How quantum resources have changed what computational problems can be solved

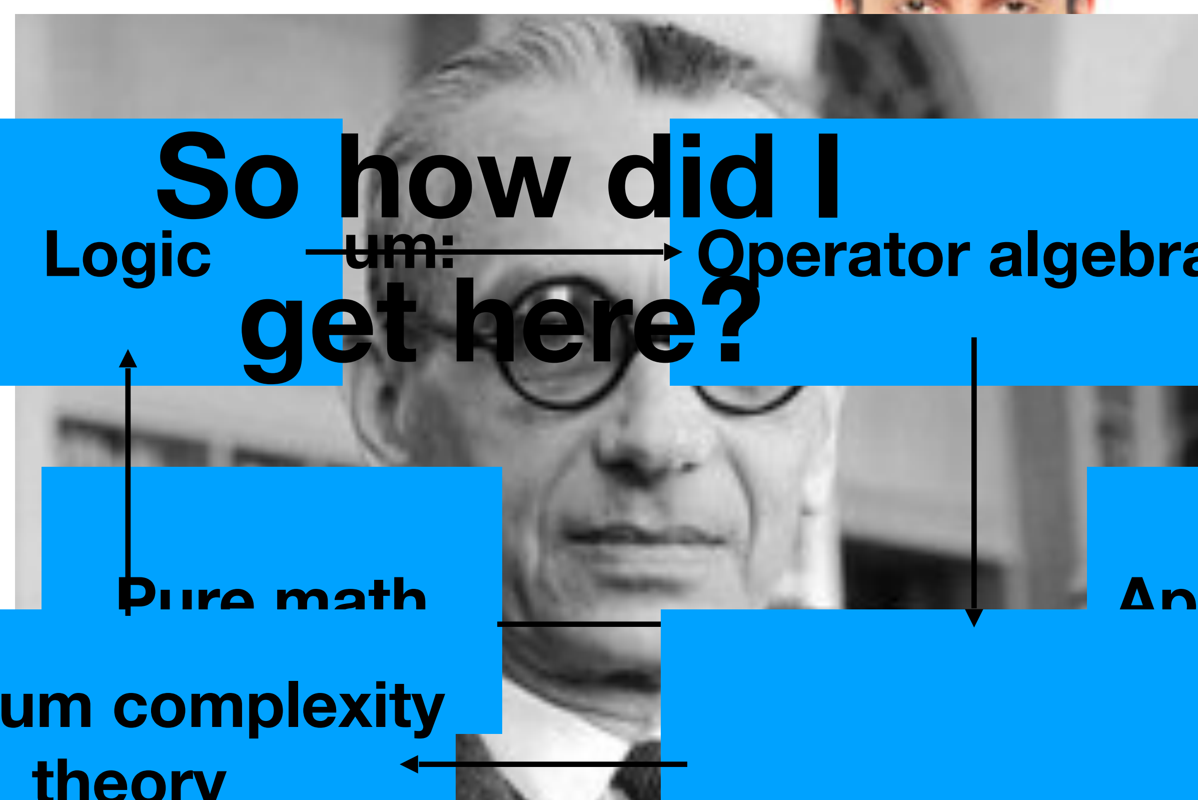
Isaac Goldbring
UC Irvine

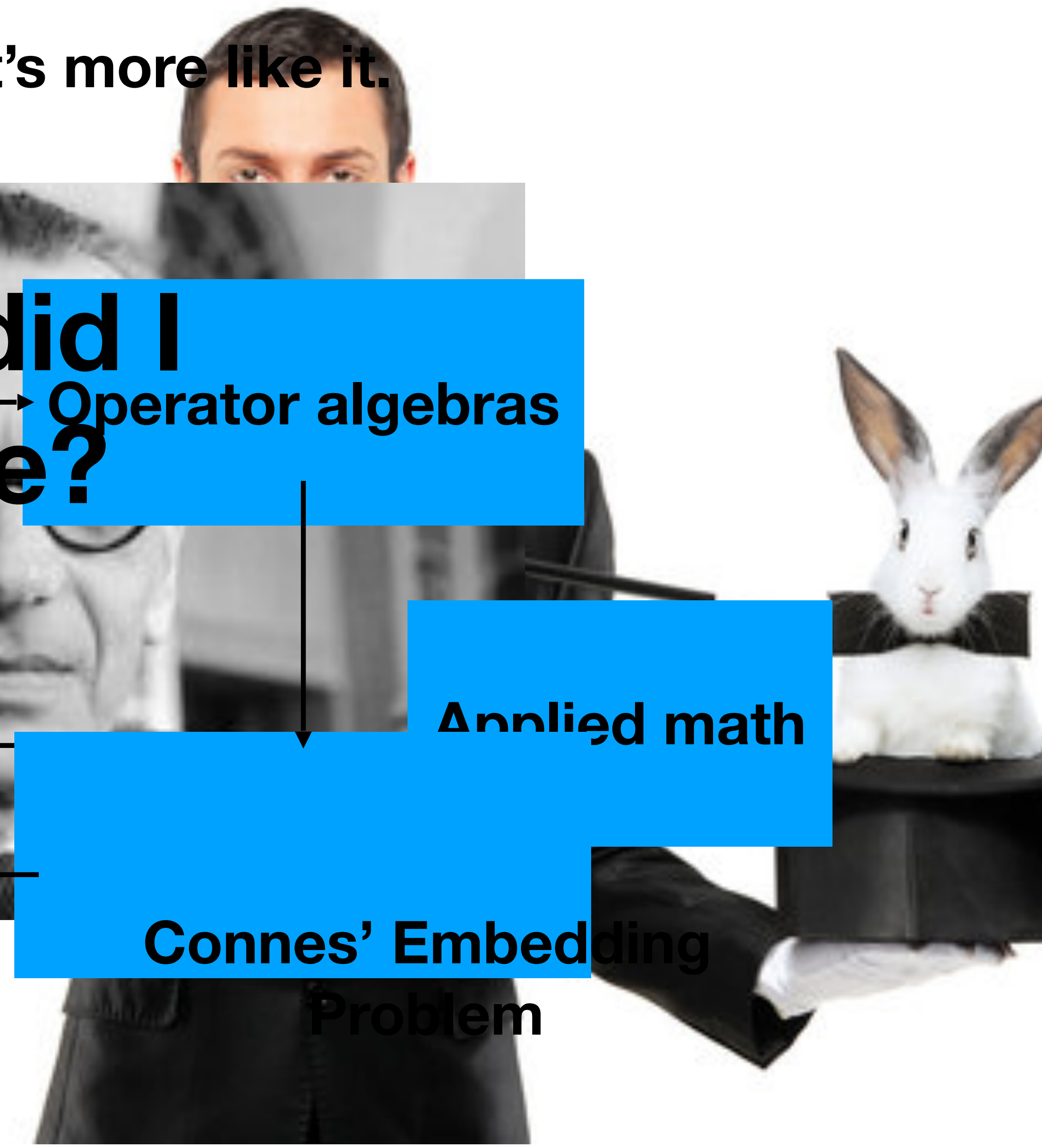
UC Irvine Physics Colloquium
January 11, 2024

How did I get here?

Hi, I'm Isaac and I'm a logician.

That's more like it.





Here is a chart of th um:

Logic

Pure math

Applied math

So how did I get here?

Logic → **Operator algebras** → **Connes' Embedding Problem** → **Quantum complexity theory**

Computational Complexity

Computational complexity in a nutshell

