Noncommutative Real Algebraic Geometry and Quantum Games

Perfect Quantum 3 XOR games
Adam Bene Watts   MIT → Waterloo

NC Real Algebraic Geometry
Jaka Cimpric   Ljubliana U
Igor Klep   Ljubliana U
Scott McCullough   University of Florida

Your narrator Bill Helton   UC San Diego

MATHEMATICAL PICTURE LANGUAGE SEMINAR
March 2021

Advertisement: Try noncommutative computation

NCAlgebra\textsuperscript{1}   NCSoSTools\textsuperscript{2}

\textsuperscript{1} Helton, de Oliveira (UCSD), Stankus (CalPoly SanLObispo), Miller
\textsuperscript{2} Igor Klep
Adam Bene Watts - 3 XOR

Adam Bene Watts
NC RAG guys: Jaka Cimpric, Igor Klep, Scott McCullough
Ingredients of Talk: NC polynomials

\[ x = (x_1, \cdots, x_g) \quad x^* = (x_1^*, \cdots, x_g^*) \quad \text{noncommuting variables} \]

Noncommutative polynomials: \( p(x) \):

\[ Eg. \quad p(x) = x_1^* x_2 + x_2^* x_1 \]

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

\[ x_1 \mapsto X_1, \quad x_2 \mapsto X_2 \quad x_1^* \mapsto X_1^*, \quad x_2^* \mapsto X_2^* \]

\[ Eg. \quad p(X) = X_1^* X_2 + X_2^* X_1. \]
Outline of talk

NC Nullstellensatz

\[ \text{Zeros}(f) \supset \text{Zeros}(p) \]

\(-f^* f = \text{SOS} + \sum h_j p h_j \)

No SOS terms: Group Algebras and special p

3XOR

PERFECT QUANTUM STRATEGIES

NC Positivstellensatz

\[ f(x) \text{ is PSD if } p(x) \text{ is PSD} \]

\[ f = \text{SOS} + \sum h_j p h_j \]

NOT PERFECT

Quantum Games

PosSS gives sharp upper bound on the value of a quantum game.

Doherty, Liang, Toner, Werner 2008
Navascués, Pironio, Acín 2008
Hj McCullough 2004

WE SKIP THIS
NC (FREE) ALGEBRAIC GEOMETRY
(Algebra formulas equivalent to polynomial equalities)
Let \( p \in \mathbb{C}\langle x, x^* \rangle \) - polys in nc variables.

**THREE TYPES OF ZEROES** of \( p \).

1. **Hard Zeros**
   \[ p(X) = 0 \text{ for } X = (X_1, \ldots, X_g) \in (\mathbb{C}^{n \times n})^g \]
   Eg. \( p(x) = x_1^2 + x_2^2 - 1 \)
   \[ Z_{\text{hard}}(p) = \{ X \mid X_1^2 + X_2^2 = 1 \} \]
   \[ Z_{\text{hard}}(p) := \bigcup_n \{ X \in (\mathbb{C}^{n \times n})^g \mid p(X) = 0 \} \]

2. **Directional Zeros**
   \[ Z_{\text{dir}}(p) := \bigcup_n \{ (X, \psi) \in (\mathbb{C}^{n \times n})^g \times \mathbb{C}^n \mid p(X)\psi = 0 \} \]

3. **Determinantal Zeros**
   \[ Z_{\text{det}}(p) = \bigcup_n \{ X \in (\mathbb{C}^{n \times n})^g \mid \det p(X) = 0 \} \]

**GENERALITY** \( p = \{ p_1, \ldots, p_k \} \)
\( p_i \) 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
Directional Zeros: - H-McCullough-Putinar Zeitsc 2007
Determinantal Zeros: H-Klep-Volcic, Advances 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, Zeits. 2007):
Suppose $p(x)$ is nc analytic poly and $f(x)$ an nc poly. Then

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

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

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

$$f^k = hp \text{ for some } k.$$

Is this the “same form” as ours?

