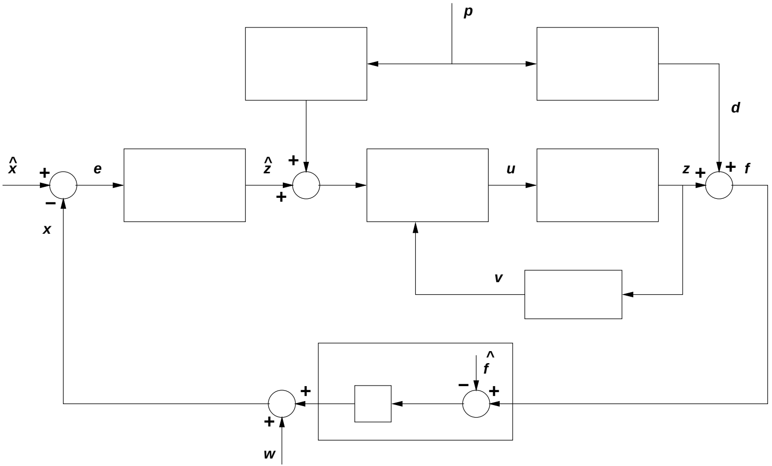
IFF

$\mathcal{D}_p$ **is a free spectrahedron, that is, there is a monic symmetric linear pencil** $L(x)$ **which "represents"** $\mathcal{D}_p$ **as**

$$\mathcal{D}_p = \mathcal{D}_L.$$

A "free convex set" $\mathcal{D}$ **has an operator coefficient LMI rep. [Effros - Winkler** $\sim$ **1999].**

A Motivation: Linear Systems give fancy nc polynomials



Convexity is very important.

Linear Systems and Algebra Synopsis

A Signal Flow Diagram with L^2 based performance, eg H^∞ gives precisely a nc polynomial

$$p(a,x) := \begin{pmatrix} p_{11}(a,x) & \cdots & p_{1k}(a,x) \\ \vdots & \ddots & \vdots \\ p_{k1}(a,x) & \cdots & p_{kk}(a,x) \end{pmatrix}$$

Such linear systems problems become exactly:

Given matrices A.
Find matrices X so that $p(A,X)$ is PosSemiDef.

The (SAD FOR ENGINEERING) MORAL OF THE STORY

THM Hay-H-Lim-McC 2008 A CONVEX in X. problem specified entirely by signal flow diagrams and L^2 performance has

$$p \text{ with degree} \leq 2 \text{ in } x.$$

Hybrid free/classical problems

1. Γ **convexity** $p(a, x)$ **is much more general than just convexity in** x **convexity but has many good properties.**
Jury, Klep, Mancuso, McC, Pascoe Tues, arXIv 2019

2. Maximize a linear functional ℓ **over** $\mathcal{C}(n)$**, level** n **of free convex set** $\mathcal{C} := \{X | \ p(X) \succ 0\}$**.**

$$X^\ell := Maximizer_{X \in \mathcal{C}(n)} \quad \ell(X)$$

What are the properties of the optimizer X^ℓ**?**
Not a free problem because n **is fixed.**

Open Question **Does the 'free part of the structure' of this problem influence the outcome?**

Max of ℓ occurs on extreme point BUT there are 3 natural kinds of extreme points

$$\textit{ordinary extreme} \supset \textit{matrix extreme} \supset \textit{free extreme}$$

Experimental Finding **Evert** **Fu, H, Yin 2020** **Yes**
Maximizer is:

1. **(provably an ordinary extreme pt with prob $= 1$)**
2. **for $g \le d$ a free extreme point with super high probability**

FREE RAG: Ex. Convex Positivstellensatz

THM Convex PosSS (H-K-McCullough Advances 2013)
SUPPOSE q is a nc sym polynomial and L is monic linear pencil with $\mathcal{D}_L$ bounded. THEN

$$q(X) \succeq 0 \qquad \textit{if} \quad L(X) \succeq 0$$

for X being tuples of matrices if and only if

$$q(x) = \sum_{j=1}^{\kappa} W_j(x)^* L(x) W_j(x),$$

where H is a finite dim space and W_j are matrix nc polynomials on $\mathcal{D}_L$ with $degW_j = \lfloor \frac{deg\ \ q}{2} \rfloor$.

