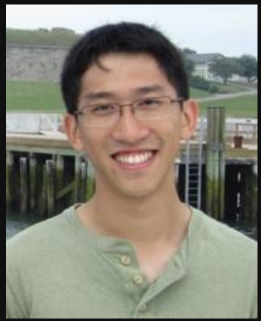
A Complexity-theoretic Solution to Connes' Embedding Problem

Zhengfeng Ji (UTS:QSI)

HIT IM Zoom Seminar, 6 July 2020

MIP* = RE

arXiv:2001.04383, 14 Jan 2020

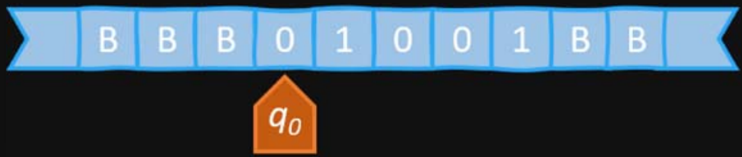
Complexity Theory

Turing Machines and the Halting Problem

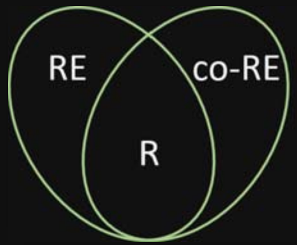
- Turing machine (1936)

> A Turing machine is a mathematical model of computation that defines an abstract machine, which manipulates symbols on a strip of tape according to a table of rules. (Wikipedia)

- The **halting problem** is the problem of determining, when given the description of a Turing machine, whether the machine halts on empty input



RE is the set of problems that can be reduced to the halting problem



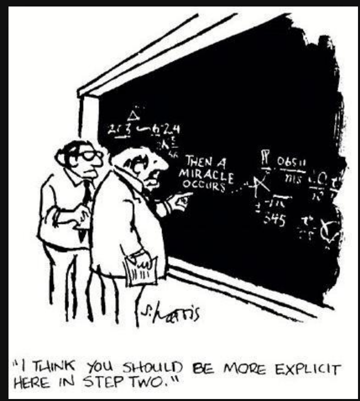
No algorithm can solve the halting problem

[Turing '36]

Nondeterminism and Proof Verification

- Nondeterministic Turing machines and proof verification
- What can a prover prove to a polynomial-time verifier?

  - NP = ?
- What can a prover prove to a verifier with interaction?



  - Known: IP = PSPACE!

    [Lund, Fortnow, Karloff and Nisan '90], [Shamir '92]
  - Arithmetisation

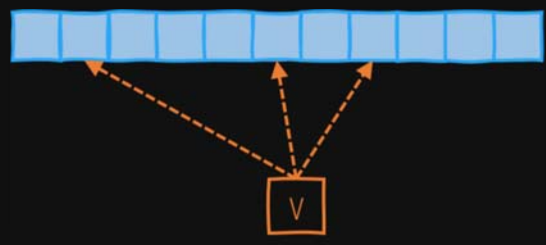
    From Boolean logic problems to problems of polynomials over (large) finite fields

    $f(x_1, x_2, \dots, x_m)$ has low-degree and vanishes on a subcube

Probabilistically Checkable Proofs (PCP)

- What can a prover prove to a verifier who flips r random coins and queries q bits from the proof?

PCP(r, q)



PCP Theorem. PCP$(O(\log n), O(1))$ = NP.

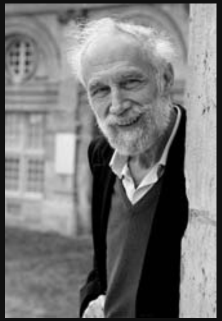
[Arora, Lund, Motwani, Sudan and Szegedy '92], [Arora and Safra '92]

- There is a format to write proofs so that if there is an error then errors are almost everywhere
- Multilinearity/low-degree tests: check if a function is close to or far from being a multilinear/low-degree polynomial

