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

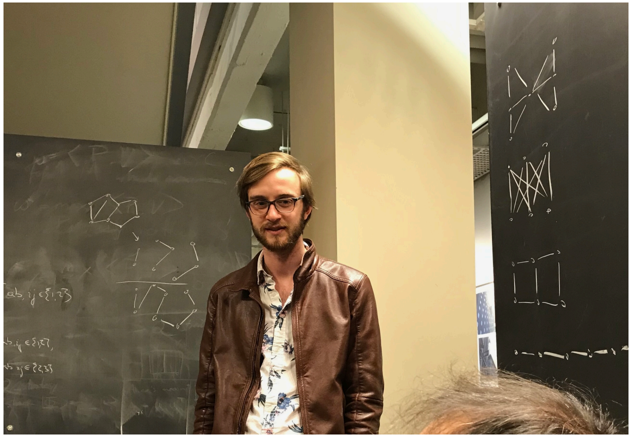
Advertisement: **Try noncommutative computation**

NCAlgebra[1] **NCSoSTools**[2]

[1] Helton, de Oliveira (UCSD), Stankus (CalPoly SanLObispo), Miller

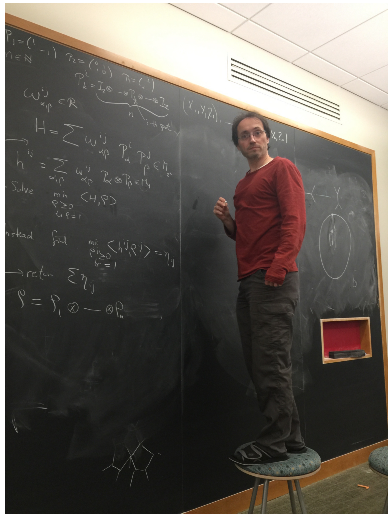
[2] Igor Klep

Adam Bene Watts - 3 XOR



Adam Bene Watts

NC RAG guys: Jaka Cimpric, Igor Klep, Scott McCullough



Ingredients of Talk: NC polynomials

$x = (x_1, \cdots, x_g)$ $\quad x^* = (x_1^*, \cdots, x_g^*)$ 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 talk

WE SKIP THIS

NC Nullstellensatz

Zeros(f) ⊃ Zeros(p)

R: $-f^*f = \text{SoS} + hp + p^*h^*$

ℂ: $f = hp$

No SoS terms: Group Algebras and special p

3XOR

PERFECT QUANTUM STRATEGIES

NC Positivstellensatz

f(x) is PsD if p(x) is PsD

$$f = \text{SoS} + \sum_{j}^{\text{Finite}} h_j^* \, p \, h_j$$

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 (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** $X = (X_1, \ldots, X_g) \in (\mathbb{C}^{n\times n})^g$
   Eg. $p(x) = x_1^2 + x_2^2 - 1$ $\quad Z_{hard}(p) = \{X | \ X_1^2 + X_2^2 = I\}$
   . $Z_{hard}(p) := \quad \bigcup_n \{X \in (\mathbb{C}^{n\times n})^g \ | \quad p(X) = 0\}$
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**
   $Z_{det}(p) = \quad \bigcup_n \{X \in (\mathbb{C}^{n\times n})^g | \ \ \det p(X) = 0\}$

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

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**

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

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

———

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

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

Is this the "same form" as ours? ———

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

———

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.

Ex: $\mathcal{A} := \mathbb{C}<\mathbf{x}, \mathbf{x}^*>$ **- 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.

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

——

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

THM - Dir Zeroes: $Z^{re}_{dir}(\mathcal{LI})$ [Cimpric,H, McCullough, 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 $f = 1$. $Z^{re}_{dir}(\mathcal{LI})$ **is empty IFF** ——

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

THM - Hard Zeroes: $Z^{re}_{hard}(\mathcal{I})$ Cimpric?
Suppose $\mathcal{I}$ is a *-closed two sided ideal.

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

Special cases with no SOS (Groups, groups, groups)
Cleve Liu Slofstra -Two sided ideals (synchronous games)

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

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

Aside: Not solvable (not perfect) games.

