MIP* = RE

Hyungmin Lim
School of EE, Yonsei Univ.

QISCA Quantum Complexity Theory
2025. 11. 15

What we’ve reviewed

- The Complexity of NISQ
- Models of quantum Complexity growth
- The Acrobatics of BQP
- NEEXP in MIP*

The complexity structure so far

Definition 1.19 (The class **DTIME**.)
Let $T : \mathbb{N} \to \mathbb{N}$ be some function. We let $\mathbf{DTIME}(T(n))$ be the set of all Boolean (one bit output) functions that are computable in $c \cdot T(n)$-time for some constant $c > 0$.

The following class will serve as our rough approximation for the class of decision problems that are efficiently solvable.

Definition 1.20 (The class **P**)
$\mathbf{P} = \cup_{c \geq 1} \mathbf{DTIME}(n^c)$

The complexity structure so far

2.1.2 Non-deterministic Turing machines.

The class **NP** can also be defined using a variant of Turing machines called *non-deterministic* Turing machines (abbreviated NDTM). In fact, this was the original definition and the reason for the name **NP**, which stands for *non-deterministic polynomial-time*. The only difference between an NDTM and a standard TM is that an NDTM has *two* transition functions δ_0 and δ_1. In addition

DEFINITION 2.5
For every function $T : \mathbb{N} \to \mathbb{N}$ and $L \subseteq \{0,1\}^*$, we say that $L \in \mathbf{NTIME}(T(n))$ if there is a constant $c > 0$ and a $cT(n)$-time NDTM M such that for every $x \in \{0,1\}^*$, $x \in L \Leftrightarrow M(x) = 1$

The next theorem gives an alternative definition of **NP**, the one that appears in most texts.

THEOREM 2.6
$\mathbf{NP} = \cup_{c \in \mathbb{N}} \mathbf{NTIME}(n^c)$

The complexity structure so far

- $\mathbf{P} \subseteq \mathbf{NP} \subseteq \mathbf{MA} \subseteq \mathbf{AM} \subseteq \mathbf{QAM} \subseteq \mathbf{PSPACE} \subseteq \mathbf{QIP} \subseteq \mathbf{EXP} \subseteq \mathbf{NEXP}$
- $\mathbf{NEEXP} \subseteq \mathbf{MIP}^*$

- **EXP :** ∃ deterministic TM M running in **exponential time** that accepts $\forall x \in A_{yes}$ and rejects $\forall x \in A_{no}$
- **NEXP :** ∃ **non-deterministic** TM M running in **exponential time** that accepts $\forall x \in A_{yes}$ and rejects $\forall x \in A_{no}$
- **NEEXP** = NTIME[exp(exp(poly(n))]

What is RE?

- **RE** stands for **Recursively Enumerable**.
- A problem is in **RE** if there exists a Turing machine (which we can think of as an algorithm) with the following properties:
  - If the answer is "YES": The machine is guaranteed to halt and output "YES" in a finite amount of time.
  - If the answer is "NO": The machine might halt and output "NO," or it might loop forever.
- This type of algorithm is called a **recognizer** or a **semi-algorithm**. It can confirm "YES" instances, but it isn't required to definitively identify "NO" instances (it's allowed to just never give an answer).

The Halting Problem

- Function **HALT**$(\alpha, x) = 1$ $\Leftrightarrow$ the TM M_α represented by α halts on input x within a finite number of steps.
- In 1936, Alan Turing proved that the Halting Problem is undecidable.

THEOREM 1.17
HALT *is not computable by any TM.*

Alan Turing
(1912~1954)

The Halting Problem is RE-complete

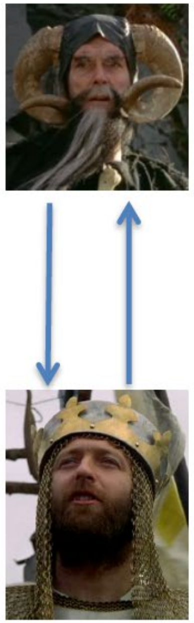
Lemma 12.8. *The Halting Problem is complete for* RE *via Karp reductions.*[36]

Proof. To see that the Halting Problem is in RE, define $\mathcal{M}$ to take as input an x that represents a Turing machine $\mathcal{N} = [x]$, and runs the universal Turing machine to simulate $\mathcal{N}$ on the empty input; if $\mathcal{N}$ halts with a 1 then so does $\mathcal{M}$.