Convex posSS for q degree 1 $\sim \Longleftrightarrow \sim$ Steinspring-Arveson -Kraus CP (fin dim) map theory

THM True for q rational (Pascoe, arXiv 2017, Volcic).

FREE RAG: Ex. A General Positivstellensatz

THM General PosSS (H-McCullough 2004)
SUPPOSE q **is a nc sym polynomial and** $\{X| \ p(X) \succeq 0\}$ **is bounded. THEN**

$$q(X) \succeq 0 \qquad if \quad p(X) \succeq 0$$

for X **being tuples of operators if and only if for** $\epsilon \geq 0$

$$q(x) + \epsilon = SOS^{\epsilon} + \sum_{j=1}^{\kappa} W_j^{\epsilon}(x)^* p(x) W_j^{\epsilon}(x),$$

W_j^{ϵ} **are matrices of nc polynomials.**

NCSOS Tools Matlab package by Igor Klep et al

NPA Hierarchy

Recall Example CHSH game.
The quantum value of the game Γ is

$$Val(\Gamma) := \sup_{A,B,|u|=1} u^* b(A,B) u \qquad where$$

$$b(A,B) := (+A_0 B_0 + A_1 B_0 + A_0 B_1 - A_1 B_1)/4$$

That is $Val(\Gamma)I - b(A,B) \succeq 0$ **sharply. By free PosSS for** $\epsilon \downarrow 0$

$$Val(\Gamma) - b + \epsilon = SOS^{\epsilon} + \sum_{j=1}^{\kappa} W_j^{\epsilon^*} p W_j^{\epsilon},$$

where $p := \{\pm(A_j^2 - 1), \pm(B_j^2 - 1), \pm(A_j B_k - B_k A_j)\}$**.**

$$Val(\Gamma) - b + \epsilon = SOS^{\epsilon} + Ideal(p) \qquad this\ an\ '\infty'\ SDP$$

NPA 2008 Navascués-Pironio- Acín 2008 and
Doherty-Liangand -Toner- Wehner 2008

Tracial PosSS

THM Klep-Schweighoffer 2009
$Trace(q(X)) \geq 0$ **on** $\{X|\ p(X) \succeq 0\}$**, a 'bounded' set.**
where X **is in a vN algebra having a trace.**
IFF **For each** $\epsilon > 0$

$$q + \epsilon = SOS^{\epsilon} + \sum_{j=1}^{\kappa} W_j^{\epsilon^*} p W_j^{\epsilon} + \quad \Sigma_j^{\tilde{k}} commutator_j$$

Much recent progress by: Klep Macron Spenko Volcic, Tues
on mixtures of polys and traces like $f(x) = p_1 tr(q_1) + tr(q_2) p_2$

THM V. Paulsen, et. al. 2016 Every synchronous (2-player) game has value function of the from:

$$Val(\Gamma) := \max_{X \in \mathcal{D}_p} \ Trace\ b(X)$$

Synchronus game Γ Examples
The $MIP^* = RE$ **treats perfect synchronous games.**
Graph coloring games are synchronous.

NC RAG not mentioned in my talk, but well represented at AIM

1. **NC Analytic Functions Theory-Interpolation Shamovic, Vinnikov**
2. **Noncommutative Bianalytic maps**
   2.1 **Polynomial Maps (Jacobian Conjecture) – –Meric Augat**

   2.2 **Classify maps f of Free Convex sets: $f : C$ onto some $\tilde{C}$ – McCullough, Klep, Volcic, H**

   2.3 **Convex functions composed with analytic,
   a.k.a NC Plurisubharmonic
   — McCullough, Klep, Volcic, H; Pascoe**

**(Commutative) determinantal representations of polynomials
— H, Vinnikov, Srivastava**

THANKS FOR CHECKING OUT THIS TALK

AND

ENJOY AIM

Ideas in the proof of perfect 3XOR Thm

Reminder:
The 3XOR Group $\mathcal{G}$ is the group with selfadjoint generators

$$A_i, B_j, C_k \quad i, j, k = 1, \dots, m \quad and \quad \sigma$$

and defining relations:

$$A_i^2 = B_j^2 = C_k^2 = 1$$

Players commute eg. $A_i B_j A_i^{-1} B_j^{-1} = 1$

$\sigma^2 = 1$ **and σ commutes everything,** **think** $\sigma = -1$

All 3XOR games live in $\mathcal{G}$.

