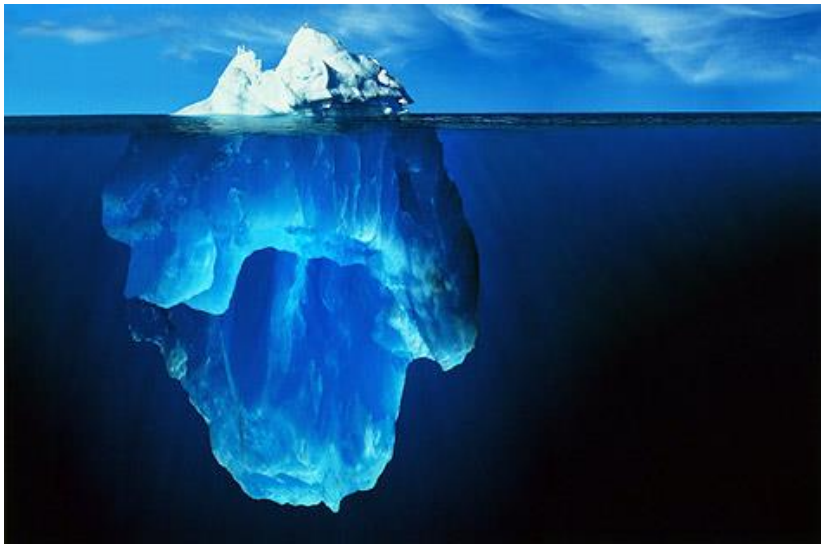
Connes' embedding problem, Tsirelson's problem, and MIP* = RE



THOMAS VIDICK

CALIFORNIA INSTITUTE OF TECHNOLOGY

Joint work with Zhengfeng Ji (UTS), Anand Natarajan (MIT), John Wright (UT Austin) and Henry Yuen (Columbia)

MIP* = RE

- In complexity theory a problem is represented as a set $S \subseteq \{0,1\}^*$
- The problem associated to S is, "given x, is $x \in S$?"
- Ex: $S =$ { binary representations of composite numbers}

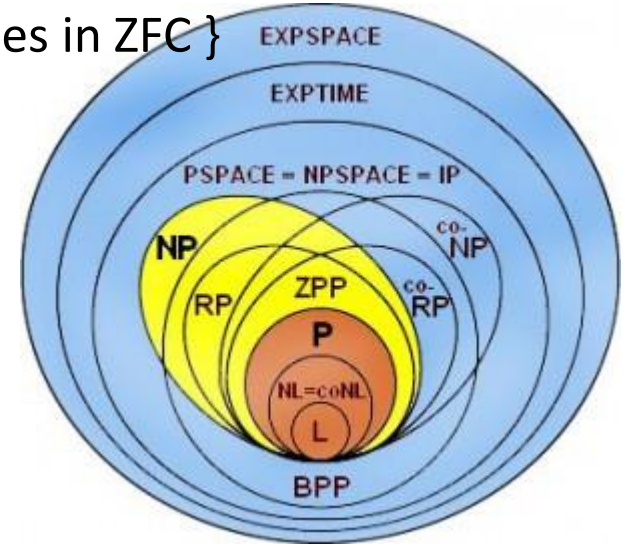
  $S =$ { binary representations of connected graphs }

  S = { binary representations of provable sentences in ZFC }

- A complexity class is a collection of problems,

  i.e. a collection of sets that share some measure

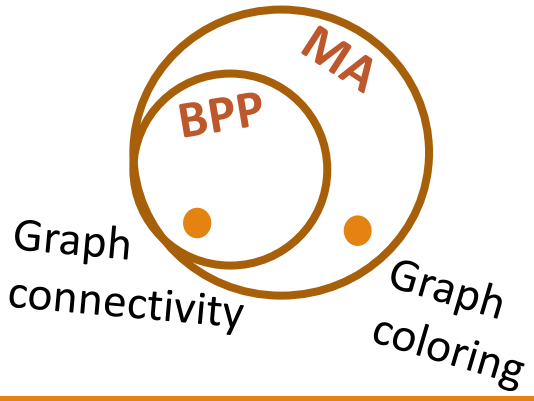
  of "complexity"



MIP* = RE

BPP: Problems for which there is a (randomized) polynomial-time algorithm that always returns the correct answer.