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

$$b(A, B) := \frac{1}{4}(+A_0 B_0 + A_1 B_0 + A_0 B_1 - A_1 B_1)$$

Then the quantum value of the game Γ **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 $\|A_i B_j\| \leq 1$ **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

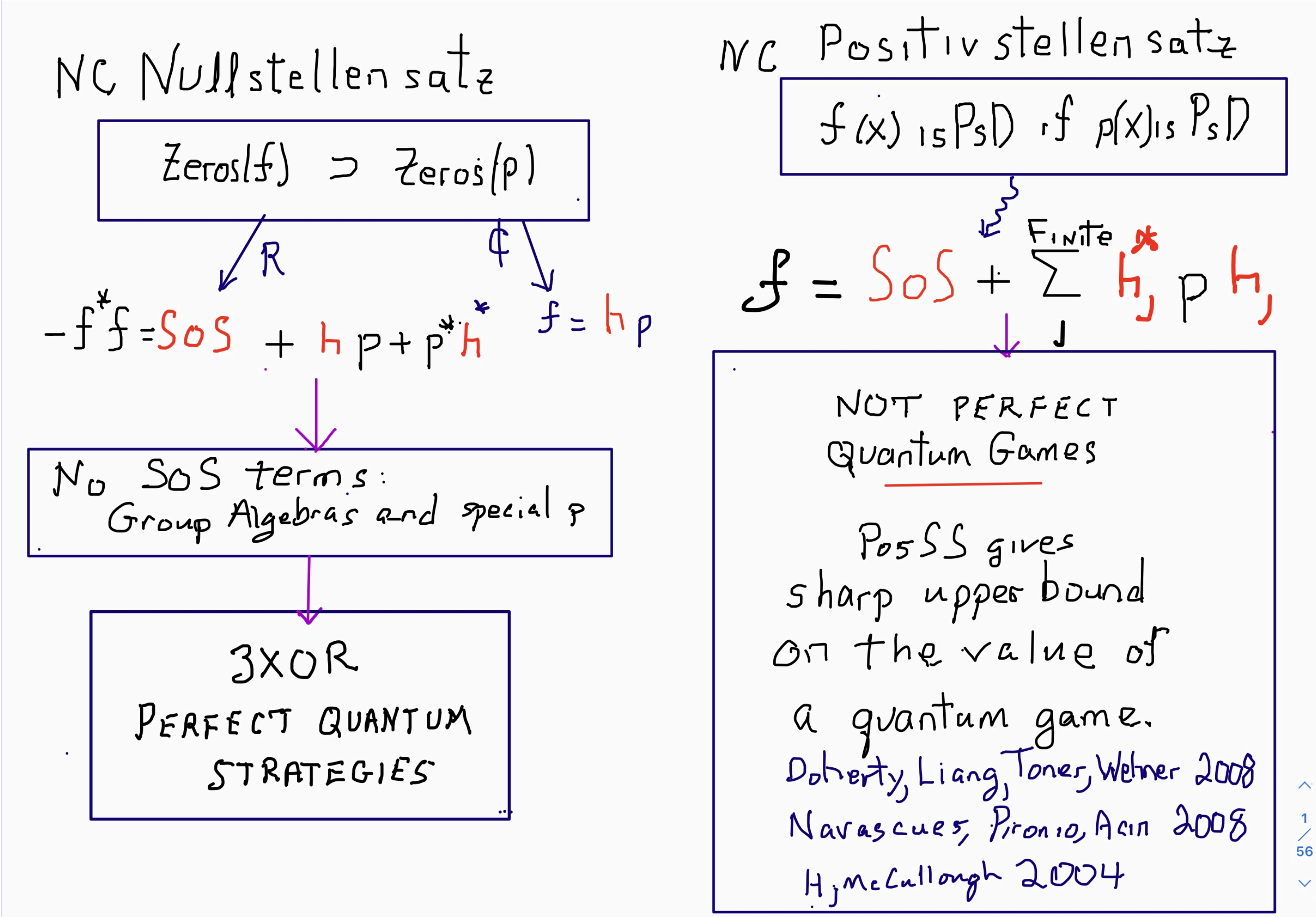
ANS: **(CHSH) (Bell 1964)**

1. $Val(CHSH) = \frac{\sqrt{2}}{2}$ **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