- Basic question: how “difficult” is some computational problem?
- Computational problem: given some finite string z of 0’s and 1’s, should we say YES or NO?
- Of course, to be useful, may need to “code” real-world problems as strings.

Best-case scenario: P

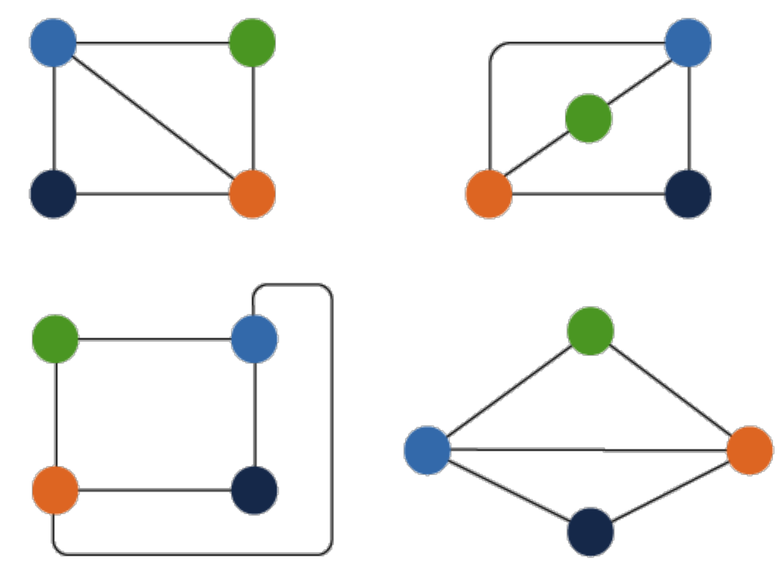
- Suppose that there is an “efficient” algorithm such that, upon input string z, decides whether or not the answer is YES or NO.
- Efficient means that the algorithm runs in polynomial time in the length of z, e.g. the length of z squared.
- Example: Deciding whether or not a number is even belongs to P.