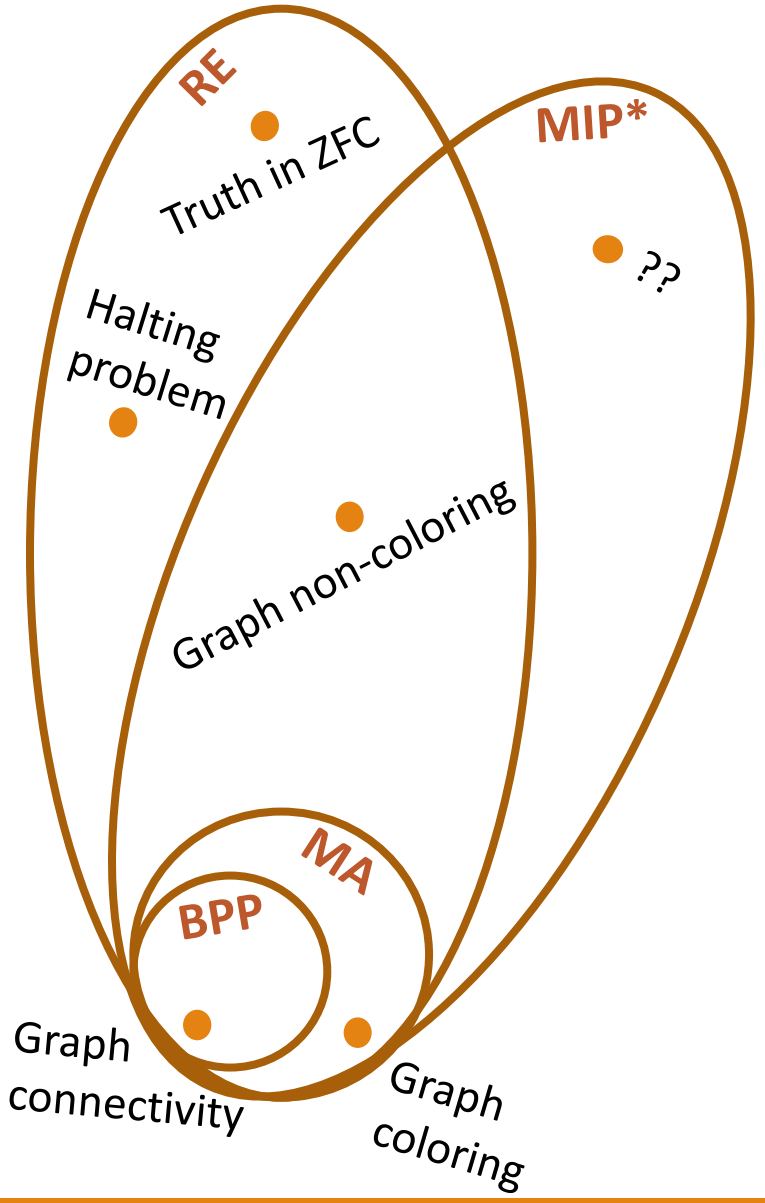
MA: Problems that can be *verified* in (randomized) polynomial time, given a polynomial-size proof



MIP* = RE

RE: Problems for which there is an algorithm that *eventually terminates and returns 'YES'* on positive instances (and doesn't terminate/returns 'NO' on negative instances)

MIP*: Problems that can be *verified* in polynomial time by interacting with quantum provers sharing entanglement



Consequences of MIP* = RE

- *Negative answer to Tsirelson's problem*: the tensor and commuting models for quantum correlations are strictly distinct

- *Negative answer to Connes' embedding problem*: there exist type II_1 von Neumann algebras that are not 'hyperfinite'

- *Verification of quantum systems*: asymptotically efficient tests for arbitrarily high-dimensional entanglement

Plan for the talk

1) Quantum correlations and Tsirelson's problem

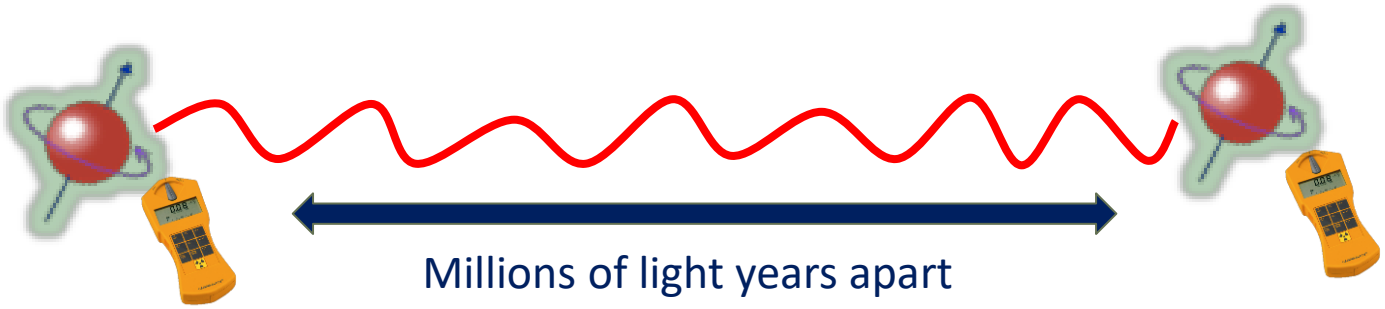
2) An approach to Tsirelson's problem via algorithms & complexity

3) Quantum multiprover interactive proofs

4) Open questions

Quantum correlations and Tsirelson's problem

Quantum nonlocality



Local measurements on far-away particles can exhibit unexpected correlations...

… almost as if one particle could instantaneously influence the other!

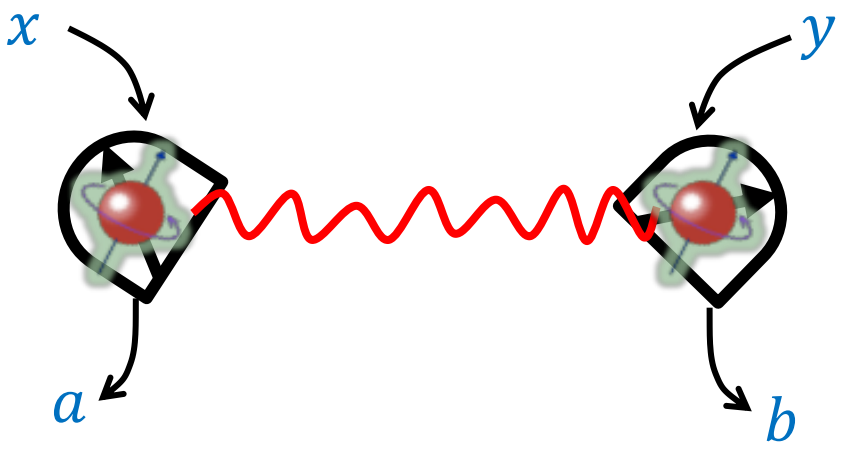
Schrödinger called this phenomenon *quantum entanglement*.