**COR** $Z_{dir}(p) = \emptyset \iff 1 \in \mathbb{C}<x, x^*> p$
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):

\[
A_0 B_0 \psi = \psi \quad A_1 B_0 \psi = \psi \\
A_0 B_1 \psi = \psi \quad -A_1 B_1 \psi = \psi.
\]

To use NullSS set $p := \{A_0 B_0 - 1, \ldots, A^2_j - 1, \ldots\}$.

$\exists p(A, B)\psi = 0$ IFF $Z_{\text{dir}}(p) \neq \text{empty}$ IFF $I \notin L_I(p)$

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 17th 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 $I$.

Ex: $\mathcal{A} := \mathbb{C}<x, x^*>$ - polys in $g$ nc variables.
Fix $X \in B(H)^g$ selfadjt $\pi(p) := p(X)$ is a $C^*$-algebra rep of $\mathcal{A}$.

General def.

$$Z_{\text{dir}}^\text{re}(f) := \{ (\pi(f), \psi) | \pi(f)\psi = 0 \text{ some } C^* \text{ representation } \pi: \mathcal{A} \to B(H), \psi \in H \}$$

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

**THM - Dir Zeroes:** $Z_{\text{dir}}^\text{re}(LI)$ [Cimpric,H, McCullough, Nelson 2013]

$$Z_{\text{dir}}^\text{re}(f) \supseteq Z_{\text{dir}}^\text{re}(LI) \quad \text{IFF} \quad -f^*f \in \text{closure}[\text{SOS}_\mathcal{A} + LI + LI^*]$$

Special case $f = 1$. $Z_{\text{dir}}^\text{re}(LI)$ is empty $\text{IFF}$

$$-1 \in \text{SOS}_\mathcal{A} + LI + LI^*$$
**THM - Hard Zeroes:** $Z_{\text{hard}}^r(I)$ Cimpric?

Suppose $I$ is a *-closed two sided ideal.

$$Z_{\text{hard}}^r(I) \text{ is empty IFF } -1 \in \text{SOS}_A + I.$$ 

---

**Special cases with no SOS (Groups, groups, groups)**

Cleve Liu Slofstra - Two sided ideals (synchronous games)


$\mathcal{G} := \text{c}ntable \ group. \ A = \mathbb{C}[Z_2 \times \mathcal{G}] := \text{group algebra}.$

$Z_2 := \{-1, 1\}$

$\mathcal{C} := \text{elements of } Z_2 \times \mathcal{G} \ (\text{think } c_i \in \mathcal{C} \text{ has form } c_i = \pm g_i \text{ for } g_i \in \mathcal{G}).$

Let $\mathcal{L}I(\mathcal{C} - 1)$ be the left ideal generated by $\{c - 1 \mid c \in \mathcal{C}\}$.

Then the following are equivalent:

1. $Z_{\text{dir}}^r(\mathcal{C} - 1)$ is empty.
2. $1 \in \mathcal{L}I(\mathcal{C} - 1) + \mathcal{L}I(\mathcal{C} - 1)^*$
3. $1 \in \mathcal{L}I(\mathcal{C} - 1)$
4. $-1 \in \langle \mathcal{C} \rangle := \text{the group generated by } \mathcal{C}$
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.

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

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

Real NC NullSS applies directly. The issue is $1 \in \mathcal{L}(C - 1)$?

This is easy to test, say, using a noncommutative (left) Groebner Basis algorithm.

Advertisement: Use NCAlegbra
Aside: Not solvable (not perfect) games.

A measure $b$ of how close to solvable game $\Gamma$ 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 $\Gamma$ is

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

Note:

$$Val(\Gamma) = 1 \iff \text{the eqs have a solution (perfect),}$$

since for all words $\|A_iB_j\| \leq 1$ and $b$ averages them.
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. \( \text{Val}(CHSH) = \frac{\sqrt{2}}{2} \) and soln matrices are \( 4 \times 4 \)

2. \( \text{Classical Val}(CHSH) = \frac{1}{2} \)

**Quantum Advantage**

\[ : = \frac{\text{Val}(CHSH)}{\text{Classical Val}(CHSH)} = \sqrt{2} \]

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

NC Nullstellensatz

\[ \text{Zeros}(f) \supset \text{Zeros}(p) \]
\[ f = \text{Sos} + \sum_{j} h_j p h_j \]

NOT PERFECT Quantum Games

PosSS gives sharp upper bound on the value of a quantum game.