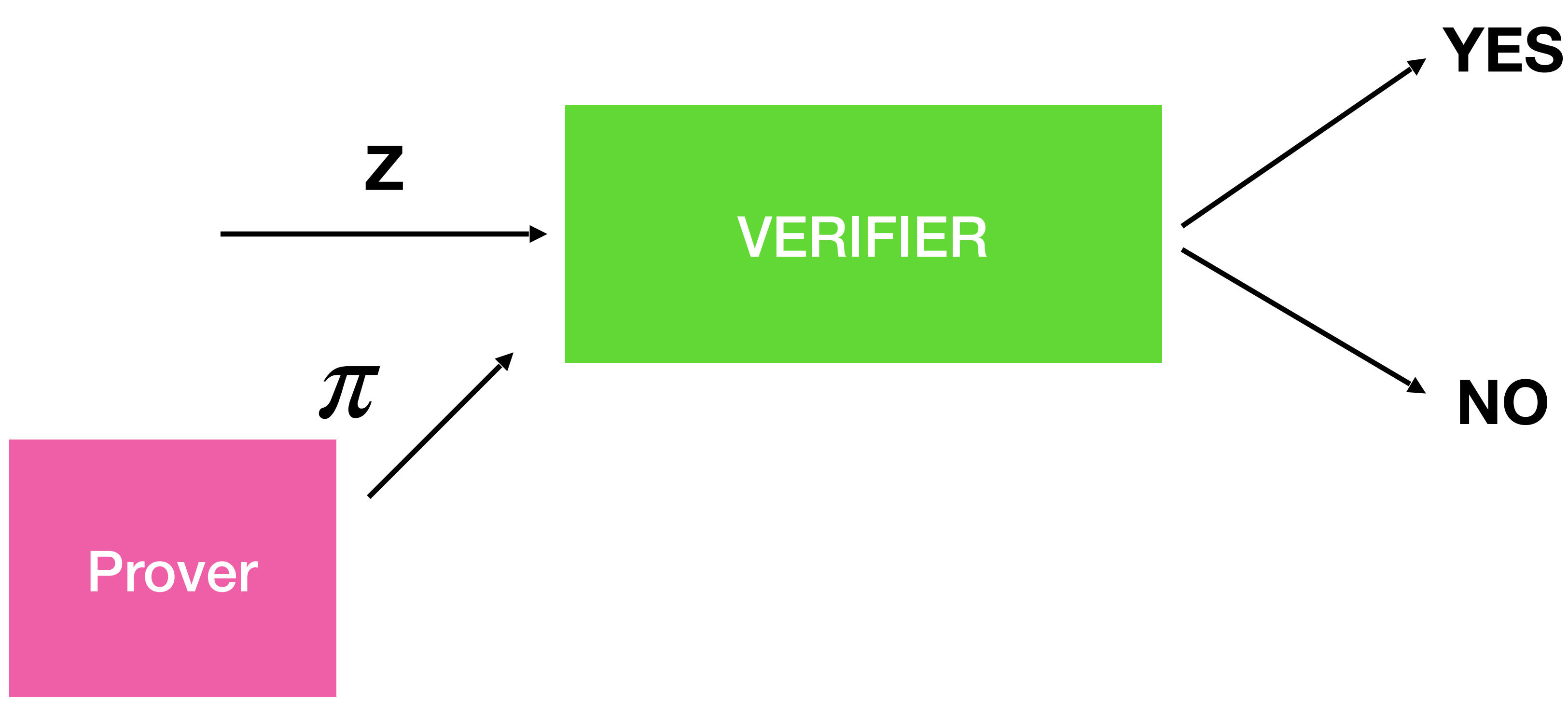
Next best-case: NP

What if we cannot efficiently solve the problem directly, but at least we know a right answer when we see one?

Example: Graph isomorphism

- **Too many pairings to check one at a time**
- **Given a "proof" from some external Prover, a Verifier can efficiently and reliably verify the validity of the purported proof**