Nonlocal correlations

- Experimental data modeled as family of distributions $\{p(a,b|x,y)\} \in \mathbb{R}^{m^2k^2}$

  x, y: m possible measurement choices

  a, b: k possible measurement outcomes



- Bell 1964: some $\{p(a,b|x,y)\}$ have a model in QM but no classical explanation
- Classical correlations:

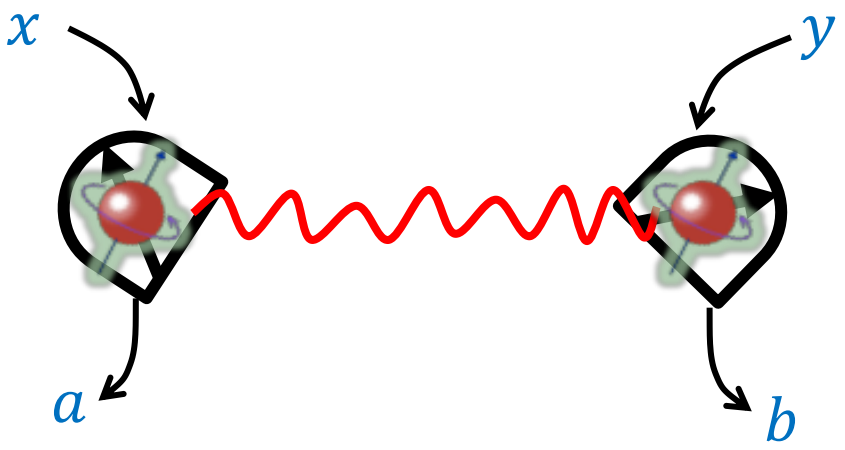
$$p(a,b|x,y) = \int_{\lambda} q_A(a|x,\lambda) q_B(b|y,\lambda) d\lambda$$

Nonlocal correlations

- Experimental data modeled as family of distributions $\{p(a,b|x,y)\} \in \mathbb{R}^{m^2k^2}$

  x, y: m possible measurement choices

  a, b: k possible measurement outcomes

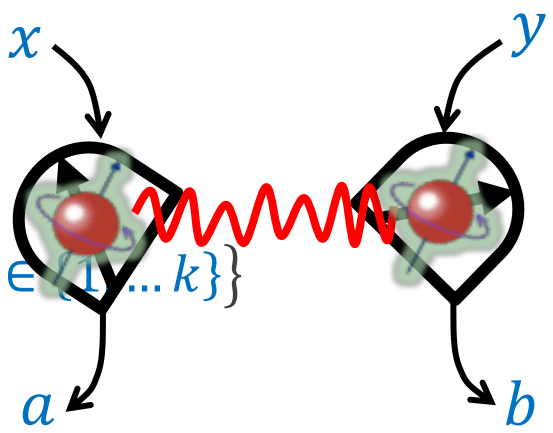


- Bell 1964: some $\{p(a,b|x,y)\}$ have a model in QM but no classical explanation
- Classical correlations:

$$p(a,b|x,y) = \int_{\lambda} q_A(a|x,\lambda) q_B(b|y,\lambda) d\lambda$$

- Tsirelson '80s: principled approach to study geometry of quantum correlations

Tsirelson's setup



- *Correlation*: family of distributions

$$\{\, p(a,b|x,y) \mid \; x,y \in \{1,\dots,n\} \;\; a,b \in \{1,\dots k\}\}$$

- Quantum correlations (1):

  Pure state $|\psi\rangle \in \mathcal{H} \otimes \mathcal{H}, \quad \||\psi\rangle\| = 1$

  For every x, psd operators $\{P_a^x\}_a$ such that $\sum_a P_a^x = I$. Similarly, $\{Q_b^y\}$

- $$p(a,b|x,y) = \langle\psi|P_a^x \otimes Q_b^y|\psi\rangle$$

- Quantum correlations (2):

  Pure state $|\psi\rangle \in \mathcal{H}, \quad \||\psi\rangle\| = 1$

  For every x, psd operators $\{P_a^x\}_a$ such that $\sum_a P_a^x = I$. Similarly, $\{Q_b^y\}$

$$p(a,b|x,y) = \langle\psi|P_a^x Q_b^y|\psi\rangle \qquad \forall xyab, \left[P_a^x, Q_b^y\right] = 0$$

Tsirelson's problem

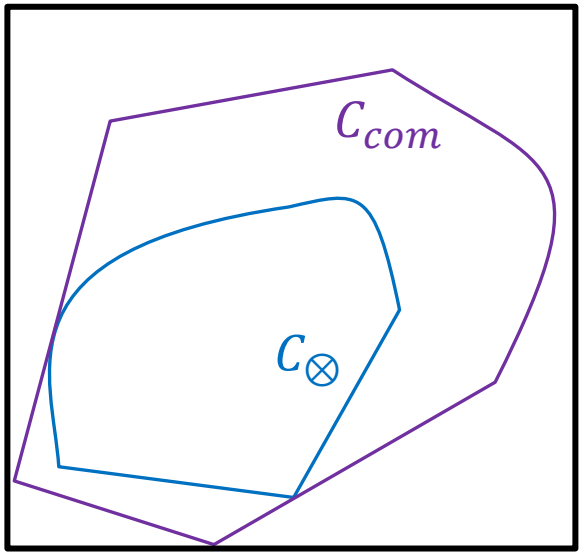
Quantum Bell-type inequalities are defined in terms of two (or more) subsystems of a quantum system. The subsystems may be treated either via (local) Hilbert spaces, - tensor factors of the given (global) Hilbert space, or via commuting (local) operator algebras. The latter approach is less restrictive, it just requires that the given operators commute whenever they belong to different subsystems.

