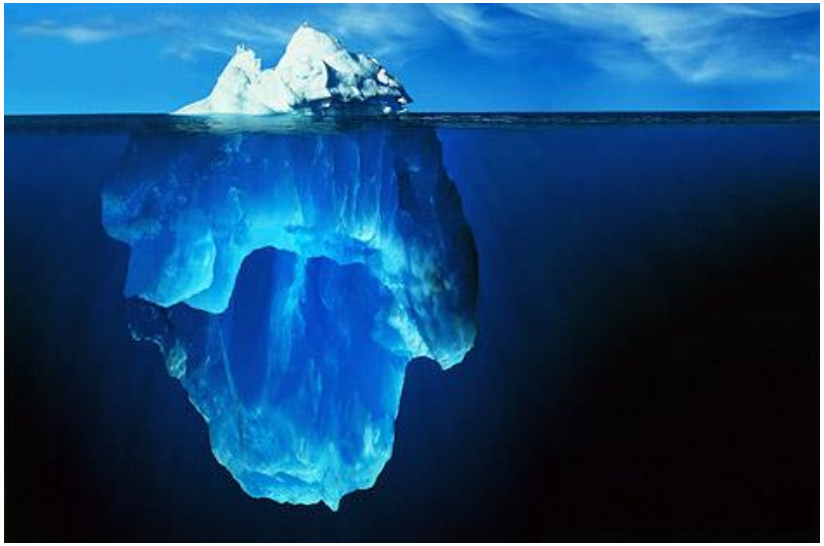
MIP* = RE

and

Tsirelson's problem



THOMAS VIDICK

CALIFORNIA INSTITUTE OF TECHNOLOGY

Joint work with

Zhengfeng Ji
(UTS)

Anand Natarajan
(MIT)

John Wright
(UT Austin)

Henry Yuen
(Columbia)