Doherty, Liang, Toner, and Wehner 2008
Navascues, Pironio, and Acín 2008
Hj Mccullough 2004

No SOS terms: Group Algebras and special p

3XOR

Perfect Quantum Strategies

\[ f \notin \mathbb{R} \]
Advertisement: XOR games package for quantum games
Needs Mathematica
Igor Klep, Zehong Zhang, Zinan Hu, Bill Helton
Mauricio de Oliveira

write Bill at
helton at ucsd dot edu
3XOR Setting

Group $\mathcal{G}$ consisting of:

Selfadjoint $A_i, B_j, C_k \quad i, j, k = 1, \ldots, m$ and $\sigma$ and defining relations:

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

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

$$\sigma^2 = 1 \quad \text{and } \sigma \text{ commutes everything} \quad \text{think } \sigma = \pm 1$$

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:**

$$(-1)^{t_1} A_{a_1} B_{b_1} C_{c_1} \psi = \psi, \quad \ldots \quad (-1)^{t_e} A_{a_e} B_{b_e} C_{c_e} \psi = \psi$$
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.
   2.2 Quantum advantage $\leq$ real Gröthendick constant $\leq 2$
   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 Conjecture.

**Aside:** Counter example to Tsierlson: by Ji, Natarajan, Vidick, Yuen and Wright in arXiv 2019 is a perfect synchronous 2 player game (seemingly in $\sim 10^4$ variables).
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 $\infty$ as the number of variables $m$ and dimension of the matrices $A_i, B_j, C_{\ell}$ go to $\infty$. Briet and Vidick 2012, Pérez-Garcia ... Junge 2008 respectively.
THIS TALK: Perfect 3 player 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 $A_i, B_j, C_\ell$ which are $8 \times 8$ matrices.

3. The quantum advantage of a perfect quantum solution is $\leq 8$
Reminder:
The **3XOR Group** $\mathcal{G}$ is the group with selfadjoint generators

$$A_i, B_j, C_k \quad i, j, k = 1, \ldots, m \quad \text{and} \quad \sigma$$

and defining relations:

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

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

$$\sigma^2 = 1 \quad \text{and} \ \sigma \ \text{commutes everything,} \quad \text{think} \ \sigma = -1$$

All 3XOR games live in $\mathcal{G}$. 
A particular game is defined by words (called clauses)

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

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

Part I:
**THM (Watts, Harrow, Kanwar, Natarajan; arXiv2018)**

A \( k \)-XOR game has no solution IFF \( \sigma \) is in \( \langle C \rangle \).
Thus the key issue is the subgroup membership problem for the group \( G \).

Sadly, there exist subgroups BAD of \( G \) where determining if a word \( w \) is in BAD is undecidable.
Part II:

\[ G^E := \text{Even subgroup of } G, \text{ is all even length words in } G. \]
\[ \langle C \rangle^E := \text{Even subgroup of } \langle C \rangle, \text{ all even length words in } \langle C \rangle. \]

Define \( K \), to be the normal subgroup of \( G^E \) generated by the commutator subgroup of \( G^E \); its generators are

\[ [A_i A_j, A_k A_\ell], [B_i B_j, B_k B_\ell], [C_i C_j, C_k C_\ell] \in K \]

**THM** [Watts, HarXiv 2020]

A 3XOR game has no solution IFF \( \sigma \) is in \( \langle C \rangle^E \) mod \( K \).