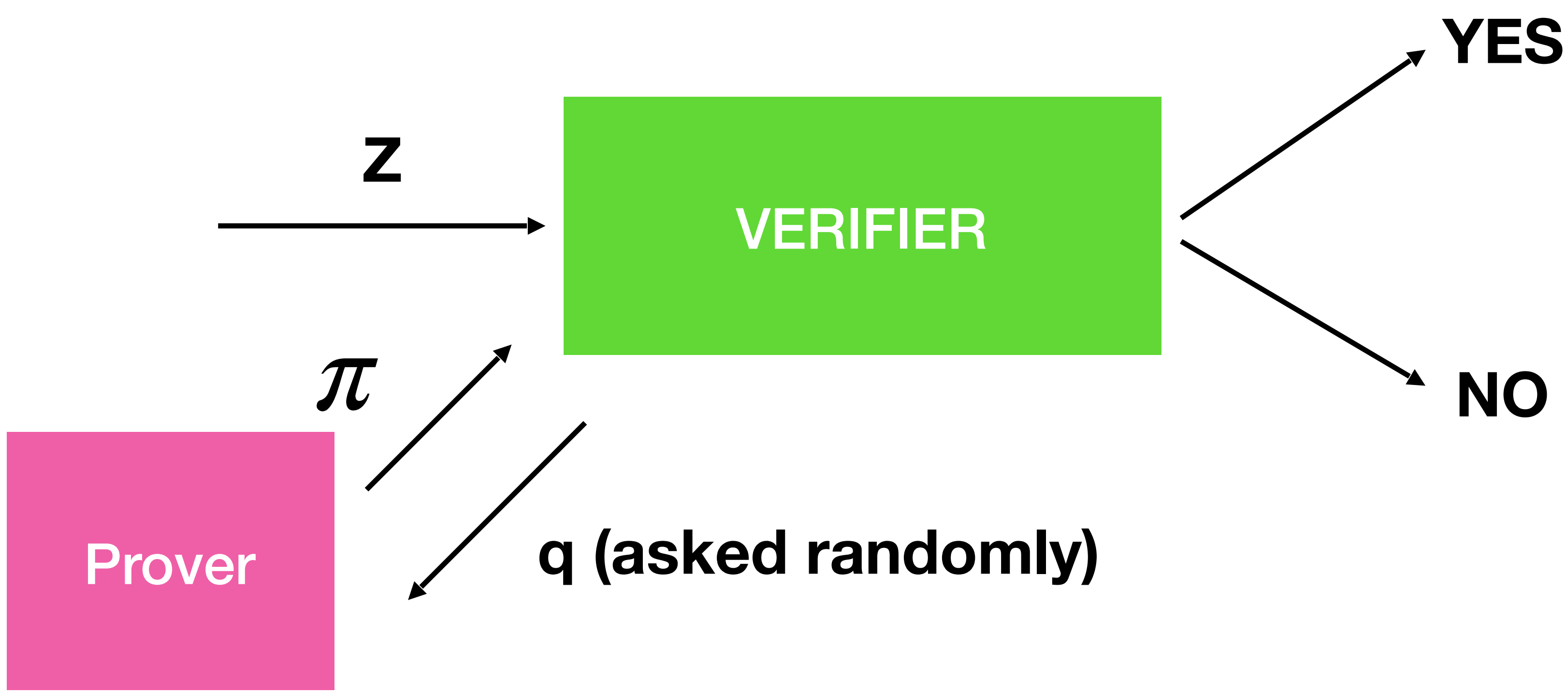




Interactive Proofs: An example

- What about graph *non-isomorphism*? It does not obviously belong to NP.
- Consider the following *interactive proof* for this problem.
- Given (G, H), the verifier randomly picks one of the graphs (say G), then randomly picks a rearrangement G' of G and sends this rearrangement to the prover.
- The prover then responds with their answer as to which graph the verifier randomly picked.
- The verifier accepts if the prover's answer is correct.
    - If G and H are not isomorphic, the prover has a strategy in which the verifier always accepts. (The prover is all-powerful!)
    - If G and H are isomorphic, the prover can do no better than guess, whence no strategy for the prover causes the verifier to accept more than half of the time.

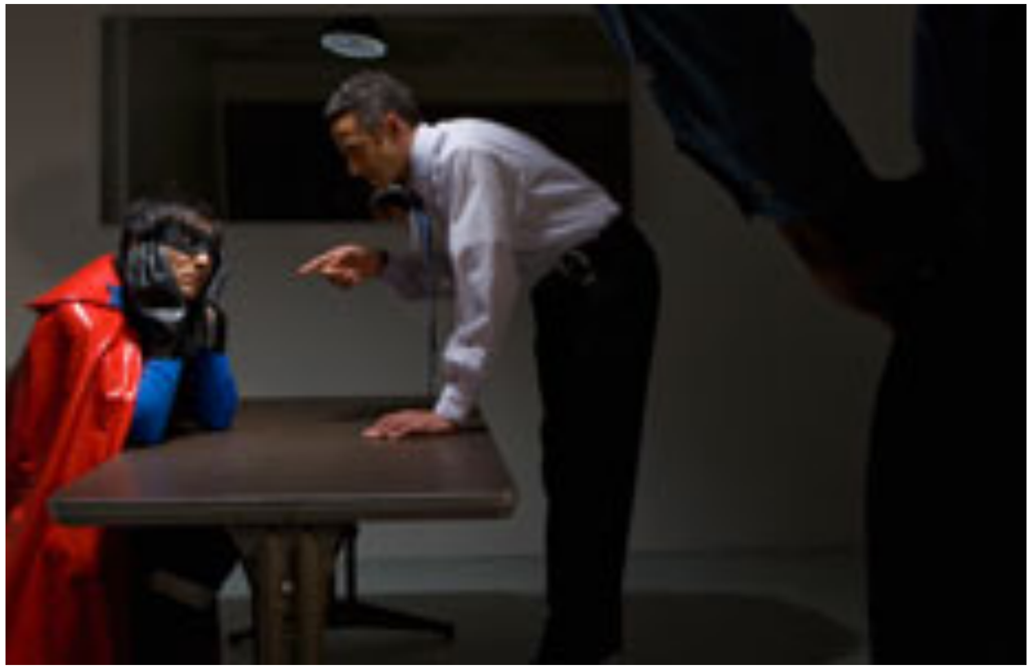
Interactive proofs in general



- **If the answer to z should be YES, then some strategy for the prover should lead to acceptance with high probability.**
- **If the answer to z should be NO, then all strategies for the prover should lead to acceptance with low probability.**
- **Probabilistic interactions are necessary, or else we are just back in NP.**