To show that the Halting problem is complete for RE, let $L \in \mathsf{RE}$ and $\mathcal{M}$ a Turing machine such that if $x \in L$, then $\mathcal{M}(x)$ halts and outputs 1. For an input x, let $\mathcal{N}_x$ be the following Turing machine. $\mathcal{N}_x$ first runs $\mathcal{M}$ on input x. If $\mathcal{M}$ accepts, then $\mathcal{N}_x$ accepts. On all other outcomes, $\mathcal{N}_x$ goes into an infinite loop. Thus $\mathcal{N}_x$ halts if and only if $x \in L$. $\square$

Interactive proofs

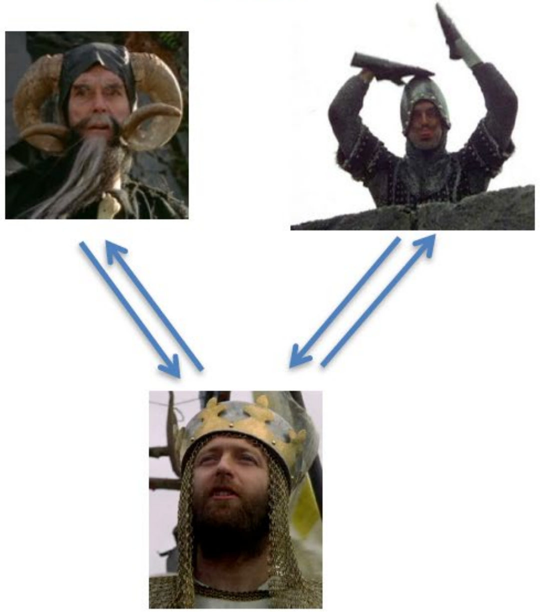
IP



= PSPACE

[Shamir ‘90]

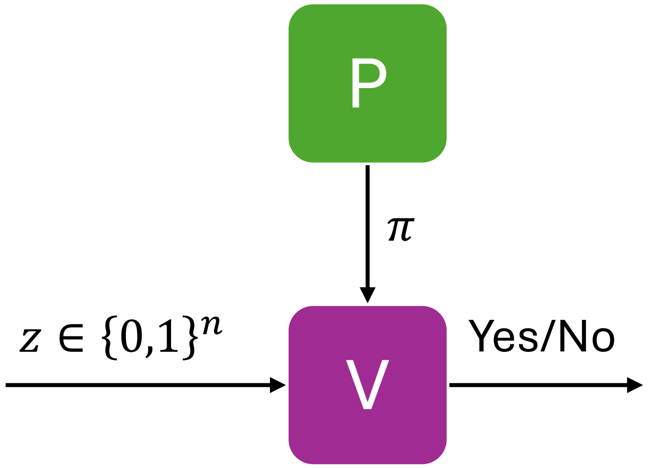
MIP



= NEXP

[BFL ‘91]

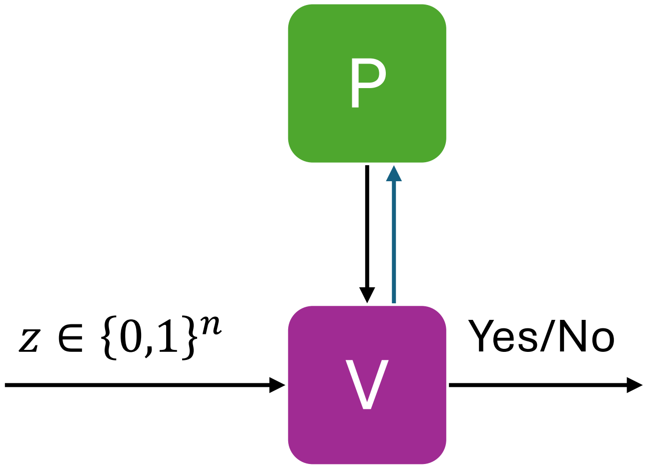
The classical complexity of verification