QIP 2008

QIP'08, Delhi

Hardness of Approximating
Entangled Games

Our Results

Entangled games are hard to approximate

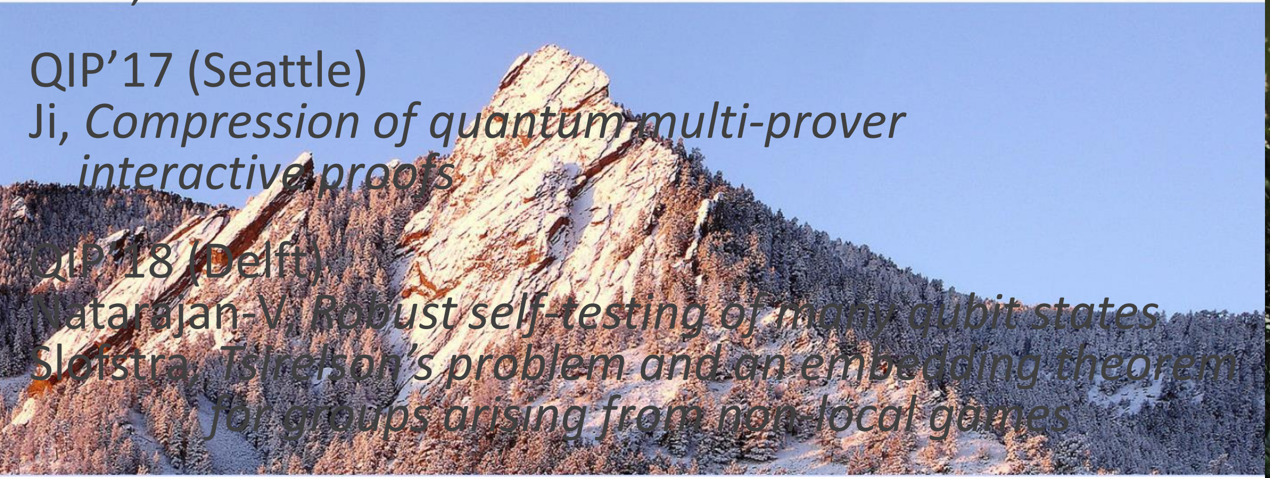
Our Results

Entangled games are hard(*er*) to approximate

QIP'04 (Waterloo)
Cleve-HTW, *Consequences and limits of nonlocal strategies*

QIP'11 (Singapore)
Fritz, *Tsirelson's problem and Kirchberg's conjecture*

QIP'13 (Beijing)
Ito-V, *NEXP in MIP**

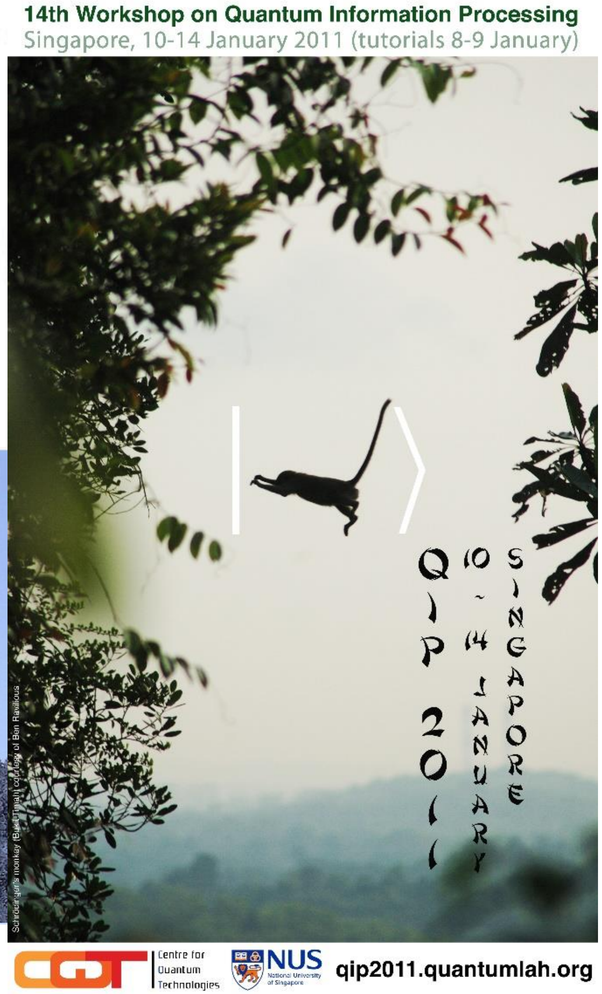


QIP'17 (Seattle)
Ji, *Compression of quantum multi-prover interactive proofs*

QIP'18 (Delft)
Natarajan-V, *Robust self-testing of many qubit states*
Slofstra, *Tsirelson's problem and an embedding theorem for groups arising from non-local games*

QIP'19 (Boulder)
Fitzsimons-JVY, *Quantum proof systems for iterated exponential time, and beyond*

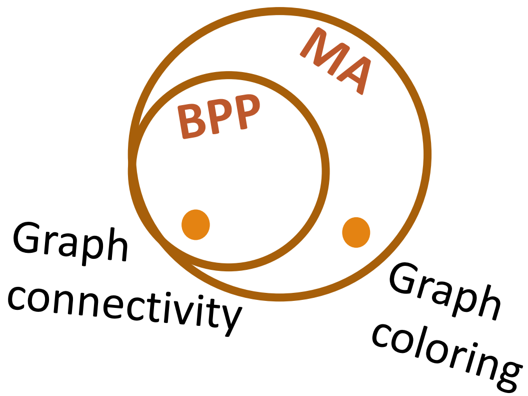
QIP'20 (Shenzhen)
Natarajan-W, *NEEXP in MIP**



MIP* = RE

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

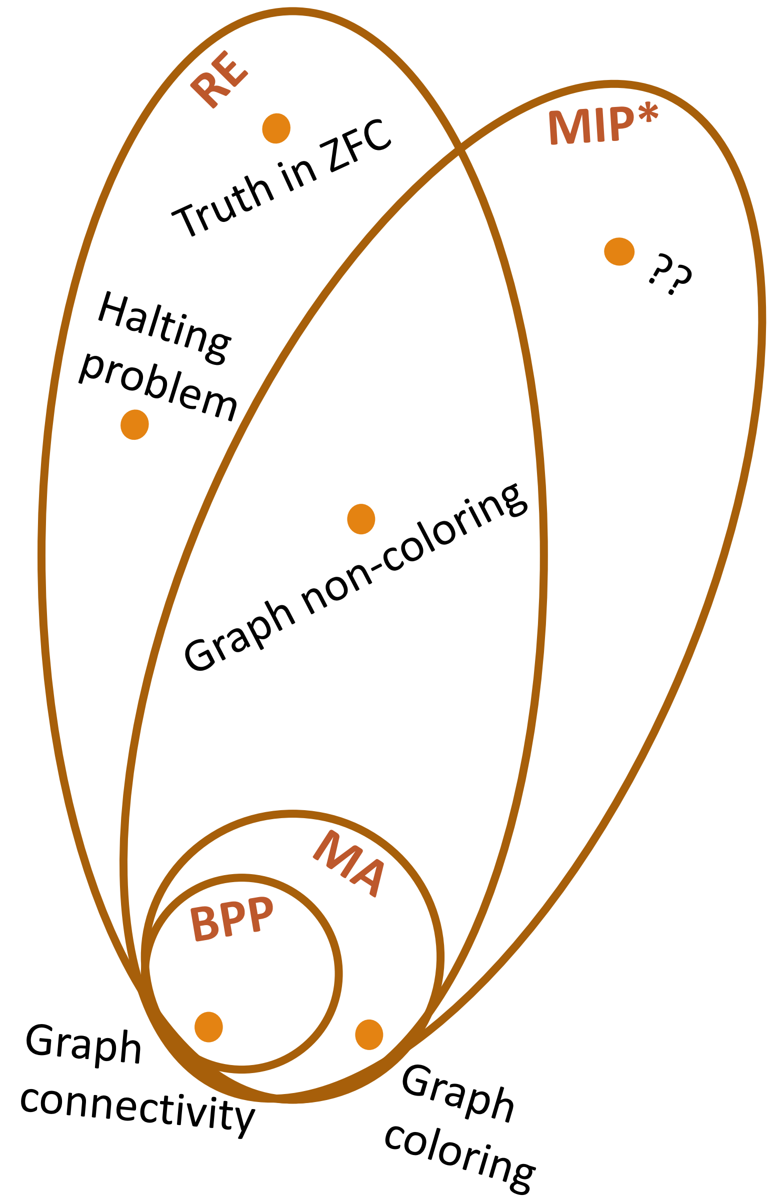
MA, QMA: Problems that can be *verified* in (randomized, quantum) polynomial time, given a polynomial-size proof



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

- ~~*NISQ systems*: provable advantage for small noisy quantum systems using deep variational quantum Boltzmann learning~~