MIP: Many provers

- Why stop at one prover?
- Having multiple, cooperating, noninteracting provers allows for the use of police-style tactics, cross-checking one prover's answers against the others, to efficiently verify exponentially long proofs.
- Theorem (Babai, Fortnow, Lund): $\mathrm{MIP} = \mathrm{NEXP}$



Nonlocal games

(x, y) **randomly chosen questions**

$D(x, y, a, b) = 1$ **or** 0
Win or lose

x a b y

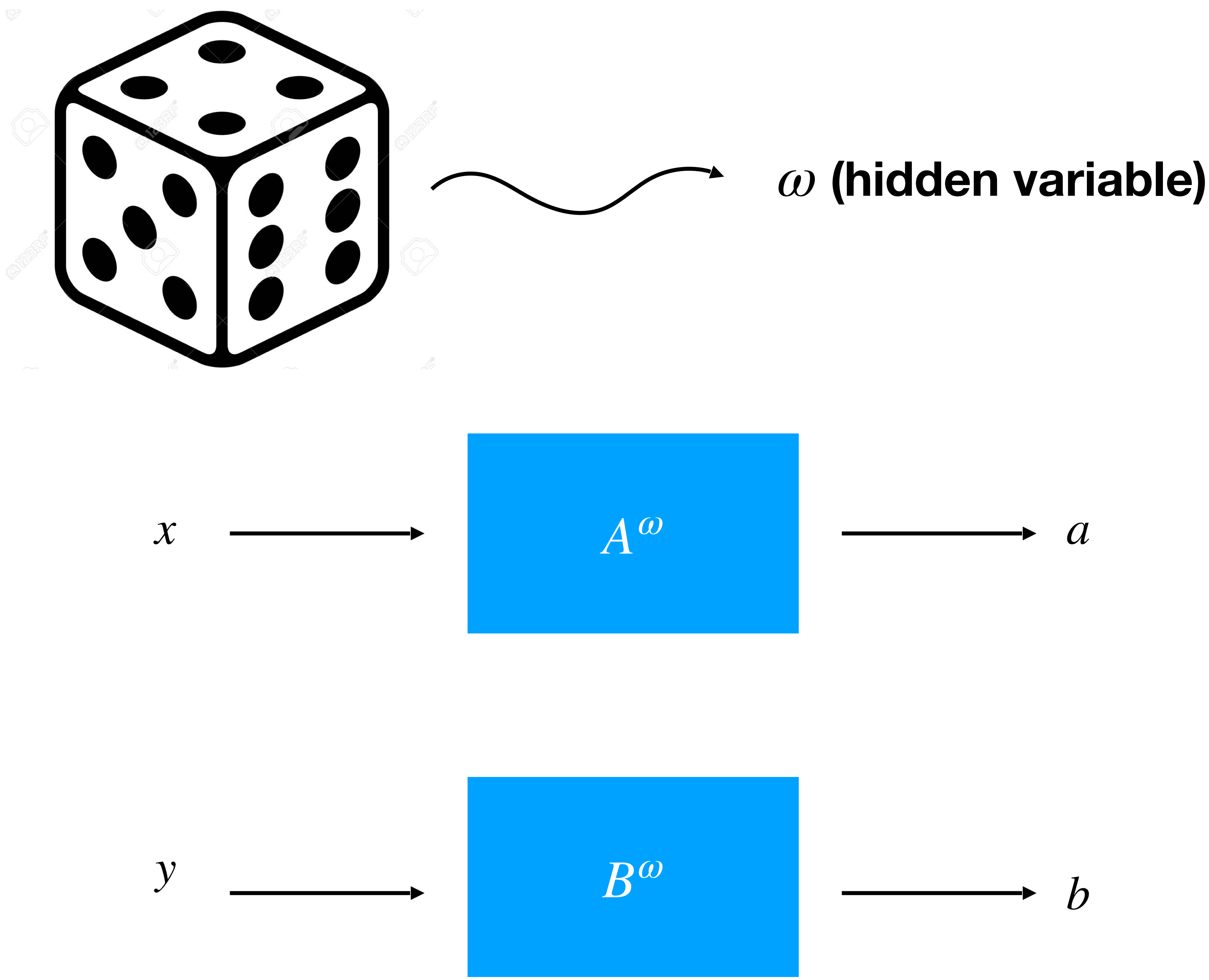
The classical value of a nonlocal game

- A *strategy* for Alice and Bob is a probability distribution $p(a, b \mid x, y)$, called a correlation.