Deterministic time poly(n)

NP

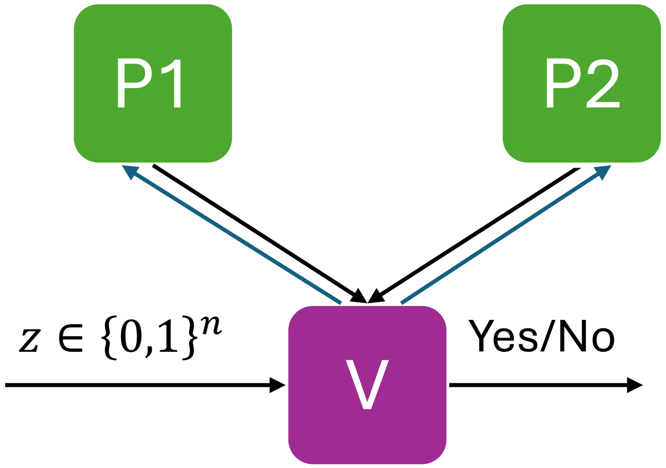
Cook-Levin:
3SAT is NP-complete
Graph coloring,
Hamiltonicity, …



Randomized time poly(n)

IP = PSPACE

Babai/GMR’85
Group membership
Zero-knowledge
#SAT



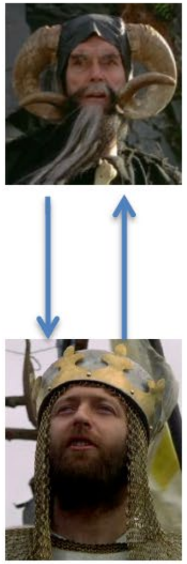
Randomized time poly(n)

MIP = NEXP

PCP theorem
Hardness of approximation
Delegated computation

Quantum Interactive proofs

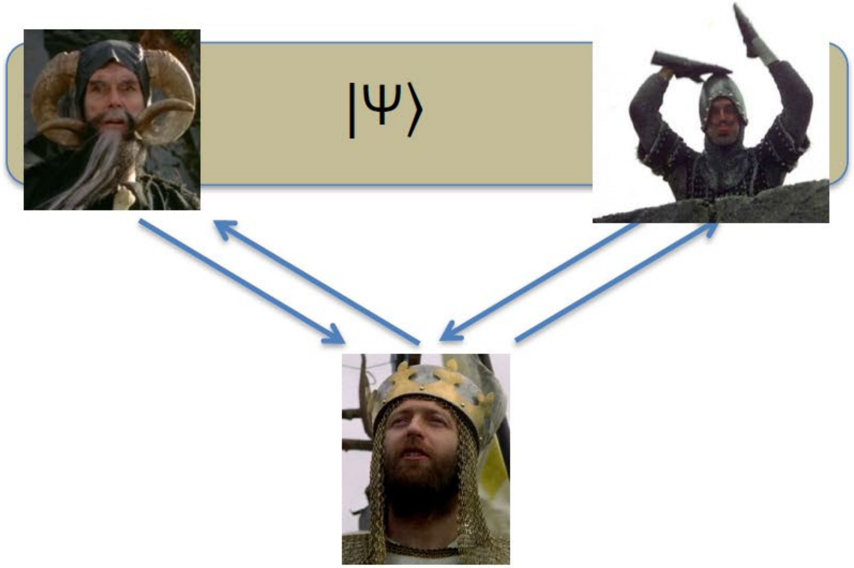
QIP



Still = PSPACE !