Plan for the talk

1) Quantum correlations and Tsirelson's problem

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

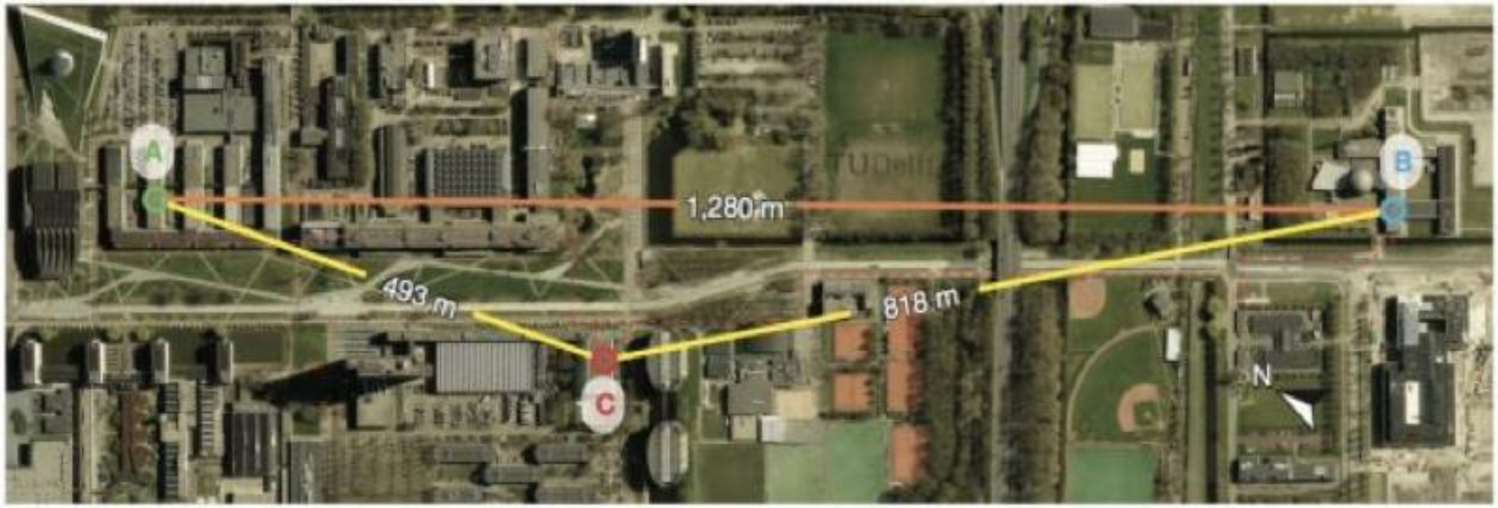
3) Quantum multiprover interactive proofs

4) Open questions

Quantum correlations and Tsirelson’s problem

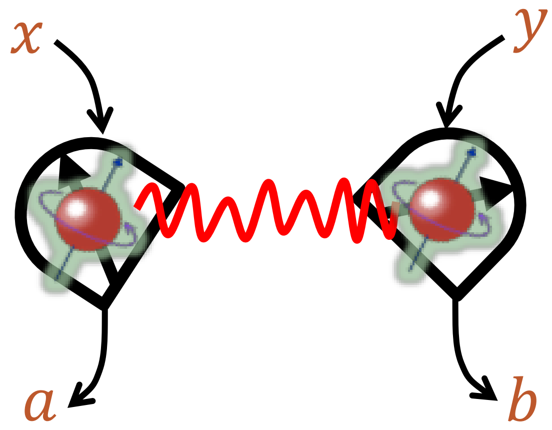
Quantum nonlocality

TU Delft, Netherlands (2015)



Local measurements on distant particles can exhibit unexpected correlations

Bell & Tsirelson's setup



- *Correlation*: family of distributions
  $\{\, p(a,b|x,y) \mid\ x,y \in \{1,\dots,n\}\ \ a,b \in \{1,\dots k\}\}$
- Bell'64: some correlations have a quantum model but no classical (LHV) explanation
- Tsirelson in the '80s introduces two possible representations for quantum correlations:

$$p(a,b|x,y) = \langle\psi|P_a^x \otimes Q_b^y|\psi\rangle : \quad |\psi\rangle \in \mathcal{H} \otimes \mathcal{H}$$

$$p(a,b|x,y) = \langle\psi|P_a^x Q_b^y|\psi\rangle : \quad |\psi\rangle \in \mathcal{H}, \quad [P_a^x, Q_b^y] = 0$$

Tsirelson's problem

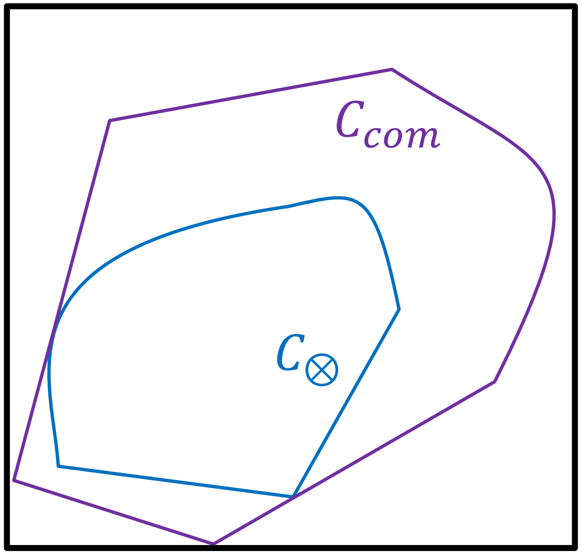
Quantum Bell-type inequalities are defined in terms of two (or more) subsystems of a quantum system. The subsystems may be treated either via (local) Hilbert spaces, - tensor factors of the given (global) Hilbert space, or via commuting (local) operator algebras. The latter approach is less restrictive,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

Are these two approaches equivalent?