Are these two approaches equivalent?

Tsirelson's problem

$$C_{\otimes}(m,k) = \{ \left(\langle\psi| P_a^x \otimes Q_b^y |\psi\rangle\right)_{abxy} : \ |\psi\rangle \in \mathcal{H} \otimes \mathcal{H} \}$$

$$C_{com}(m,k) = \{ \left(\langle\psi| P_a^x Q_b^y |\psi\rangle\right)_{abxy} : \ |\psi\rangle \in \mathcal{H}, [P_a^x, Q_b^y] = 0 \}$$



- Both sets are convex
- $C_{\otimes}(m,k) \subseteq C_{com}(m,k)$ for all m, k.
- $C_{com}(m,k)$ is closed, but [Slofstra'18] $C_{\otimes}(n,k)$ is not!

Is $\overline{C_{\otimes}(m,k)} = C_{com}(m,k)$ for all $m, k \geq 2$?

The connection with operator algebras

A von Neumann algebra is an algebra $M \subset \mathcal{B}(\mathcal{H})$ s.t.:

- $I \in M$
- M is closed under adjoints
- M is closed in the weak operator topology

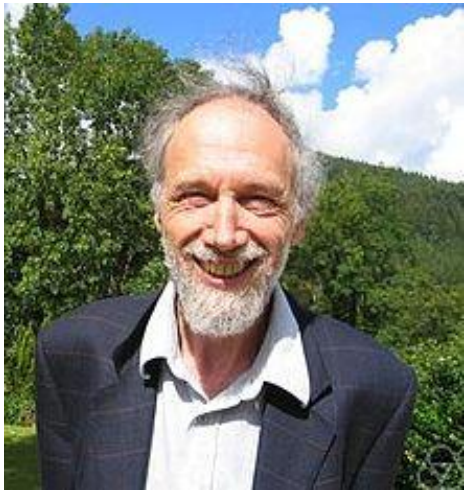
- Over the next decade, von Neumann (with F. Murray) wrote a series of papers that launched the field of operator algebras

- Important goal of operator algebras: classification of von Neumann factors
  - Main species: Type I, Type II, Type III
  - Within each type, there are subspecies. Type I factors were completely solved by Murray and von Neumann. They also made progress on Type II factors.
  - 1970s: Alain Connes won the Fields Medal for his contributions to the theory of operator algebra, including the classification of Type III factors.

The connection with operator algebras

- In a 1976 paper, Connes makes a casual remark about Type II_1 factors:

> *"We now construct an approximate embedding of N into R. Apparently such an embedding ought to exist for all II_1 factors."*



- This throwaway line became known as Connes' Embedding Problem: roughly speaking, can every finite subset of a II_1 factor be approximately embedded in the finite-dimensional matrices?
- Easier to state, weaker conjecture: are all countable groups hyperlinear?

A countable group Γ is *hyperlinear* if $\forall n \geq 1$ there is $\sigma_n : \Gamma \to U_n$ s.t.

- $\forall g, h \in \Gamma, \quad \|\sigma_n(gh) - \sigma_n(g)\sigma_n(h)\|_F \to_{n\to\infty} 0$
- $\forall g \neq 1_\Gamma, \quad \|\sigma_n(g) - I_n\|_F \to_{n\to\infty} 1$

($\|\cdot\|_F$ is the dimension-normalized Frobenius norm)

Equivalent formulations of CEP

- CEP: "Every type II_1 von Neumann algebra embeds in an ultrapower of the hyperfinite II_1 factor $\mathcal{R}$"
- Kirchberg in 1993 introduces QWEP conjecture and shows its equivalence to