[JJUW'09]

MIP*



- $|\Psi\rangle$ is finite-dim but arbitrarily big
- Contained in RE (search over all $|\Psi\rangle$)
- Obviously, $\mathbf{MIP}^* \subseteq \mathbf{RE}$

MIP* and QMIP

- **NEEXP $\subseteq$ MIP* $\subseteq$ QMIP**

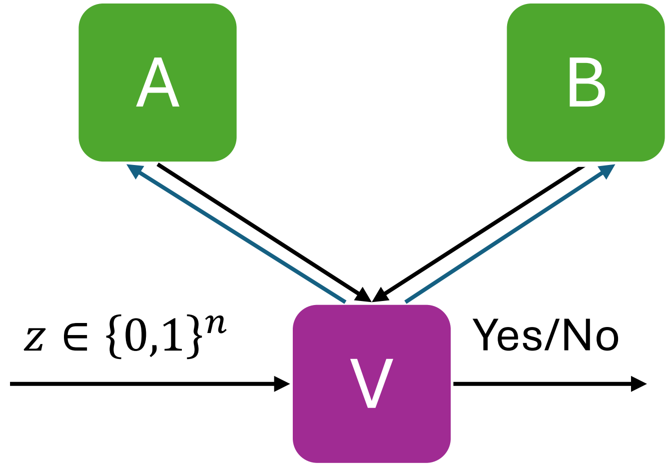
MIP* A promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ is in MIP* if and only if there exists a multiple-prover interactive proof system for A wherein the verifier is classical and the provers may share an arbitrary entangled state.

One may also consider fully quantum variants of multiple-prover interactive proofs, which were first studied by Kobayashi and Matsumoto [73].

QMIP A promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ is in QMIP if and only if there exists a multiple-prover quantum interactive proof system for A.

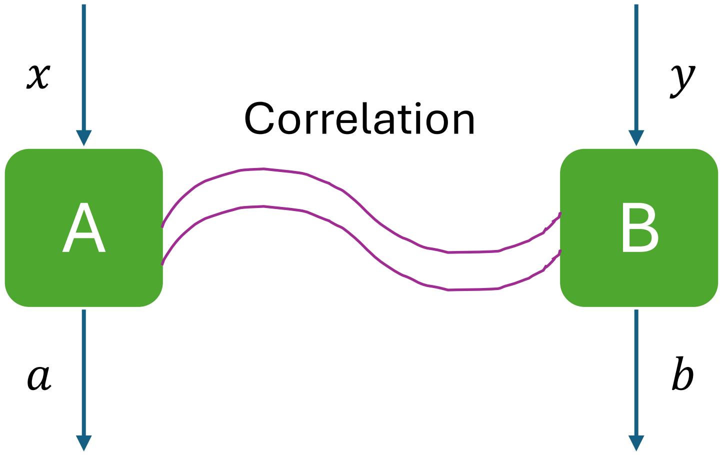
The power of quantum interactive proofs

- How to delegate a computation?
  Encode tableau in ECC and do random local checks
- How to delegate an interactive proof?
  Receive & check answers: deterministic
  Sample questions: needs a random seed!
- Idea: Use “quantumness” no certify randomness generation
  Ekert’91 “Quantum Cryptography based on Bell’s theorem”

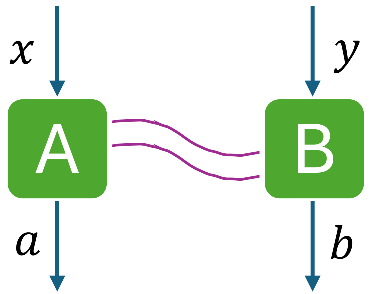


Correlations

- Two separated systems receive inputs $x, y \in [n]$, and produce outputs $a, b \in [k]$.
- A (n, k)-correlation is conditional probability $p(a, b|x, y)$ describing the joint behavior of the two systems.
- Correlations represented as vectors in $[0,1]^{n^2k^2}$



Quantum Correlations

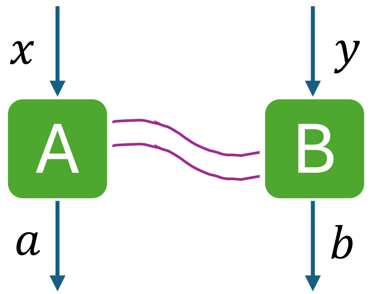


- $p(a,b|x,y)$ is **quantum** if $p(a,b|x,y) = \langle\psi|A_{x,a} \otimes B_{y,b}\,|\psi\rangle$ where