Tsirelson's Problem

Connes' Embedding Problem and Tsirelson's Problem

- Let ω be a free ultrafilter on the natural numbers and let R be the hyperfinite type II_1 factor. Can every type II_1 factor on a separable Hilbert space be embedded into some R^ω?
    - Kirchberg's QWEP conjecture in C*-algebra theory, Voiculescu's free entropy, Tsirelson's problem

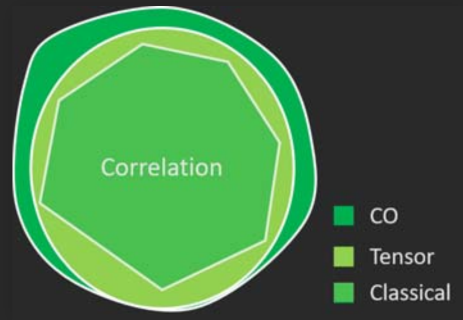


- Why does CEP have anything to do with complexity theory?

> *... and now it is called "Tsirelson's problem" (rather than "Tsirelson's error").*
>
> *— B. Tsirelson*

Correlation Sets

The correlation set $C_{\mathrm{q}}(r, s)$ for integers r and s is the set of points $p = (p_{xyab})$ in $\mathbb{R}^{r^2 s^2}$ where there are finite dimensional Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, a unit vector $\phi \in \mathcal{H}_A \otimes \mathcal{H}_B$, and POVMs $\{A_a^x\}$, $\{B_b^y\}$ such that for all $x, y \in \{1, 2, \ldots, r\}$, and $a, b \in \{1, 2, \ldots, s\}$, $p_{xyab} = \phi^*(A_a^x \otimes B_b^y)\phi$.



The correlation set $C_{\mathrm{qa}}(r, s)$ is the closure of $C_{\mathrm{q}}(r, s)$.

The correlation set $C_{\mathrm{qc}}(r, s)$ is the set of points $p = (p_{xyab})$ in $\mathbb{R}^{r^2 s^2}$ such that there is a separable Hilbert space $\mathcal{H}$, a unit vector $\phi \in \mathcal{H}$, POVMs $\{A_a^x\}$ and $\{B_b^y\}$ such that for all x, y, a, b, A_a^x and B_b^y commute and $p_{xyab} = \phi^* A_a^x B_b^y \phi$.

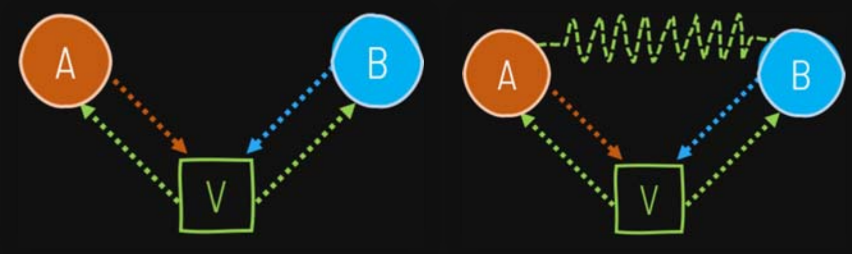
- $C_{\mathrm{loc}} \subsetneq C_{\mathrm{q}} \subsetneq C_{\mathrm{qa}} \subseteq C_{\mathrm{qc}}$

[Bell '64], [Solfstra '17]

- Tsirelson's problem: Does $C_{\mathrm{qa}} = C_{\mathrm{qc}}$?

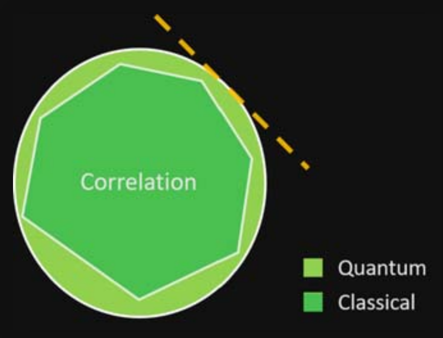
Nonlocal Games

- What can multiple provers prove to a verifier?
  - Known MIP = NEXP



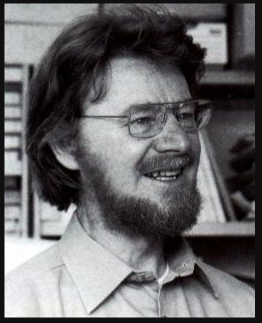
- What can multiple entangled provers prove to a verifier?
  - MIP* = ?