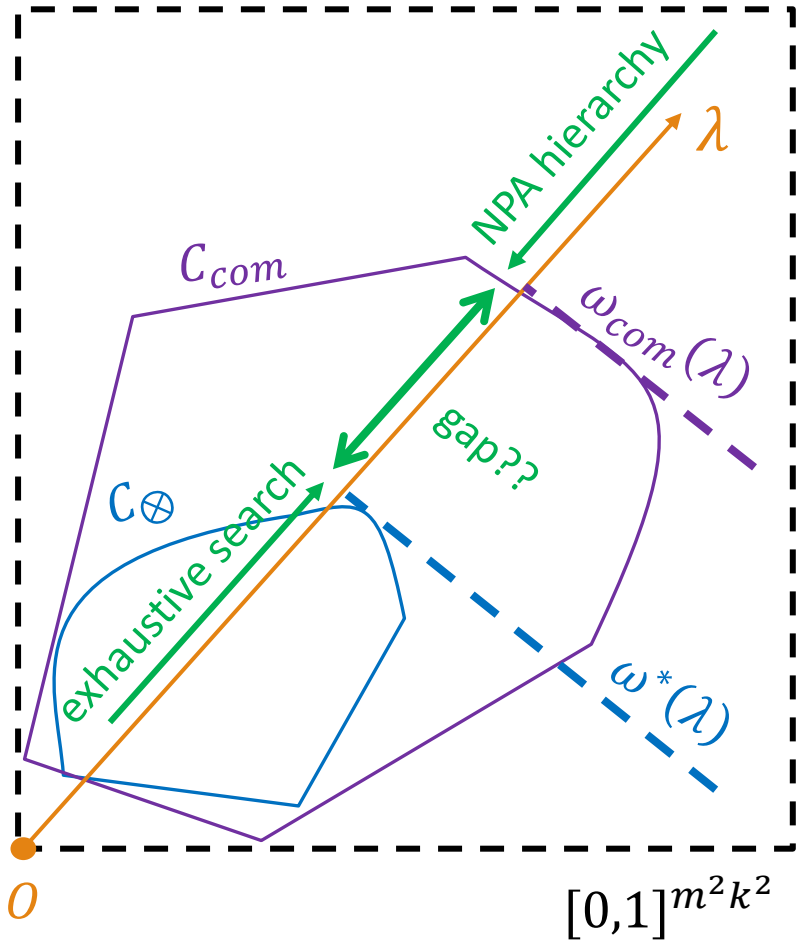
$$C^*(F_2) \otimes_{min} C^*(F_2) \stackrel{?}{=} C^*(F_2) \otimes_{max} C^*(F_2)$$

- Kirchberg proved the equivalence CEP $\leftrightarrow$ QWEP
- Multiple other reformulations: free entropy, group theory, etc.
- [Fritz,Junge et al.'11] QWEP/CEP imply a positive answer to Tsirelson's problem
- [Ozawa'12] Equivalence:

$$\overline{C_{qs}(m,k)} = C_{qc}(m,k) \quad \text{for all } n,k \geq 2 \text{ iff CEP holds}$$

An approach to Tsirelson's problem via algorithms & complexity

Optimizing linear functionals over a convex set



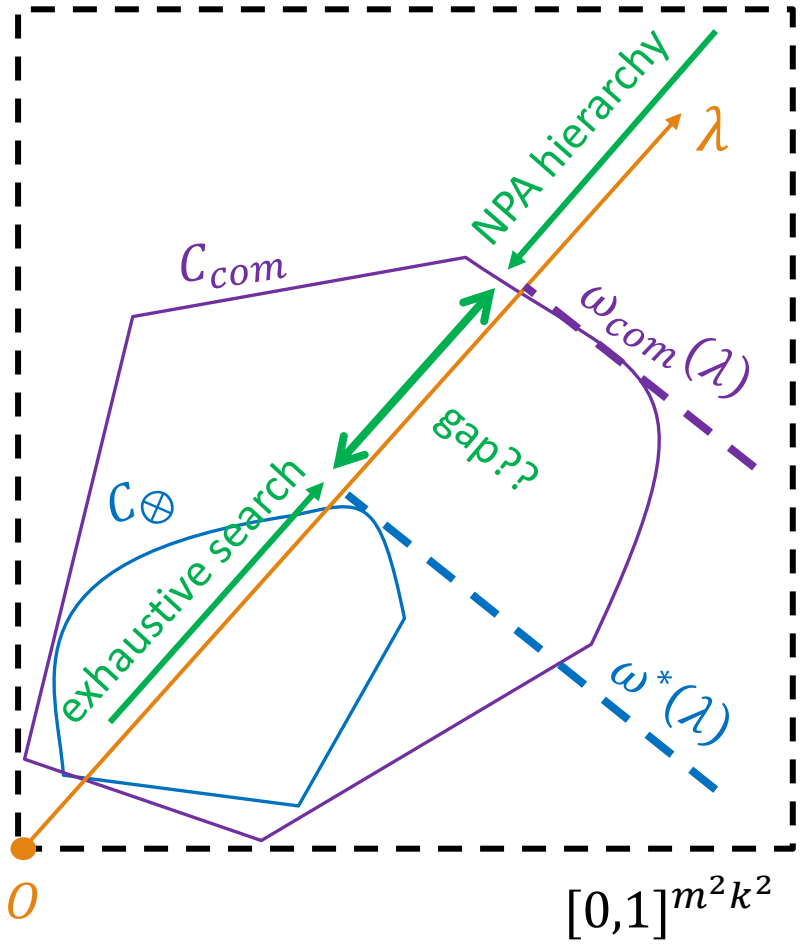
$$C_{\otimes}(m,k) = \{ \left(\langle\psi|P_a^x \otimes Q_b^y|\psi\rangle\right)_{abxy} : |\psi\rangle \in \mathcal{H} \otimes \mathcal{H} \}$$

$$\omega^*(\lambda) = \sup_{p \in C_{\otimes}(m,k)} |\lambda \cdot p|$$

$$C_{com}(m,k) = \{ \left(\langle\psi|P_a^x Q_b^y|\psi\rangle\right)_{abxy} : |\psi\rangle \in \mathcal{H}, [P_a^x, Q_b^y] = 0 \}$$

$$\omega_{com}(\lambda) = \sup_{p \in C_{com}(m,k)} |\lambda \cdot p|$$

Optimizing linear functionals over a convex set



- Suppose exhaustive search & NPA converge to the same value, for all λ

→ *Tsirelson's problem has a positive answer*

- Suppose exhaustive search & NPA *do not* converge to the same value, for some λ