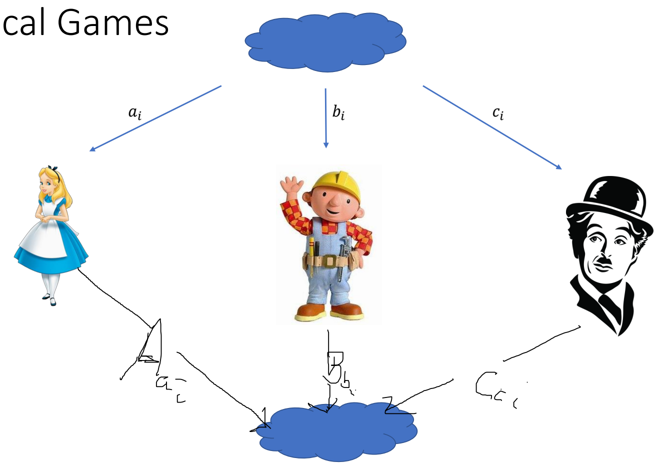
. 3 XOR GAMES

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

Nonlocal Games



3XOR Setting

Group $\mathcal{G}$ consisting of:
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. $A_i B_j A_i^{-1} B_j^{-1} = I$

$\sigma^2 = 1$ **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:

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

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 ≤ 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 Tsierlsen: by Ji, Natarajan, Vidick, Yuen and Wright in arXiv 2019 is a perfect synchronus 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 ∞ 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.**

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_ℓ which are 8×8 matrices.**

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

Ideas in the proof.

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

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

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

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

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)

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

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

MERP solution satisfies this.

$\square$

SUMMARY

Real NC Nullstellensatz $\quad \mathcal{Z}^{re}_{dir}$

$$\text{Zeros}(f) \supset \text{Zeros}(p)$$

$\mathcal{Z}^{re}$ ↙ $\qquad\qquad$ ↘ $\mathbb{C}$

$$-f^*f = \text{clos}\left[\text{SoS} + h\,p + p^*h^*\right] \qquad\qquad f = h\,p$$

↓

No SoS terms:
Group Algs and special p

↓

3XOR

∃ PERFECT QUANTUM STRATEGIES
decidable in poly time.