Tsirelson's problem

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

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



$[0,1]^{n^2k^2}$

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

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

The connection with operator algebras

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

- [Kirchberg'93, Fritz'11, Junge-NPPSW'11, Ozawa'13]:

  Tsirelson's problem $\leftrightarrow$ CEP $\leftrightarrow$ QWEP

- Connes' 1976 "Embedding Problem" (CEP) :

  "Every type II_1 von Neumann algebra embeds in an ultrapower of the hyperfinite II_1 factor $\mathcal{R}$"

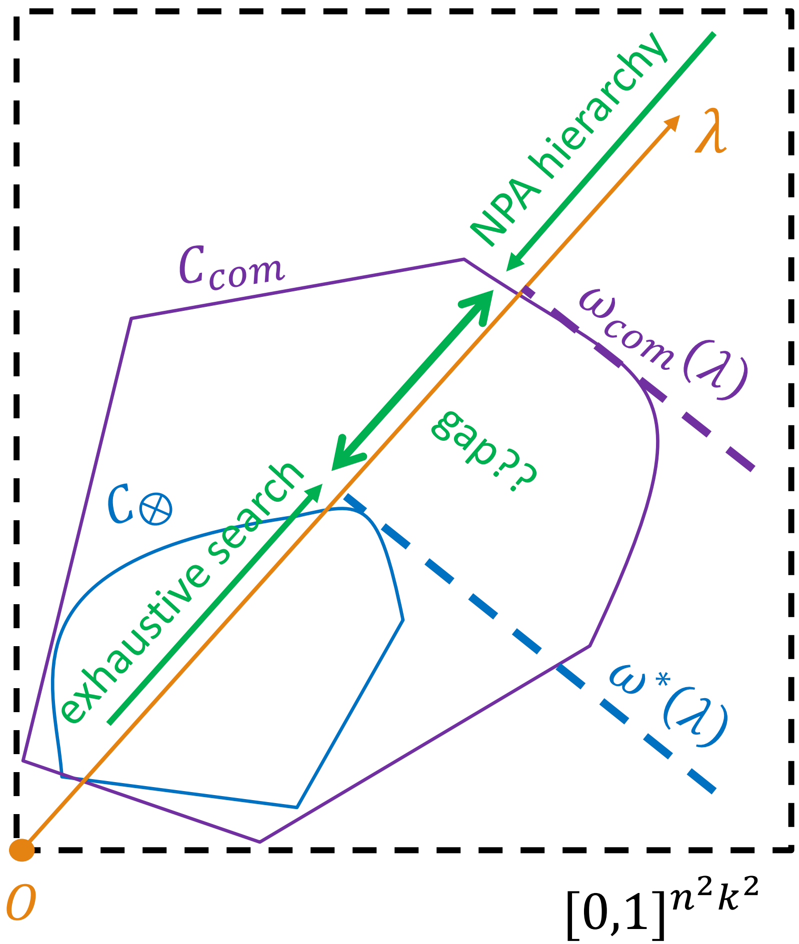
- Kirchberg's 1993 QWEP conjecture:

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

- Multiple reformulations: free entropy (Voiculescu), group theory (Radulescu), etc.

An approach to Tsirelson’s problem via algorithms & complexity

Computing the quantum bound



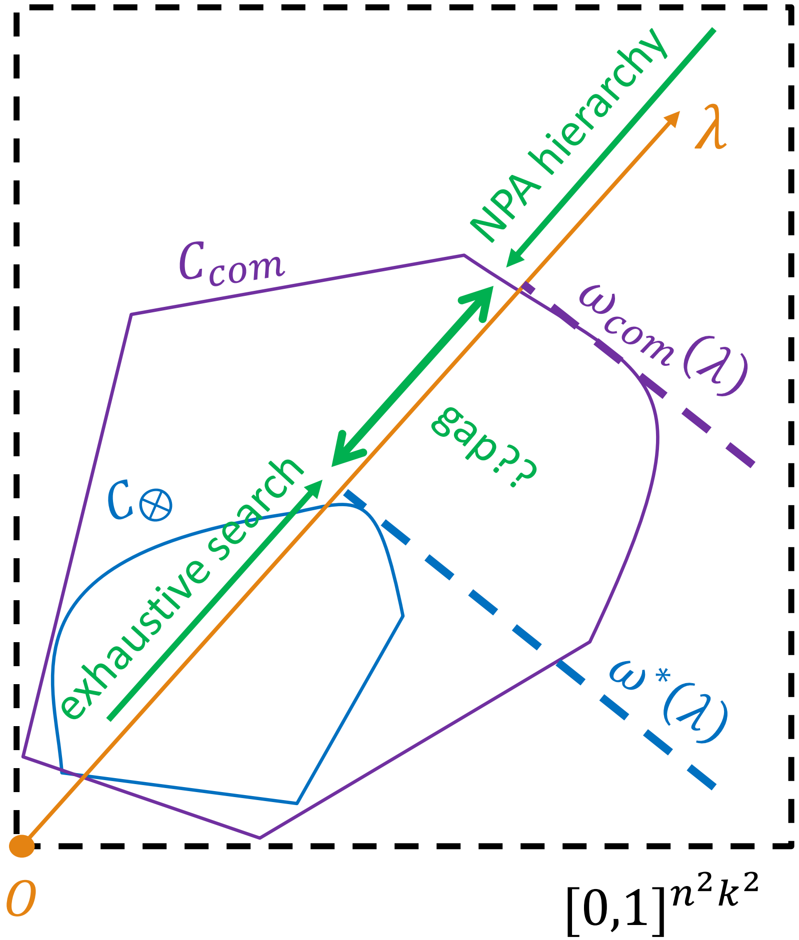
$$C_\otimes(n,k) = \{ \left(\langle\psi|P_a^x \otimes Q_b^y|\psi\rangle\right)_{abxy} : |\psi\rangle \in \mathcal{H} \otimes \mathcal{H} \}$$

$$\omega^*(\lambda) = \sup_{p \in C_\otimes(n,k)} |\lambda \cdot p| = \sup_{p \in C_\otimes(n,k)} \left| \sum_{xyab} \lambda_{xyab}\, p(a,b|x,y) \right|$$