- Given a correlation p, the expected value for winning the nonlocal game $\mathfrak{G}$ when they play according to p is denoted $\mathrm{val}(\mathfrak{G}, p)$. So $\mathrm{val}(\mathfrak{G}, p) = .9$ means they win the game 90% of the time if they play according to p.

- The *classical value* of $\mathfrak{G}$, denoted $\mathrm{val}(\mathfrak{G})$, is the maximum of $\mathrm{val}(\mathfrak{G}, p)$ when Alice and Bob use *classical* strategies.

Classical strategies for nonlocal games



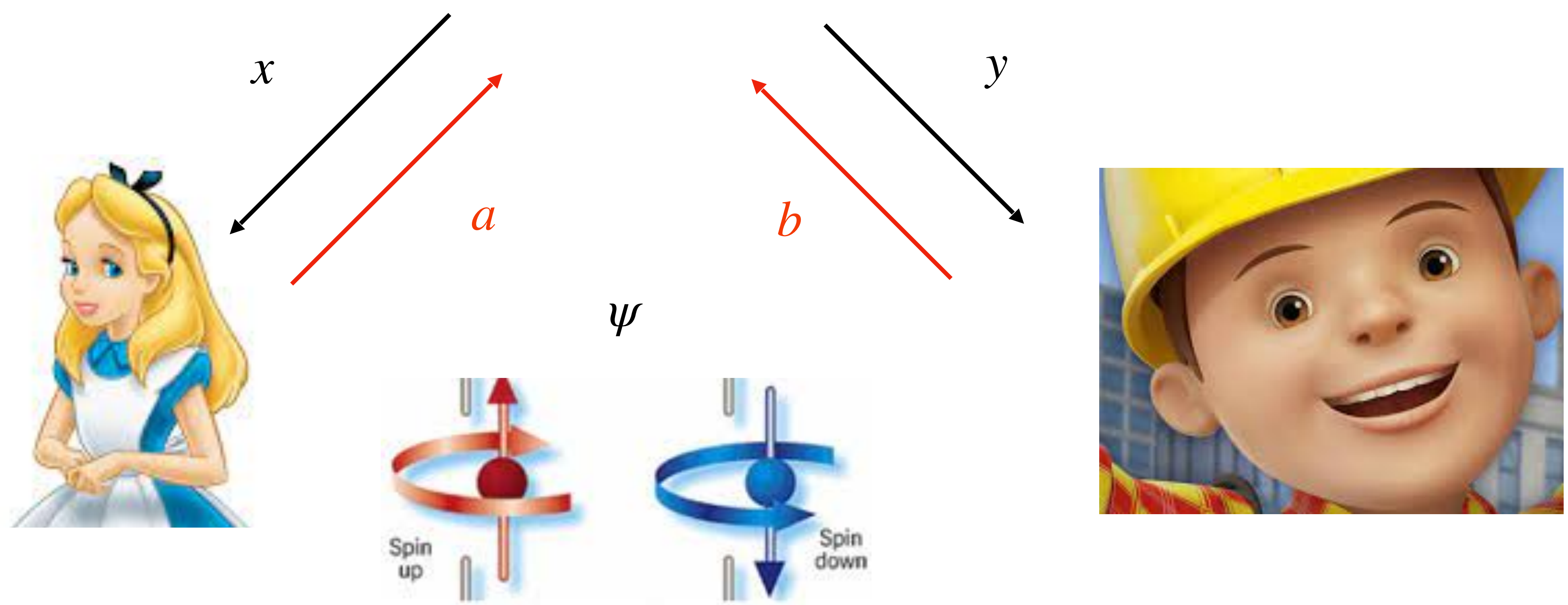
MIP reformulated

- A problem belongs to MIP provided one can effectively assign to each string z a nonlocal game $\mathfrak{G}_z$ such that:
  - If the answer upon input z is YES, then $\mathrm{val}(\mathfrak{G}_z) = 1$.
  - If the answer upon input z is NO, then $\mathrm{val}(\mathfrak{G}_z) \leq \frac{1}{2}$.

Quantum complexity

Quantum strategies

$$p(a, b \,|\, x, y) = \left\langle (A_a^x \otimes B_b^y)\psi, \psi \right\rangle$$



Bell's Theorem via the CHSH Game

- The CHSH game $\mathfrak{G}_{CHSH}$ has as questions and answers bits 0and1:
  - If either receives question 0, they win when their answers agree.
  - If both receive question 1, they win when their answers disagree.
- Easy to check $\mathrm{val}(\mathfrak{G}_{CHSH}) \leq \frac{3}{4}$.
- However, using a quantum strategy based on the EPR pair $\psi_{\mathrm{EPR}} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, one can see that the quantum value of the game satisfies $\mathrm{val}^*(\mathfrak{G}_{CHSH}) \geq \frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.85$.
- This is a version of Bell's Theorem refuting that quantum mechanics could have a local hidden variable interpretation.