[Cleve, Høyer, Toner and Watrous '04]

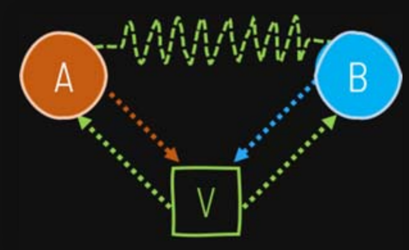


- Optimization over the correlation sets
- Connects multi-prover interactive proofs to Bell inequalities!

$$\langle A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1 \rangle \leq 2$$

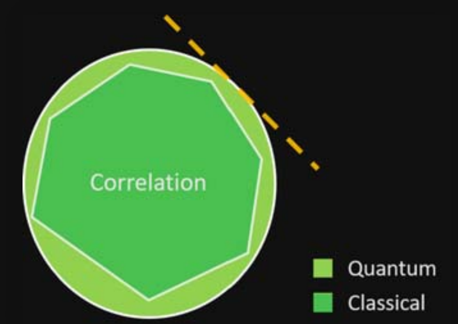


- Definition of a nonlocal game G
  - Finite question sets $\mathcal{X}$ and $\mathcal{Y}$ and answer sets $\mathcal{A}$ and $\mathcal{B}$
  - Question distribution μ over $\mathcal{X} \times \mathcal{Y}$
  - Decider $\mathcal{D} : \mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times B \to \{0, 1\}$



- Family of games defined by verifier $\mathcal{V} = (\mathcal{S}, \mathcal{D})$
  - Turing machine $\mathcal{S}$ takes input $(n, \ldots)$
  - Turing machine $\mathcal{D}$ takes input (n, x, y, a, b)
  - The n-th game $\mathcal{V}_n$ defined by $\mathcal{S}_n$ and $\mathcal{D}_n$

$(L^{\mathrm{A}}(z), L^{\mathrm{B}}(z))$

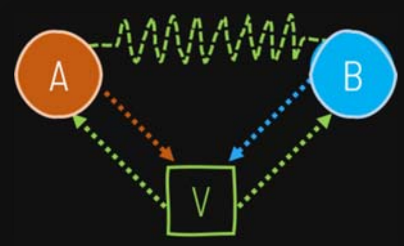


- A family of linear functionals on the correlation sets (for increasing r, s) from a pair of Turing machines

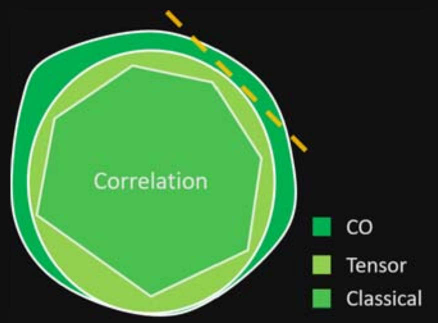
Entangled Value and Commuting Operator Value

- Value of p for a nonlocal game G

$$\mathrm{val}(G,p) = \mathop{\mathbb{E}}_{(x,y)\sim\mu} \sum_{a,b \text{ accepted by } \mathcal{D}_{x,y}} p_{xyab}$$



- Entangled value $\mathrm{val}^*(G) = \max_{p \in C_{\mathrm{qa}}} \mathrm{val}(G,p)$



- MIP* corresponds to the approximation of val^*
- Commuting-operator value

$$\mathrm{val}^{\mathrm{co}}(G) = \max_{p \in C_{\mathrm{qc}}} \mathrm{val}(G,p)$$

- If Tsirelson's problem has a positive answer, then val^* equal to $\mathrm{val}^{\mathrm{co}}$ for all games

Two Algorithms

- Algorithm 1: Exhaustively search for better tensor-product strategies of increasing Hilbert space dimensions and approximation precision