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

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

Computing the quantum bound



- 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*

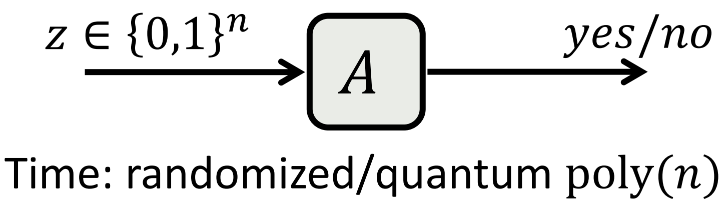
- [Fritz-NT'14] Suppose that $\omega^*(\lambda)$ is *uncomputable*

  → *Tsirelson's problem has a negative answer*

Quantum multiprover interactive proofs

Interactive proofs

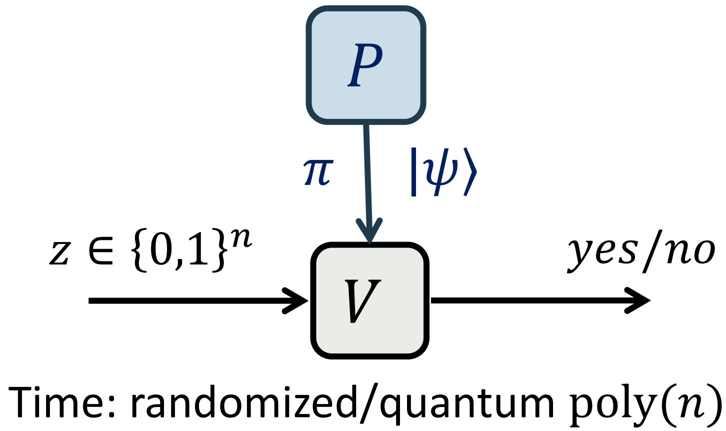
- **BPP/BQP**: efficient *decision*



- **MA/QMA**: efficient *verification*

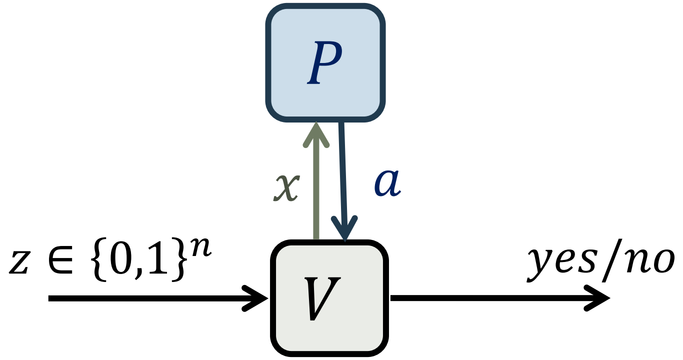
  z is "yes" ⇒ $\exists\, \pi$, accepted by V whp

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



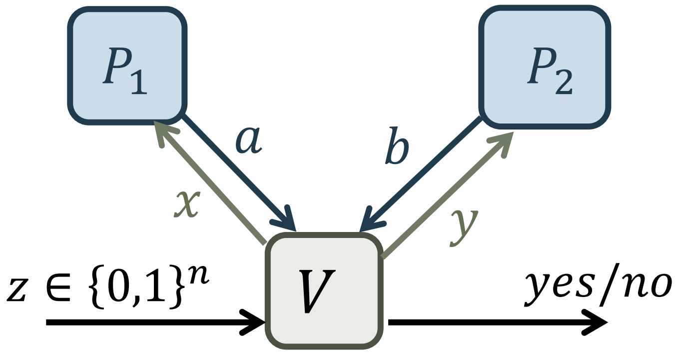
Interactive proofs

- **IP/QIP**: efficient *interactive verification*



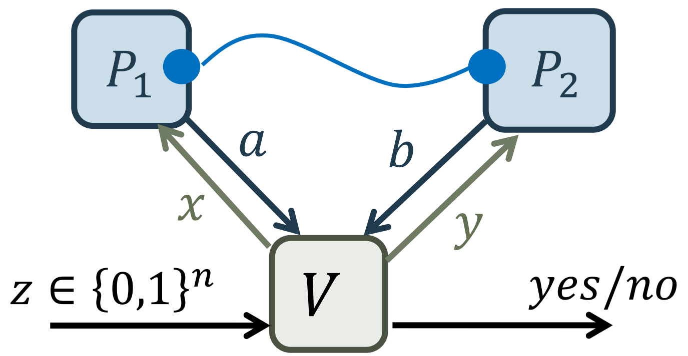
Time: randomized/quantum poly(n)

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



Time: randomized/quantum poly(n)