- Unit vector $|\psi\rangle \in H_A \otimes H_B$
- Finite dimension Hilbert space H_A, H_B
- Positive operators $\{A_{x,a}\}$ acting on $\{B_{y,b}\}$ acting on H_B
  - For all x, $\sum_a A_{x,a} = I$
  - For all y, $\sum_b B_{y,b} = I$

$C_q(n,k) \coloneqq$ quantum correlation set $\subseteq$ $C_{qa}(n,k) \coloneqq$ closure of $C_q(n,k)$ (approximately finite dimensional)

Quantum Commuting Correlations



- $p(a,b|x,y)$ is **quantum commuting** if $p(a,b|x,y) = \langle\psi|A_{x,a} \cdot B_{y,b}\,|\psi\rangle$ where

- Unit vector $|\psi\rangle \in H$
- Hilbert space H (possibly infinite dimensional)
- POVMs $\{A_{x,a}\}, \{B_{y,b}\}$ acting on H
  - Where $[A_{x,a}, B_{y,b}] = 0$ for all x, y, a, b

Tensor product structure not a priori present in general Quantum Field Theory

$C_{qc}(n,k)$:= quantum commuting correlation set

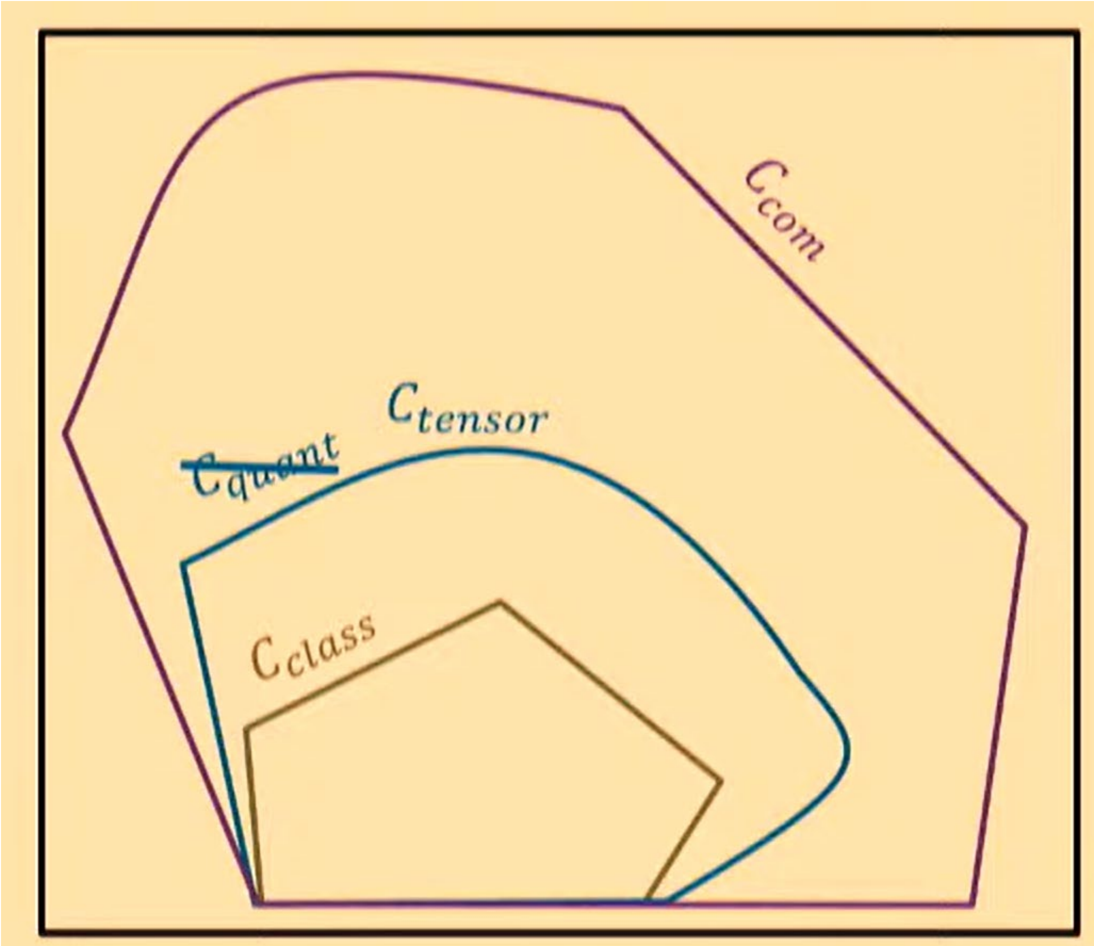
Finite dim | Aprrox finite dim | Commuting operator