**PF:** Hard:

The (multi) graph associated to the clauses.
This subgroup membership problem is decidable in polynomial time, since $G^E/K$ is a commutative group (finitely generated). (Classical fact)

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

**PF quantum advantage $\leq 8$** was previously known for any solution based on a state $\psi$ of the form

$$\psi = \frac{1}{\sqrt{2}} \left( \begin{array}{l} 1 \\ 0 \end{array} \right) \otimes \left( \begin{array}{l} 1 \\ 0 \end{array} \right) \otimes \left( \begin{array}{l} 1 \\ 0 \end{array} \right) + \left( \begin{array}{l} 0 \\ 1 \end{array} \right) \otimes \left( \begin{array}{l} 0 \\ 1 \end{array} \right) \otimes \left( \begin{array}{l} 0 \\ 1 \end{array} \right) = \frac{1}{\sqrt{2}} (1, 0, 0, 0, 0, 0, 0, 0, 1)$$

MERP solution satisfies this.
SUMMARY

Real NC Nullstellensatz

\[ \text{Zeros}(f) \supset \text{Zeros}(p) \]

\[ -f^* f = \text{Idns} \left[ \text{Sos} + \lambda p + p^* \hat{p} \right] \]

\[ f = \lambda p \]

No SOS terms:
- Group Aigts and special p

3XOR

\[ \exists \text{ Perfect Quantum Strategies } \]

\[ \text{decidable in poly time.} \]

But quantum advantage < 0
THANKS FROM
Jaka Cimpric, Scott McCullough, Igor Klep
and Adam Benne Watts and Bill
TO THE AUDIENCE FOR PERSISTING

Open Questions

Hardness of Deciding XOR Game’s Value

- [Vidick ‘13]
- $(\omega_p^2)$
- K-modding + ncSoS?
- ?
- $K$ modding with smaller $K$?
- ?? (Open)
Epilogue
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 \( M_{\star_i} \) is a \( 2 \times 2 \) signature matrix (a qubit) and the solution vector \( \psi \) is
\[ \psi = \frac{1}{\sqrt{2}} (1, 0, 0, 0, 0, 0, 0, 1)^T \]

2. (More detail) The matrices \( M_{a_i}, M_{b_j}, M_{c_\ell} \) have the form
\[ M_{\star} = \exp(i \theta \sigma_z) \sigma_x \exp(-i \theta \sigma_z) \] (3)
for some \( \theta \)'s which depend on \( a_i, b_j, c_\ell \). Here \( \sigma_x, \sigma_z \) are the Pauli \( X \) and \( Z \) matrices:
\[ \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \]
Open Questions

Hardness of Deciding XOR Game’s Value

- T.sel'son '80
- $\omega^*_t p$
- $K$-modding + $ncSoS$?
- [Vidick '13]

- $P$
- Probably Hard
- ?? (Open)
Quantum graph coloring  A 2 player synchronous game.

$G$ is a graph and $k$-quantum colors can be associated with selfadjoint unitary matrices $X^r_i$, ie. $(X^r_i)^2 = I$, vertex $i$ and color $r$.

$$\left( X^r_i \right) = \left( X^r_i \right)^*, \quad \left( X^r_i \right)^2 = I \quad (4)$$

$$X^r_i X^s_i X^r_i X^s_i = I \quad (5)$$

$$X^1_i X^2_i \cdots X^k_i = -I \quad (6)$$

$$(I - X^r_i)(1 - X^r_j) = 0 \text{ if } (i, j) \text{ is an edge of } G, \text{ all } r \quad (7)$$

**Q coloring problem:** Do matrix (or operator) solutions exist?

The issue is **hard zeroes**

$\mathbb{C}[G]$ group algebra for $G$ defined by relations $(4)(5)(6)$

$\mathcal{I}_k :=$ the two sided ideal defined by $(11)$ for $k$ quantum colors.
THM [Paulsen, H, Meyer, Satriano 2019] For EVERY graph the quotient algebra $\tilde{A} := \mathbb{C}[G]/\mathcal{I}_4$ is non trivial. I.e.

$$-1 \notin \mathcal{I}_4$$

However, many graphs are not 4 q colorable. For these

$$-1 \in \text{SOS} + \mathcal{I}_4.$$ 

Eg. A 5 clique is not 4 quantum colorable,

THM [Paulsen, H, Meyer, Satriano 2019] Any 2 player synchronous game has an associated *-algebra $\tilde{A}$ and the game having a perfect strategy is equivalent to there being a unital $\mathcal{C}^*$-representation into $B(H)$. 