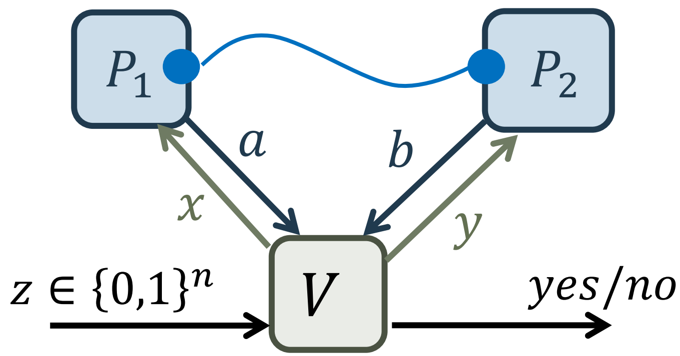
Interactive proof systems as Bell functionals



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

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

Interactive proof systems as Bell functionals

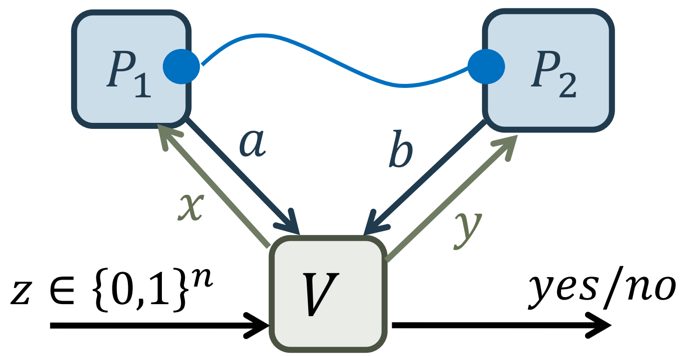


Max $\mathrm{acc}(V, z)$

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

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

Interactive proof systems as Bell functionals

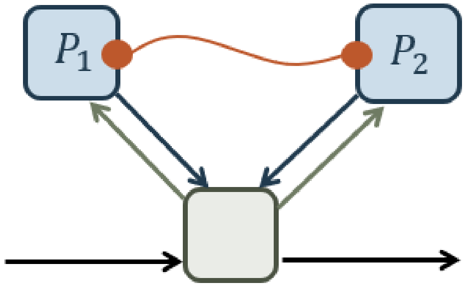


MIP*: problems that admit efficient *interactive verification with two provers sharing entanglement*

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

Using entanglement to delegate verification

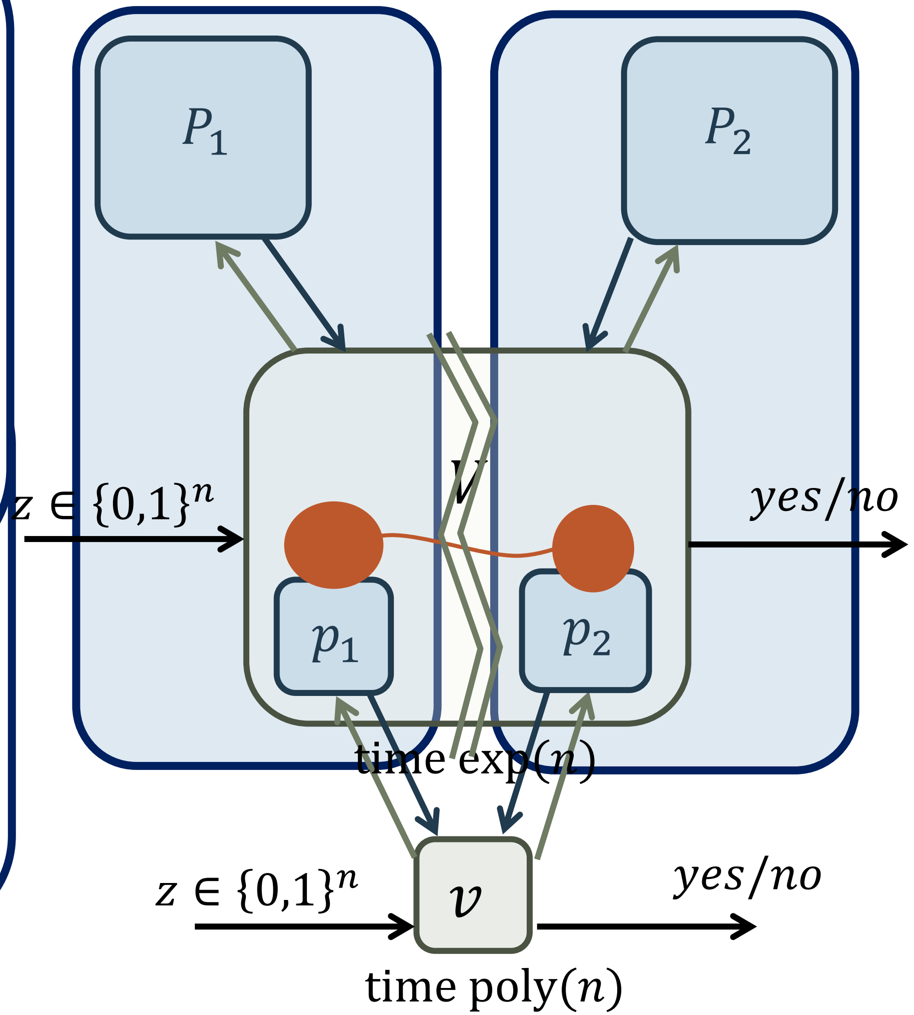
[Natarajan-W'19]

Probabilistically checkable proofs: p_1 and p_2 prepare encoded certificate that they performed the correct classical computation. v checks it efficiently by making small queries