But
quantum advantage < 8

THANKS FROM

Jaka Cimpric, Scott McCullough Igor Klep and Adam Benne Watts and Bill

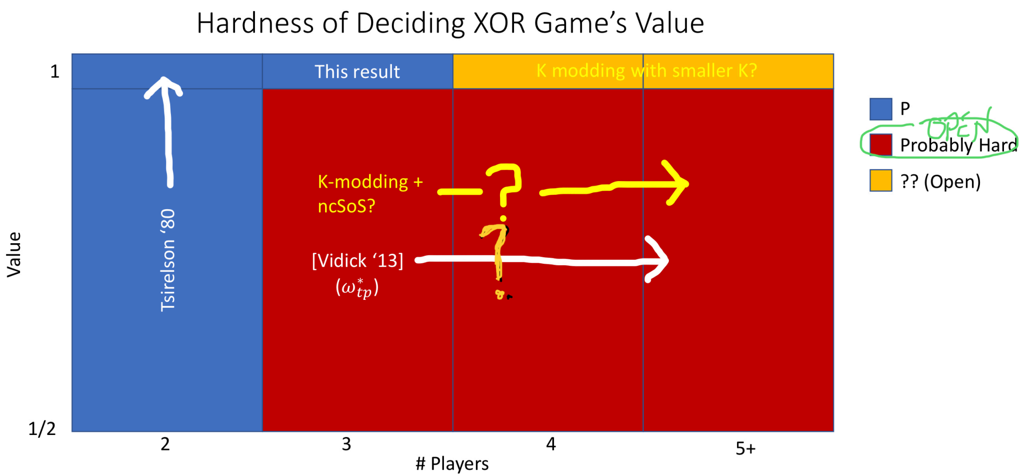
TO THE AUDIENCE FOR PERSISTING

Jaka

Scott

Adam Igor

Open Questions



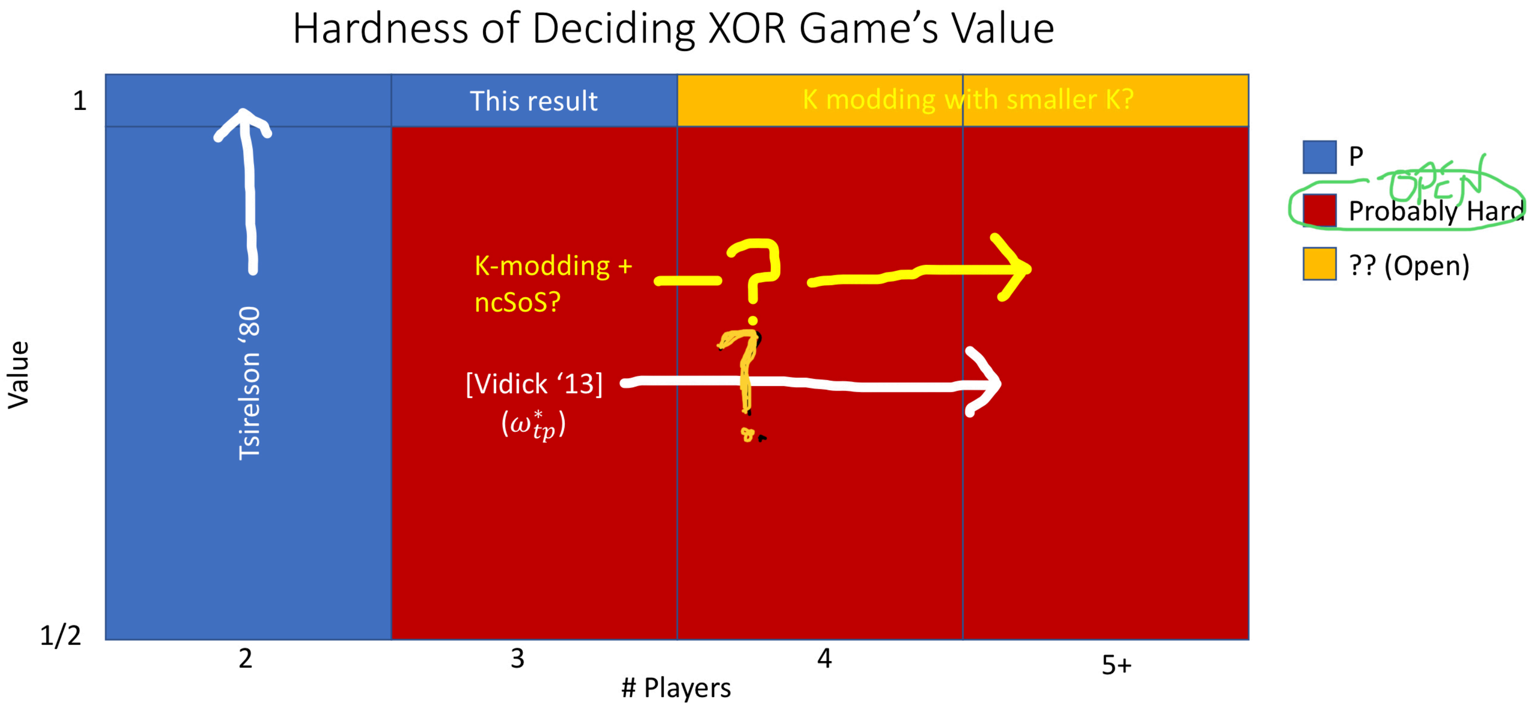
Epilogue

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_{*_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 $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$,

Open Questions



Quantum graph coloring   A 2 player synchronous game.

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

$$(X_i^r) = (X_i^r)^*, \qquad (X_i^r)^2 = I \tag{4}$$

$$X_i^r X_i^s X_i^r X_i^s = I \tag{5}$$

$$X_i^1 X_i^2 \cdots X_i^k = -I \tag{6}$$

$$(I - X_i^r)(1 - X_j^r) = 0 \ \mathit{if}\, (i,j) \ \mathit{is\ an\ edge\ of}\ \mathcal{G}, \ \mathit{all}\ r \tag{7}$$

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 $\widehat{\mathcal{A}} := \mathbb{C}[G]/\mathcal{I}_4$ is non trivial. Ie.

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

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

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

Eg. A 5 clique is not 4 quantum colorable,

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