  A sequence of values approaching $\mathbf{val}^*$ from **below**

- Algorithm 2: NPA SDP hierarchy / Non-commutative Positivstellensatz

  [Navascués, Pironio, and Acín '08], [Doherty, Liang, Toner, and Wehner '08]
  [Helton and McCullough '04]

  A sequence of values approaching $\mathbf{val}^{\mathrm{co}}$ from **above**

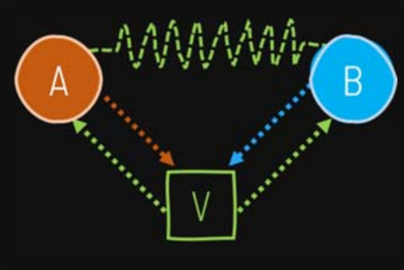
Algorithm 1 $\rightarrow$ $\mathbf{val}^* \leq \mathbf{val}^{\mathrm{co}}$ $\leftarrow$ Algorithm 2

- Algorithm 1 establishes that MIP* ⊆ RE
- Computability consequences of CEP and TP

  CEP true $\Longrightarrow$ TP true $\Longrightarrow$ an algorithm to approximate $\mathbf{val}^*$

Main Result and Implications

- MIP* = RE: no algorithm that approximate val^* because it is as hard as the halting problem

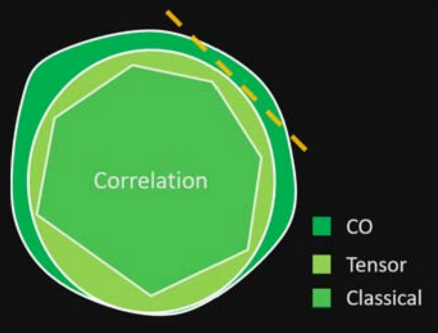


- A negative answer to Tsirelson's problem

  Infinite quantum systems cannot be approximated by finite ones

  $$C_{\mathrm{loc}} \subsetneq C_{\mathrm{qa}} \subsetneq C_{\mathrm{qc}}$$

  Could there be an experimental test for infinite dimensionality (like Bell tests for quantumness)?



- A negative answer to Connes' embedding problem via its known equivalence to Tsirelson's problem

  [Fritz '12], [Junge, Navascués, and Palazuelos et al. '11], [Ozawa '13]

Proof Overview

Compression Theorem

Compression Theorem. There is an algorithm $\mathrm{Compress}$ that on input $\mathcal{V} = (\mathcal{S}, \mathcal{D})$ outputs $\mathcal{V}^\sharp = (\mathcal{S}^\sharp, \mathcal{D}^\sharp)$ such that for all $n \geq n_0$

1. (Completeness). If $\mathrm{val}^*(\mathcal{V}_{2^n}) = 1$ then $\mathrm{val}^*(\mathcal{V}_n^\sharp) = 1$.
2. (Soundness). If $\mathrm{val}^*(\mathcal{V}_{2^n}) \leq \frac{1}{2}$ then $\mathrm{val}^*(\mathcal{V}_n^\sharp) \leq \frac{1}{2}$.
3. (Entanglement). $\mathcal{E}(\mathcal{V}_n^\sharp) \geq \max\{\mathcal{E}(\mathcal{V}_{2^n}), 2^n\}$.

Kleene's Recursion Theorem

- For all Turing machine $\mathcal{M}$, consider verifier $\mathcal{V}^{\text{Halt}}$

Turing machine $\mathcal{D}^{\text{Halt}}$:

1. Simulate $\mathcal{M}$ for n steps. If $\mathcal{M}$ halts, accept.
2. Compute $(\mathcal{S}^\sharp, \mathcal{D}^\sharp) = \text{Compress}(\mathcal{S}^\sharp, \mathcal{D}^{\text{Halt}})$.
3. Accept iff $\mathcal{D}^\sharp(n, x, y, a, b)$ accepts.