Builds on [Arora-S'98, Harsha'04, Ben-Sasson-S'08,++]

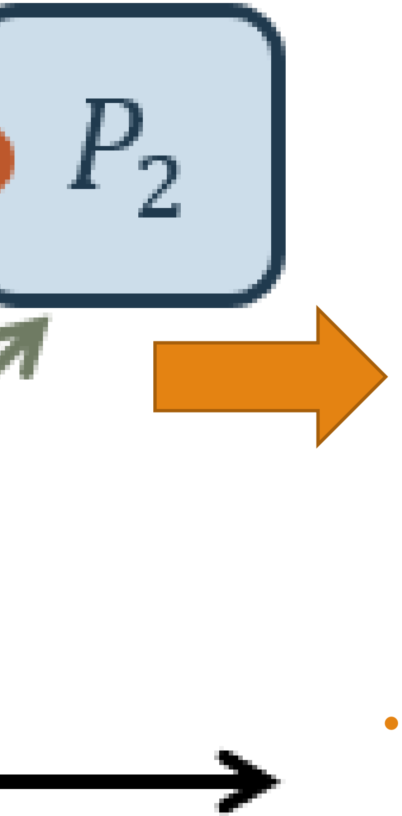
obtained exactly the right information, in the right way.

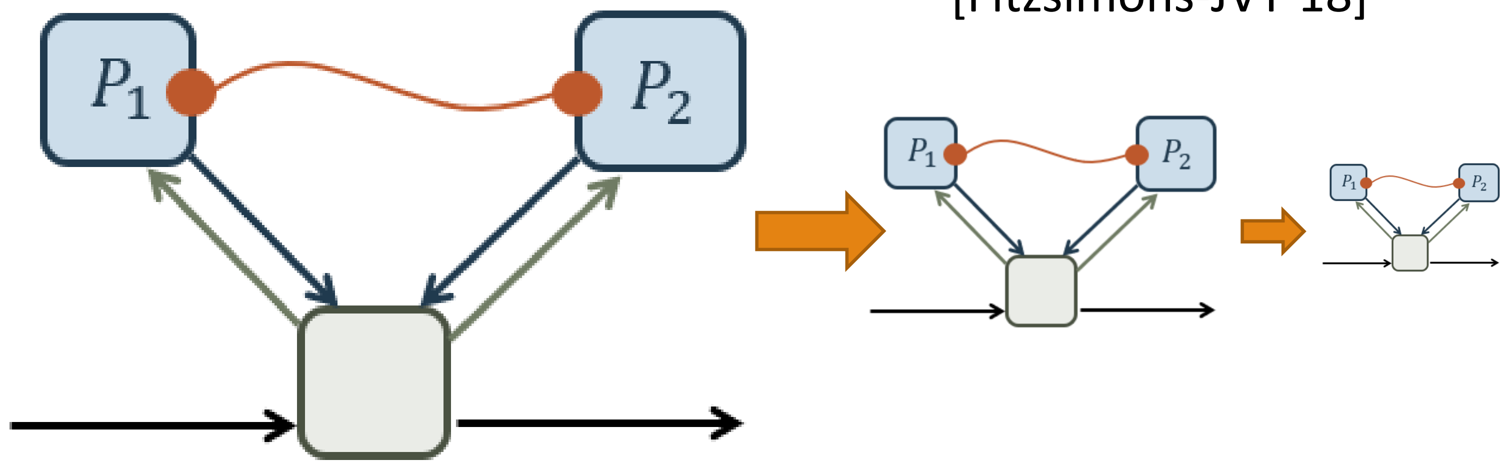
Builds on [Werner-S'88, Mayers-Yao'98, Natarajan-V'18,++]



Recursive compression

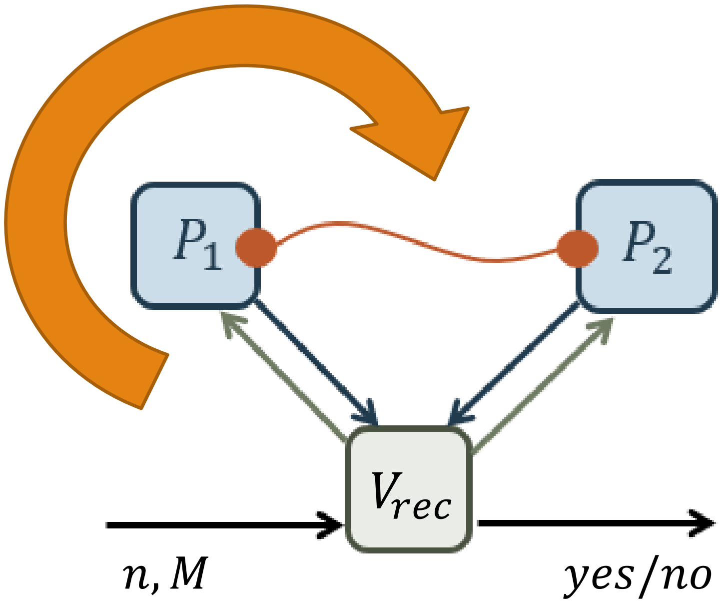
[Fitzsimons-JVY'18]





- Recursive construction yields polynomial-time verifiers for languages in NTIME(2^n), NTIME(2^{2^n}), NTIME($2^{2^{2^n}}$), …
- Main difficulty: identify a class of distributions $\mathcal{C}$ for the questions such that sampling from a distribution in $\mathcal{C}$ can be tested using a distribution in the same class $\mathcal{C}$
- Class $\mathcal{C}$ generalizes plane-point distribution from low-degree tests