→ *Tsirelson's problem has a negative answer*

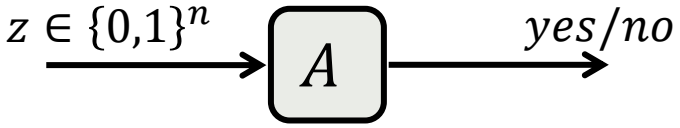
- [Fritz-NT'14] Suppose that $\omega^*(\lambda)$ is *uncomputable*

→ *Tsirelson's problem has a negative answer*

Quantum multiprover interactive proofs

Interactive proofs

- **BPP**: efficient *decision*

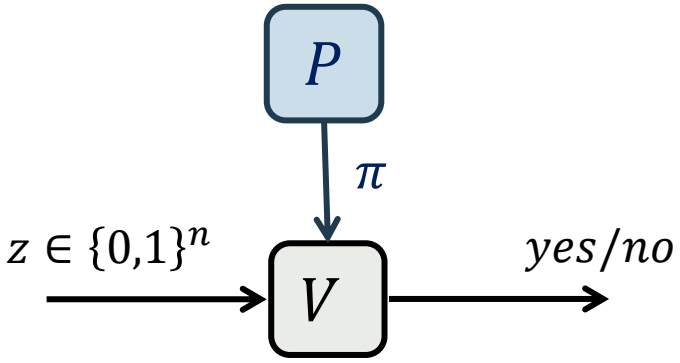


Time: randomized/quantum poly(n)

- **MA**: efficient *verification*

  z is "yes" $\Rightarrow$ $\exists\, \pi$, accepted by V whp

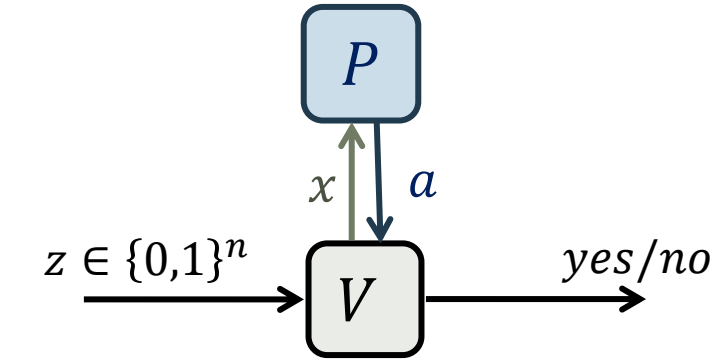
  z is "no" $\Rightarrow$ $\forall\, \pi$, rejected by V whp



Time: randomized/quantum poly(n)

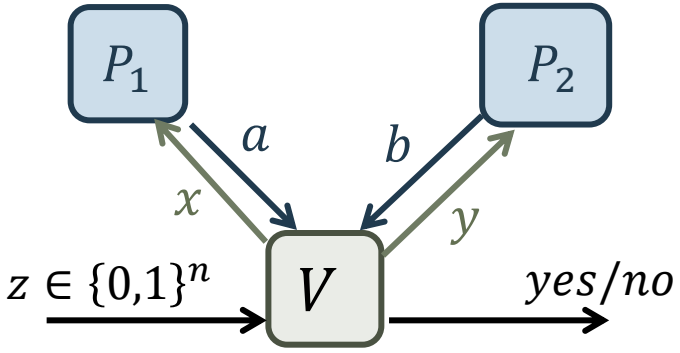
Interactive proofs

- **IP**: efficient *interactive verification*



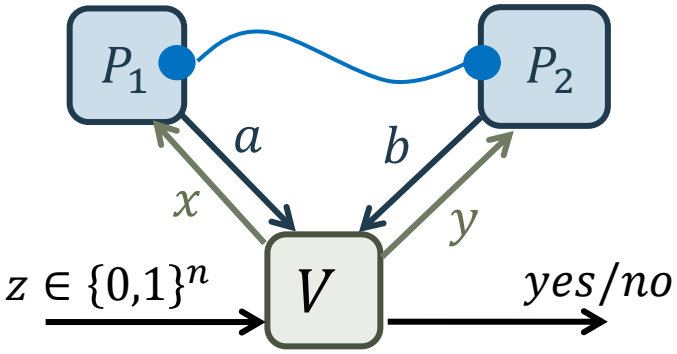
Time: randomized/quantum $\mathrm{poly}(n)$

- **MIP**: efficient *interactive verification with two provers*



Time: randomized/quantum $\mathrm{poly}(n)$

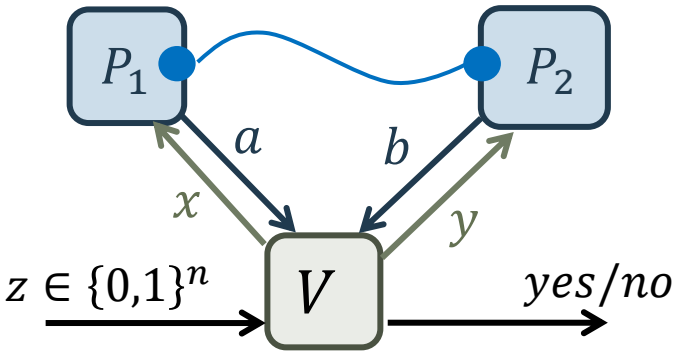
Interactive proof systems as optimization problems