A particular game is defined by words (called clauses)

$$\mathcal{C} := \{c_1 := \sigma^{t_1} A_{a_1} B_{b_1} C_{c_1}, \quad \ldots, \quad c_e := \sigma^{t_e} A_{a_e} B_{b_e} C_{c_e}\}$$

The point is we are given words with signs.
The Clause subgroup $\langle \mathcal{C} \rangle$ of $\mathcal{G}$ is the subgroup generated by the clauses $\mathcal{C} := \{c_1, \ldots, c_e\}$.

Part I:
THM (Watts, Harrow, Kanwar, Natarajan; arXiv2018)
A k- XOR game has no solution IFF σ is in $\langle \mathcal{C} \rangle$.
Thus the key issue is the subgroup membership problem for the group $\mathcal{G}$.

Sadly, there exist subgroups BAD of $\mathcal{G}$ where determining if a word w is in BAD is undecidable.

Part II:

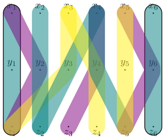
$\mathcal{G}^E :=$ **Even subgroup of $\mathcal{G}$**, is all even length words in $\mathcal{G}$.
$\langle\mathcal{C}\rangle^E :=$ **Even subgroup of $\langle\mathcal{C}\rangle$**, all even length words in $\langle\mathcal{C}\rangle$.

Define $\mathcal{K}$, to be the normal subgroup of $\mathcal{G}^E$ generated by the commutator subgroup of $\mathcal{G}^E$; its generators are

$$[A_iA_j, A_kA_\ell],\ [B_iB_j, B_kB_\ell],\ [C_iC_j, C_kC_\ell] \in \mathcal{K}$$

THM [Watts, H arXiv 2020]
A 3XOR game has no solution **IFF** σ is in $\langle\mathcal{C}\rangle^E$ *mod* $\mathcal{K}$.

PF: Hard:



The (multi) graph associated to the clauses.

COR This subgroup membership problem is decidable in polynomial time, since $G^E/\mathcal{K}$ is a commutative group (finitely generated). (Classical fact)

QED

MERP Solution to 3XOR

1. **Moreover, if a (perfect) quantum solution to a 3XOR game exists, then an 8 dimensional solution exists of the tensor form**
   $A_i := M_{a_i} \otimes I_2 \otimes I_2, \quad B_i := I_2 \otimes M_{b_i} \otimes I_2 \quad C_i := I_2 \otimes I_2 \otimes M_{c_i}$
   where each M_{*_i} **is a** 2×2 **signature matrix (a qubit) and the solution vector** ψ **is**

$$\psi = \frac{1}{\sqrt{2}}(1,0,0,0,0,0,0,1)^T$$

2. **(More detail) The matrices** M_{a_i} M_{b_j}, M_{c_ℓ} **have the form**

$$M_* = \exp(i\theta\sigma_z)\sigma_x \exp(-i\theta\sigma_z) \tag{3}$$

   for some $\theta's$ **which depend on** a_i, b_j, c_ℓ**. Here** σ_x, σ_z **are the Pauli** X **and** Z **matrices:** $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ **and**
   $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$,

PF of MERP comes from WHKN2018: if a solution exists mod K, then there is a MERP solution.

PF quantum advantage ≤ 8 was previously known for any solution based on a state ψ of the form

$$\psi = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad = \quad \frac{1}{\sqrt{2}}(1,0,0,0,0,0,0,1)$$

MERP solution satisfies this.

$\square$