The final step



For any Turing machine M, there is a *computable* $\lambda = \lambda(M)$ such that

- M halts $\rightarrow \omega^*(\lambda) = 1$
- M does not halt $\rightarrow \omega^*(\lambda) \leq \frac{1}{2}$

$\mathrm{RE} \subseteq \mathrm{MIP}^*$

Summary

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

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

- Tsirelson's problem: Is $\overline{C_{\otimes}(n,k)} = C_{com}(n,k)$ for all $n, k \geq 2$?
- We give a negative answer: $\overline{C_{\otimes}(n,k)} \neq C_{com}(n,k)$ for some n, 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

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

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 interesting "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

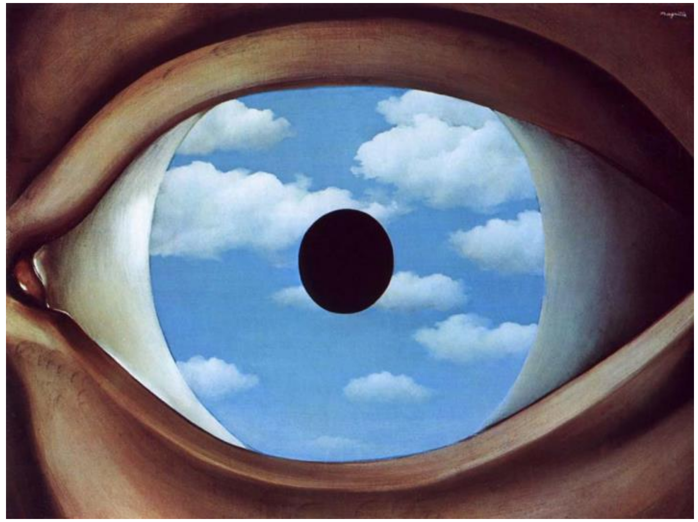
Some questions

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

Thank you

Caltech



IQIM
INSTITUTE FOR QUANTUM INFORMATION AND MATTER

Zhengfeng Ji
(UTS)

Anand Natarajan
(MIT)

John Wright
(UT Austin)

Henry Yuen
(Columbia)

References

[Babai-FL'91] Babai, László, Lance Fortnow, and Carsten Lund. "Non-deterministic exponential time has two-prover interactive protocols." Computational complexity 1.1 (1991): 3-40.

[Blum-K'89] Blum, Manuel, and Sampath Kannan. "Designing programs that check their work." Journal of the ACM (JACM) 42.1 (1995): 269-291.

[Blum-LR'93] Blum, Manuel, Michael Luby, and Ronitt Rubinfeld. "Self-testing/correcting with applications to numerical problems." Journal of computer and system sciences 47.3 (1993): 549-595.

[Cleve-HTW'04] Cleve, Richard, et al. "Consequences and limits of nonlocal strategies." Proceedings. 19th IEEE Annual Conference on Computational Complexity, 2004.. IEEE, 2004.

[Connes'76] Alain Connes. Classification of injective factors $II, II_\infty, III_\lambda, \lambda \neq 1$. Annals of Mathematics, pages 73–115, 1976

[Coudron-S'19] Coudron, M., & Slofstra, W. (2019). Complexity lower bounds for computing the approximately-commuting operator value of non-local games to high precision. arXiv preprint arXiv:1905.11635.

[Cubitt-PW'15] Cubitt, Toby S., David Perez-Garcia, and Michael M. Wolf. "Undecidability of the spectral gap." *Nature* 528.7581 (2015): 207-211.

[Fritz'12] Fritz, Tobias. "Tsirelson's problem and Kirchberg's conjecture." Reviews in Mathematical Physics 24.05 (2012): 1250012.

[Fritz-NT'14] Tobias Fritz, Tim Netzer, and Andreas Thom. "Can you compute the operator norm?" Proceedings of the American Mathematical Society, 142(12):4265–4276, 2014

References

[Jain-JUW’10] Jain, R., Ji, Z., Upadhyay, S., & Watrous, J. (2010). Qip= pspace. Communications of the ACM, 53(12), 102-109.

[Junge-NPPSW’11] Junge, Marius, et al. "Connes' embedding problem and Tsirelson's problem." Journal of Mathematical Physics 52.1 (2011): 012102.

[Kempe-KMTV’11] Kempe, J., Kobayashi, H., Matsumoto, K., Toner, B., & Vidick, T. (2011). Entangled games are hard to approximate. SIAM Journal on Computing, 40(3), 848-877.

[Kirchberg’93] Kirchberg, Eberhard. "On non-semisplit extensions, tensor products and exactness of group C*-algebras." Inventiones mathematicae 112.1 (1993): 449-489.

[Mousavi-NY’20] Mousavi, H., Nezhadi, S. S., & Yuen, H. (2020). On the complexity of zero gap MIP. arXiv preprint arXiv:2002.10490.

[Natarajan-W’19] Natarajan, A., & Wright, J. (2019, November). NEEXP is Contained in MIP. In 2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS) (pp. 510-518). IEEE.

[Osawa’13] Ozawa, Narutaka. "About the Connes embedding conjecture." Japanese Journal of Mathematics 8.1 (2013): 147-183.

[Slofstra’19] Slofstra, William. "The set of quantum correlations is not closed." Forum of Mathematics, Pi. Vol. 7. Cambridge University Press, 2019.

[Yao’19] Yao, P. (2019). A doubly exponential upper bound on noisy EPR states for binary games. arXiv preprint arXiv:1904.08832