- Kleene's recursion theorem: $\mathcal{D}^{\text{Halt}}$ above is well-defined

MIP* Protocol for the Halting Problem

- For all Turing machine $\mathcal{M}$
    1. If $\mathcal{M}$ halts, then $\mathrm{val}^*(\mathcal{V}_{n_0}^{\mathrm{Halt}}) = 1$

       If the Turing machine $\mathcal{M}$ halts in T steps and $n < T \leq 2^n$, then by the compression theorem

$$\cdots = \mathrm{val}^*(\mathcal{V}_n^{\mathrm{Halt}}) = \mathrm{val}^*(\mathcal{V}_n^{\sharp}) = \mathrm{val}^*(\mathcal{V}_{2^n}^{\mathrm{Halt}}) = 1.$$

    2. If $\mathcal{M}$ does not halt, then $\mathrm{val}^*(\mathcal{V}_{n_0}^{\mathrm{Halt}}) \leq \frac{1}{2}$

       Entanglement $\mathcal{E}(\mathcal{V}_n^{\mathrm{Halt}}) = \mathcal{E}(\mathcal{V}_n^{\sharp}) \geq \mathcal{E}(\mathcal{V}_{2^n}^{\mathrm{Halt}}) \geq \cdots$

Turing machine $\mathcal{D}^{\mathrm{Halt}}$:

1. Simulate $\mathcal{M}$ for n steps. If $\mathcal{M}$ halts, accept.
2. Compute $(\mathcal{S}^{\sharp}, \mathcal{D}^{\sharp}) = \mathrm{Compress}(\mathcal{S}^{\sharp}, \mathcal{D}^{\mathrm{Halt}})$.
3. Accept iff $\mathcal{D}^{\sharp}(n, x, y, a, b)$ accepts.

Explicit Separation Between C_{qa} and C_{qc}

- Consider verifier $\mathcal{V}^{\mathrm{Sep}} = (\mathcal{S}^{\sharp}, \mathcal{D}^{\mathrm{Sep}})$

Turing machine $\mathcal{D}^{\mathrm{Sep}}$:

1. Compute a description of game $\mathcal{V}^{\mathrm{Sep}}_{n_0}$.
2. Run NPA on $\mathcal{V}^{\mathrm{Sep}}_{n_0}$ for n steps. If NPA halts, then accept.
3. Compute $(\mathcal{S}^{\sharp}, \mathcal{D}^{\sharp}) = \mathrm{Compress}(\mathcal{S}^{\sharp}, \mathcal{D}^{\mathrm{Sep}})$.
4. Accept iff $\mathcal{D}^{\sharp}(n, x, y, a, b)$ accepts.

- Claim: $\mathrm{val}^*(\mathcal{V}^{\mathrm{Sep}}_{n_0}) \leq \frac{1}{2}$ and $\mathrm{val}^{\mathrm{co}}(\mathcal{V}^{\mathrm{Sep}}_{n_0}) = 1$
- If $\mathrm{val}^{\mathrm{co}}(\mathcal{V}^{\mathrm{Sep}}_{n_0}) < 1$, then $\mathrm{val}^*(\mathcal{V}^{\mathrm{Sep}}_{n_0}) = 1$, a contradiction

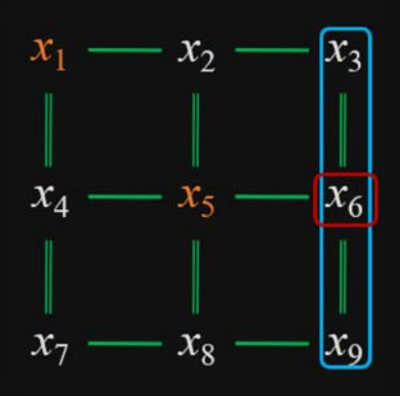
Proof Techniques

Rigidity and Self-testing

- The players have to measure the honest measurement to achieve a near-optimal value