MIP*

- One can define the complexity class MIP* in the same way as MIP, using $\mathrm{val}^*(\mathfrak{G}_z)$ instead of $\mathrm{val}(\mathfrak{G}_z)$.

- Theorem (Ito and Vidick): Every problem in MIP is also in MIP*. (Not obvious: why can't quantum provers "cheat"?)

- Theorem (Natarajan and Wright): Every problem in NEEXP is also in MIP*. Thus, MIP* contains problems not contained in MIP.

- Question: How big is the class MIP*?

MIP*=RE!

- The halting problem HALT is the problem that asks, given a Turing machine $\mathscr{M}$, will $\mathscr{M}$ halt on the empty input.
- Theorem (Turing): HALT is an undecidable problem.
- Theorem (Ji, Natarajan, Vidick, Wright, Yuen): HALT belongs to MIP*!!!!!!

Alan designed the perfect computer

An important consequence

- Corollary: There is no algorithm to compute $\mathrm{val}^*(\mathfrak{G})$, for otherwise HALT would be solvable.
- There is, however, an algorithm for finding $r_1 \leq r_2 \leq \cdots \leq \mathrm{val}^*(\mathfrak{G})$ which converge to $\mathrm{val}^*(\mathfrak{G})$.
- Takeaway: there does not exist an algorithm for finding $s_1 \geq s_2 \geq \cdots \geq \mathrm{val}^*(\mathfrak{G})$ that converges to $\mathrm{val}^*(\mathfrak{G})$.

Tsirelson's problem

- Instead of considering quantum strategies with Alice and Bob each having their own "lab", what about if they share a state ψ from a single Hilbert space H?

- To be able to simultaneously measure, their measurement operators must commute: $A_a^x B_b^y = B_b^y A_a^x$.

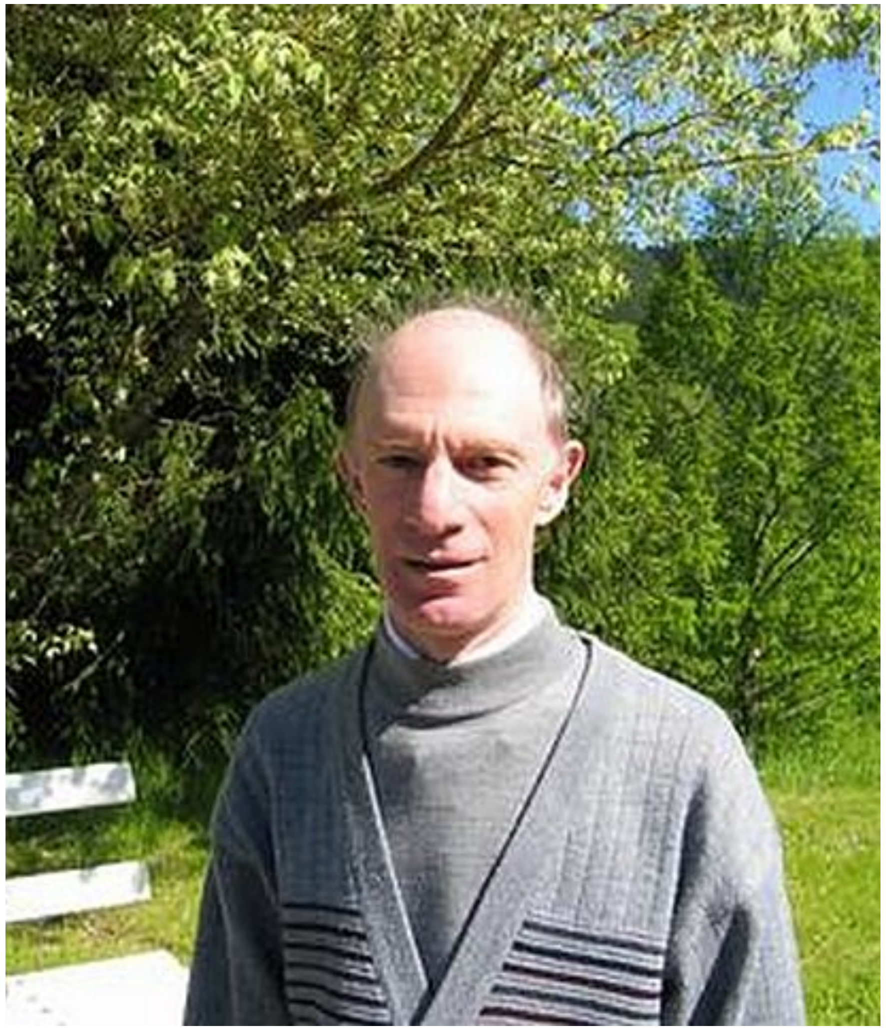
- This leads to the notion of $\mathrm{val}^{co}(\mathfrak{G})$.