$$\mathrm{C_q} \quad \subseteq \quad \mathrm{C_{qa}} \quad \subseteq \quad \mathrm{C_{qc}}$$

Boris Tsirelson

- Slofstra 2017: $\mathrm{C_q} \neq C_{qa}$. Quantum correlation are not closed.
- Tsirelson's problem: $C_{qa} = C_{qc}$?
  - i.e. can every infinite dimensional commuting operator correlation be approximated in finite dimensions?
  - Note : finite dim commuting operator correlations are also tensor product correlations.
- Conclusion : There is a gap between them. MIP* = RE implies it.

Diagram of Tsirelson's problem



$p(a, b|x, y) \subseteq [0,1]^{n^2k^2}$

The connection with operator algebras

- In 1932, von Neumann pup Quantum Mechanics on a firm mathematical basis
  - Quantum state = vector in a complex Hilbert space
  - Measurement = bounded linear operator on that space
- 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
- In 1976 paper, Conne suggested conjecture named Connes' Embedding Problem

The connection with operator algebras

- Connes' Embedding Problem is roughly speaking, can every finite subset of a II_1 factor be approximately embedded in the finite-dimensional matrices?
- In 1993, Kirchberg proved that QWEP Conjecture is equivalent to Connes' embedding conjecture
- Firtz, Junge et al., Ozawa '11 : Connes' embedding conjecture and Tsirelson's problem are equivalent.

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.

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

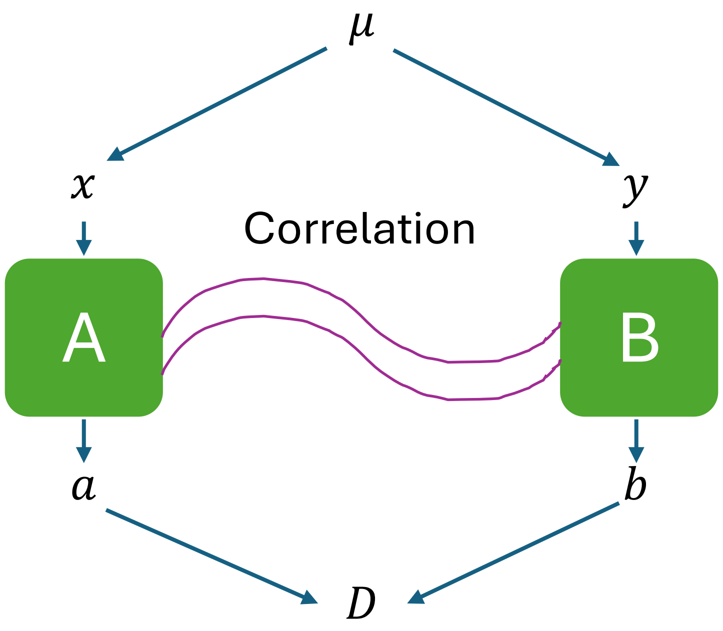
Nonlocal games

- $G(\mu, D)$ is a two-player **nonlocal game** with question alphabet **Q** and answer alphabet **A**

- μ is the probability distribution over $Q \times Q$
- $D: Q \times Q \times A \times A \to \{0,1\}$

- Verifier samples $(\mathrm{x}, \mathrm{y}) \sim \mu$
- Player win if $D(x, y, a, b) = 1$