  From $\mathbf{val}^*$ to $(|\psi\rangle, \{A_a^x\}, \{B_b^y\})$

- Magic square game



> Send Alice a row or a column, send Bob a variable in it; accept if
>
> 1. the row/column constraint is satisfied, and
> 2. Alice and Bob's answers are consistent

$$|\mathrm{EPR}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

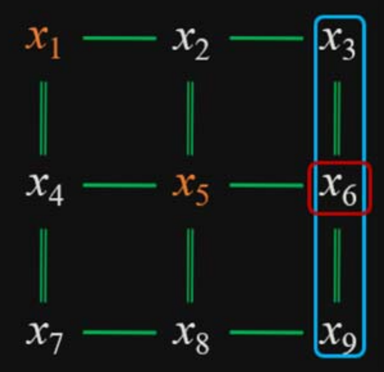
$$\sigma^X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\sigma^Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- The entangled value $\mathbf{val}^*(G_{\boxplus}) = 1$

$$X_1 = \sigma^X \otimes I, \ldots, X_5 = \sigma^Z \otimes I, \ldots, |\psi\rangle = |\mathrm{EPR}\rangle^{\otimes 2}$$

- The rigidity of the magic square game: all about commutativity and anticommutativity



If the value of a strategy is at least $1-\varepsilon$, then $X_1 X_5 \approx_{\sqrt{\epsilon}} -X_5 X_1$.

Let R_0, R_1 be two observables, if $R_0 R_1 \approx -R_1 R_0$, then there is a local isomorphism ϕ such that up to the isomorphism

$$R_0 \approx \sigma^X \otimes I, \quad R_1 \approx \sigma^Z \otimes I.$$

- Approximate representation of the group generated by σ^X and σ^Z
- Inverse and stability theorems for approximate representations of finite groups

[Gowers and Hatami '15]

Efficient Self-test for Multiple Qubits

- Pauli basis game: rigidity + low-degree test

[Natarajan and Vidick '18], [Natarajan and Wright '19]

Rigidity Theorem. For any strategy that uses measurement $\hat{A}^{\text{Pauli},W}$ for the question (Pauli, W) and has value at least $1-\varepsilon$, there is a local isomorphism $\phi = \phi_A \otimes \phi_B$ such that

$$A_z^{\text{Pauli},W} \otimes I_B \approx_{\delta(\varepsilon)} \sigma_z^W \otimes I_B,$$

where $A_z^{\text{Pauli},W} = \phi_A \hat{A}^{\text{Pauli},W} \phi_A^*$.