MIP* : efficient *interactive verification*
with two provers sharing entanglement

- [Cleve-HTW'04] The class MIP* characterizes the complexity of optimizing over the sets $C_{\otimes}(m,k)$

Interactive proof systems as optimization problems

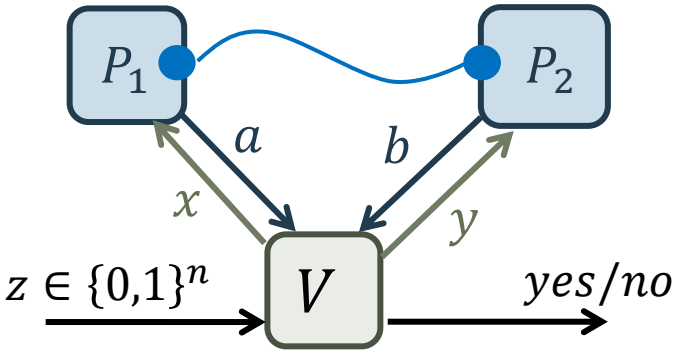


Max $\mathrm{acc}(V, z)$

$$= \sup_{\text{strategy}} \Sigma_{xyab}\, \pi(x,y) 1_{ab\text{: correct for } x\,y} \langle \psi | P_a^x \otimes Q_b^y | \psi \rangle$$

$$= \omega^*(\lambda) \qquad \text{for} \quad \lambda_{abxy} = \pi(x,y) 1_{ab\text{: correct for } x\,y}$$

Interactive proof systems as optimization problems

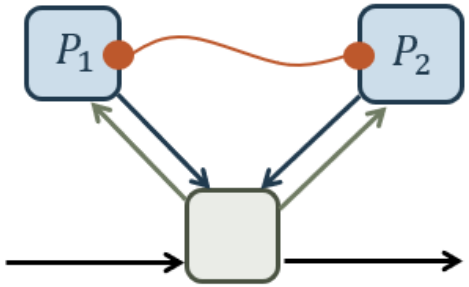


MIP* : efficient *interactive verification with two provers sharing entanglement*

- [Cleve-HTW'04] The class MIP* characterizes the complexity of optimizing over the sets $C_{\otimes}(m,k)$
- What can be said about problems in MIP*?
- $\omega^*(\lambda)$ uncomputable $\leftrightarrow$ MIP* contains undecidable languages

MIP* ⊇ RE

- [Ito-V'12] MIP* contains all problems in MIP = NEXP
  - Proof shows that error correction-based probabilistically checkable proofs used in the proof of NEXP = MIP are sound in the presence of entanglement



- [Natarajan-W'19] MIP* contains all problems in NEEXP
  - Proof leverages entanglement between the provers as a tool to aid verification

- [Natarajan-JVYW'20] MIP* ⊇ RE by recursively applying technique from [NW'19]

- [Turing'1936] RE contains the halting problem, which is undecidable
  - MIP* contains undecidable languages

The compression theorem

COMPRESS: $V \mapsto V'$ s.t.

i. Size(V') $\approx$ Size(V)

ii. $\omega^*(\lambda_{n+1}) = 1 \Longrightarrow \omega^*(\lambda'_n) = 1$

iii. $\mathcal{E}\left(\lambda'_n, \frac{1}{2}\right) \geq \max\{\, \mathcal{E}\left(\lambda_{n+1}, \frac{1}{2}\right), n \,\}$

Smallest dim($\mathcal{H}$) required to find p such that $|\lambda \cdot p| \geq 1/2$

V, V' are Turing machines

On input n, V returns coefficients of linear functional λ_n on $\mathbb{R}^{m(n)^2 k(n)^2}$

- Proof uses PCP + self-testing techniques to "simulate" λ_{n+1} using λ'_n
- Using (i) + (iii), N steps of compression gives "constant-size" functional $\lambda = \lambda_1$ that requires $\geq N$-dimensional spaces to to find p such that $|\lambda \cdot p| \geq 1/2$

Recursive compression

- Fix a Turing Machine M. Define a computable map T: $V \mapsto V''$
  - Let n be given as input to V''
  - Run M for n steps. If M halts then accept. (Return trivial $\lambda''_n = 1$.) Otherwise, return λ''_n = COMPRESS(V, n)

- Let $\hat{V}$ be a *fixed point* of T. Let λ be returned by $\hat{V}$ on input $n = 1$
- Suppose M halts. Then $\omega^*(\lambda) = 1$. Proof:
  - For all large enough T, $\omega^*\left(\widehat{\lambda_T}\right) = 1$
  - By (ii), $\omega^*(\lambda) = \omega^*(\widehat{\lambda_1}) \geq \omega^*(\widehat{\lambda_2}) \geq \cdots \geq \omega^*\left(\widehat{\lambda_T}\right) = 1$

Recursive compression

- Fix a Turing Machine M. Define a computable map T: $V \mapsto V''$
  - Let n be given as input to V''
  - Run M for n steps. If M halts then accept. (Return trivial $\lambda_n'' = 1$.) Otherwise, return λ_n'' = COMPRESS(V, n)