- Players' behavior described by correlations



Measuring success

- If players use correlation $\mathrm{p}(a, b|x, y)$ then success probability is

$$\omega(G, p) = \sum_{x,y,a,b} \mu(x, y)\, D(x, y, a, b)\, p(a, b|x, y)$$

- **Quantum value** : $\omega_q(G) = \sup_{\mathrm{p} \in C_q} \omega(G, p) = \sup_{\mathrm{p} \in C_{qa}} \omega(G, p)$
- **Commutating operator value** : $\omega_{qc}(G) = \sup_{\mathrm{p} \in C_{qc}} \omega(G, p)$
- Since $\mathrm{C}_{\mathrm{qa}} \subseteq \mathrm{C}_{\mathrm{qc}}$, we have $\omega_q(G) \leq \omega_{qc}(G)$ for all games G.
- If Tsirelson's problem had positive answer, then $\omega_q(G) = \omega_{qc}(G)$ always.

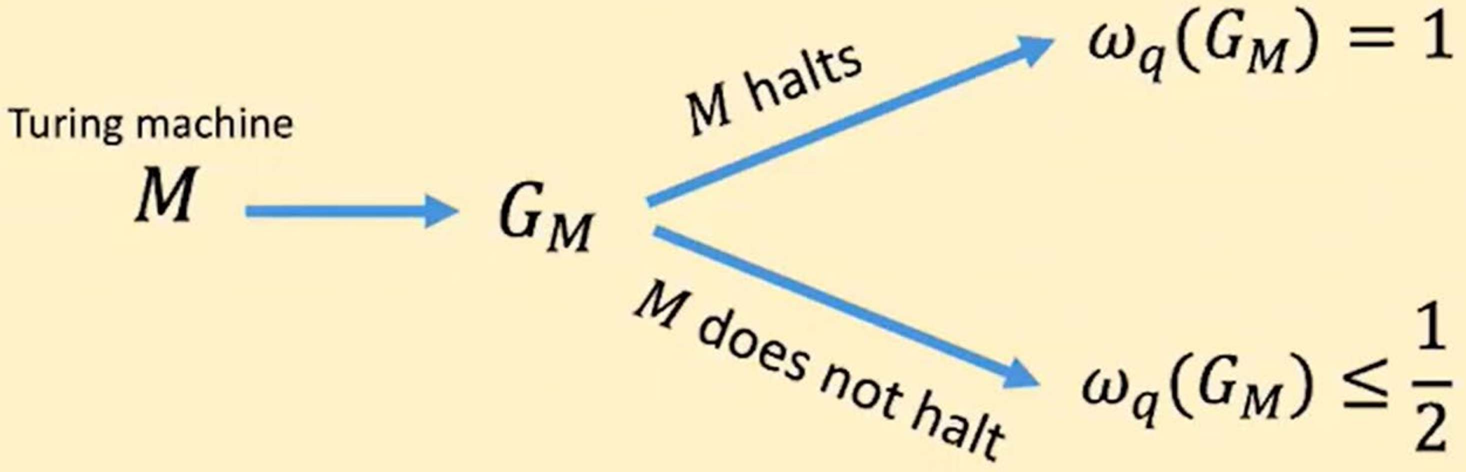
Example: CHSH game

- Questions $x, y \in \{0,1\}$ are uniformly random
- Answers $a, b \in \{0,1\}$
- $D(x, y, a, b) = 1$ if and only if a $\bigoplus b = x^\wedge y$

- **Classical value** : $\omega_c(CHSH) = \frac{3}{4}$
- **Quantum value** : $\omega_q(CHSH) = \omega_{qc}(CHSH) = \cos^2 \frac{\pi}{8} \approx 0.854 \ldots$

MIP* = RE

Main result There exists an computable map $M \mapsto G_M$ from Turing machines to nonlocal games such that



Implications

- Turing 1936: No algorithm can solve the Halting Problem
- Thus there is no algorithm to approximate $\omega_q \pm \epsilon$ for any ϵ, and in particular the Search above/ Search below algorithm cannot converge for all G
- Thus there exists a game G such that $\omega_q(G) \neq \omega_{qc}(G)$
- This implies negative answer to Tsirleson's problem: $C_{qa} \neq C_{qc}$
- Therefore Connes' embedding conjecture is false.