- An efficient self-test for Pauli X/Z measurements on EPRs

  For self-testing of n EPRs, the questions have length $\text{polylog}(n)$

Four Steps of Compression

1. Introspection

   Question reduction

2. Oracularisation

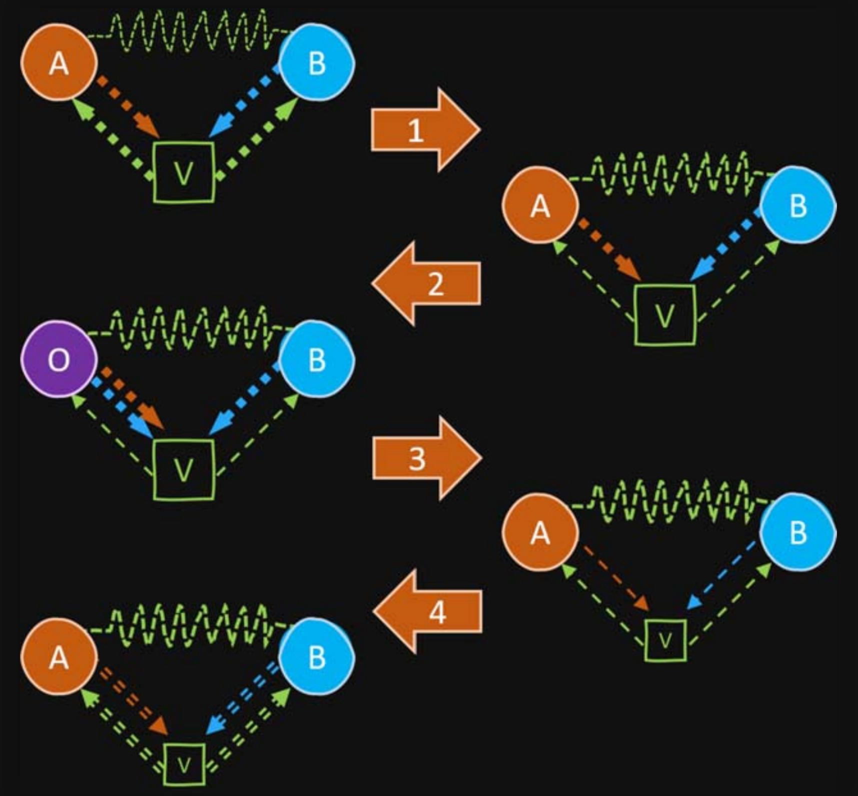
   Preprocessing for PCP

3. PCP

   Answer reduction

4. Parallel repetition

   Gap recovery



Introspection + PCP

Verifier: I am lazy. How about you two come up with the questions yourselves, answer them, and prove to me that I would have accepted the questions and answers?

Provers: What?!

[Natarajan and Wright '19]

Introspection

- Let L^A and L^B be functions such that $(L^A(z), L^B(z))$ is the question distribution μ for z the σ^Z measurement outcome on EPRs

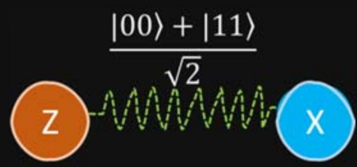
Desirable situation: Verifier simply sends (Intro, A) to Alice and (Intro, B) to Bob

The player receiving (Intro, v) replies (y, a) where for $v \in \{A, B\}$

1. the introspectively sampled question y is supposedly $L^v(z)$ and,
2. a is the answer in the original game for question y

- Why would the provers follow the commands?

Control the information that the provers can and cannot see using the Pauli basis game and Heisenberg uncertainty



Answer Reduction Using PCPs

- Basic idea

  The verifier needs to check if $\mathcal{D}(n, x, y, a, b)$ accepts

  Verifier: "Do not send me the long answers a, b, please compute a probabilistically checkable proof for the fact that $\mathcal{D}(n, x, y, a, b)$ accepts"

Recursive Gap-preserving Compression

Turing machine $\mathcal{D}^{\text{Halt}}$:

1. Simulate $\mathcal{M}$ for n steps. If $\mathcal{M}$ halts, accept.
2. Compute $(\mathcal{S}^\sharp, \mathcal{D}^\sharp) = \text{Compress}(\mathcal{S}^\sharp, \mathcal{D}^{\text{Halt}})$.
3. Accept iff $\mathcal{D}^\sharp(n, x, y, a, b)$ accepts.

$\mathcal{S}^\sharp$ is universal

- Two problems are important
  1. What kind of distributions/functions can be introspectively sampled
  2. What is the distribution of the compressed game

$(L^{\text{A}}(z), L^{\text{B}}(z))$

- Match the two?
- Conditionally linear distributions and normal-form nonlocal games

Conclusions

- Recursive gap-preserving compression of two-prover one-round protocols
- Compression theorem + Kleene's recursion theorem prove $\mathrm{RE} \subseteq \mathrm{MIP}^*$
- $\mathrm{MIP}^* = \mathrm{RE}$ follows as $\mathrm{MIP}^* \subseteq \mathrm{RE}$
- Negative answers to both Tsirelson's problem and CEP
- Open problems:
    1. Simpler proofs?
    2. Does $\mathrm{MIP}^{co} = \mathrm{coRE}$?
    3. Explicit counter-examples to CEP

Physics

- 1935 EPR paradox, entanglement
- 1964 Bell inequality
- 1990's Tsirelson's problem

Computer Science

- 1936 Turing's Halting problem
- 1970's Complexity theory
- 1990's PCP theorem

Mathematics

- 1930 von Neumann algebra
- 1976 Connes
- 1993 Kirchberg

MIP* = RE

Thank you!

Sydney Quantum Academy (SQA) PhD Scholarships

- The SQA Primary PhD Scholarship provides a stipend of $35,000 per annum AUD for a maximum duration of four years. Student tuition fees will be waived for successful international applicants.
- For more information, see

  SQA: https://www.sydneyquantum.org/research/phd-scholarships

  UTS: https://qsi.uts.edu.au