- Let $\hat{V}$ be a *fixed point* of T. Let λ be returned by $\hat{V}$ on input $n = 1$
- Suppose M *does not* halt. Then $\omega^*(\lambda) \leq 1/2$. Proof:
  - By (iii), for any $\mathrm{n} \geq 1$, $\mathcal{E}\left(\lambda, \frac{1}{2}\right) = \mathcal{E}\left(\widehat{\lambda_1}, \frac{1}{2}\right) \geq \cdots \geq \mathcal{E}\left(\hat{\lambda}, \frac{1}{2}\right) \geq n$
  - No finite-dimensional p can witness $|\lambda \cdot p| \geq 1/2$

Summary

$$C_{\otimes}(m,k) = \{ \left(\langle\psi| P_a^x \otimes Q_b^y |\psi\rangle\right)_{abxy} : \ |\psi\rangle \in \mathcal{H} \otimes \mathcal{H} \}$$

$$C_{com}(m,k) = \{ \left(\langle\psi| P_a^x Q_b^y |\psi\rangle\right)_{abxy} : \ |\psi\rangle \in \mathcal{H}, [P_a^x, Q_b^y] = 0 \}$$

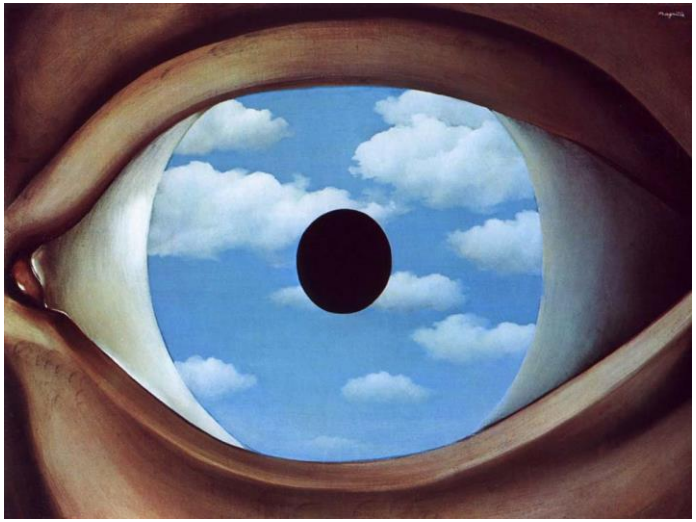
- Tsirelson's problem: Is $\overline{C_{\otimes}(m,k)} = C_{com}(m,k)$ for all $m, k \geq 2$?
- We give a negative answer: $\overline{C_{\otimes}(m,k)} \neq C_{com}(m,k)$ for some m, k
- Proof shows that that linear optimization over $C_{\otimes}$ (= computing the quantum value) for specific class of λ (coming from interactive proofs) is intractable
- Techniques combine proof verification and self-testing. Entanglement used to certify increasingly complex computations in a recursive fashion

Some questions

Operator algebras:

- Complexity-theoretic argument implies *existence* of a correlation that can be realized in the commuting model, but not in the tensor model
- Working through the proof gives an explicit example.
  - We could write python code to list the coefficients; at most 10^{20}. Can we do better?
- To get an explicit "non-embeddable" von Neumann algebra, we need to identify the state and measurement operators.
- Refining the construction could give a non-hyperlinear group
  - Our correlation is a synchronous correlation
  - A linear system game would give a group

Thank you



Open questions

Some questions

Complexity theory:

- What is the complexity of commuting-strategy MIP, MIP^{co}?
- Proof requires only two provers. Corollary: MIP(k provers) = MIP(2 provers)
  - Direct argument?
- Can we verify QMA statements using log-length questions and quantum polynomial-time provers (+ access to the witness)?
- Can we show uncomputability of $\lambda \mapsto \omega^*(\lambda)$ for *fixed* n, k ?
- Beyond RE: can higher levels of the arithmetical hierarchy be characterized by interactive proof variants?
  - [Coudron-S'19] characterize zero-gap MIP^{co}
  - [Mousavi-NY'20] characterize zero-gap MIP*

Some questions

Verification:

- Results characterize very high-complexity problems
  - Can resources be scaled down to obtain highly efficient verifiers for, e.g. BQP?
  - Cryptographic techniques could reduce interaction or even remove the need for two provers
- Protocols inherently non robust to noisy entanglement
  - [Yao'19] noisy-MIP* collapses to finite level of non-deterministic time hierarchy

Tsirelson's problem

$$C_{\otimes}(n,k) = \{ \left(\langle\psi| P_a^x \otimes Q_b^y |\psi\rangle\right)_{abxy} : \ |\psi\rangle \in \mathcal{H} \otimes \mathcal{H} \}$$

$$C_{com}(n,k) = \{ \left(\langle\psi| P_a^x Q_b^y |\psi\rangle\right)_{abxy} : \ |\psi\rangle \in \mathcal{H}, [P_a^x, Q_b^y] = 0 \}$$

[Slofstra '18]: $C_{\otimes} \neq C_{com}$

- Proof based on "universal embedding theorem":

  Finitely presented group $G, w \in G \ \mapsto$ functional λ_G on $\mathbb{R}^{n^2k^2}$ such that

  $\sup_{p \in C_{com}} |\lambda_G \cdot p| = 1$ and

a) $w \in G$ is non-trivial in *approximate* finite-dim. reps $\Leftrightarrow \exists p \in C_{\otimes}, |\lambda_G \cdot p| = 1$

b) $w \in G$ is non-trivial in finite-dim. representations $\Leftrightarrow \exists p \in C_{com}, |\lambda_G \cdot p| = 1$

- Byproduct: membership problem "is $p \in C_{\otimes}$?" is undecidable