- Note that $\mathrm{val}^{co}(\mathfrak{G}) \geq \mathrm{val}^{*}(\mathfrak{G})$.

- Tsirelson's problem*: $\mathrm{val}^{co}(\mathfrak{G}) = \mathrm{val}^{*}(\mathfrak{G})$?

- Corollary: Tsirelson's problem has a negative solution!

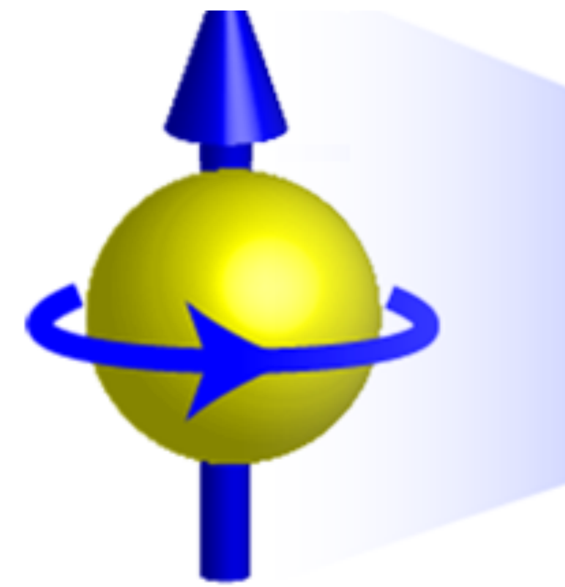
- Reason: $\mathrm{val}^{co}(\mathfrak{G})$ can be effectively approximated from above.



The Connes Embedding Problem

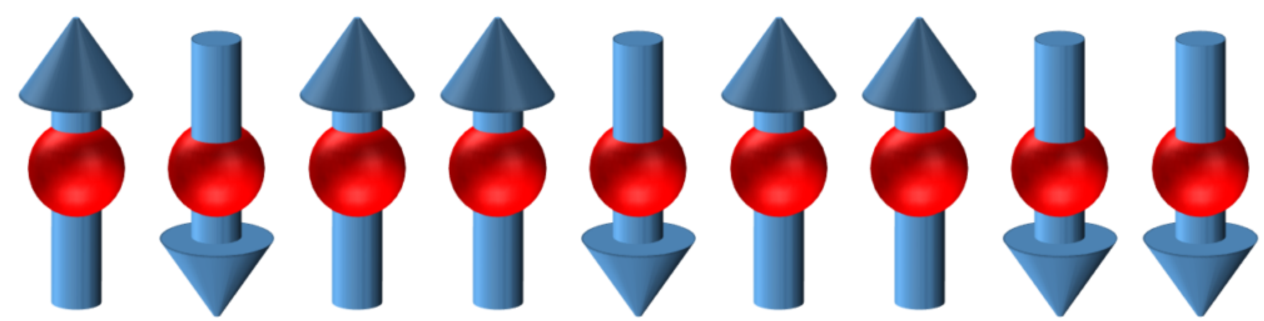
Algebras of observables

$M_2(\mathbb{C})$



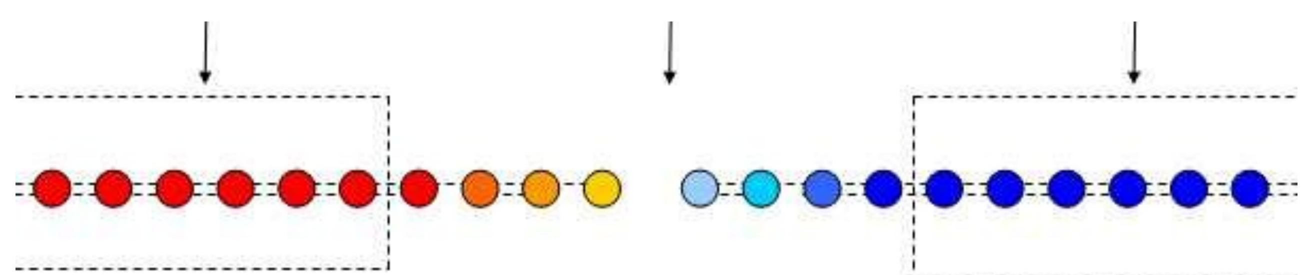
One electron

$M_2(\mathbb{C}) \otimes \cdots \otimes M_2(\mathbb{C}) = M_{2^N}(\mathbb{C})$



N electrons

$\mathscr{R}$**, the hyperfinite** II_1 **factor**



Infinitely many electrons

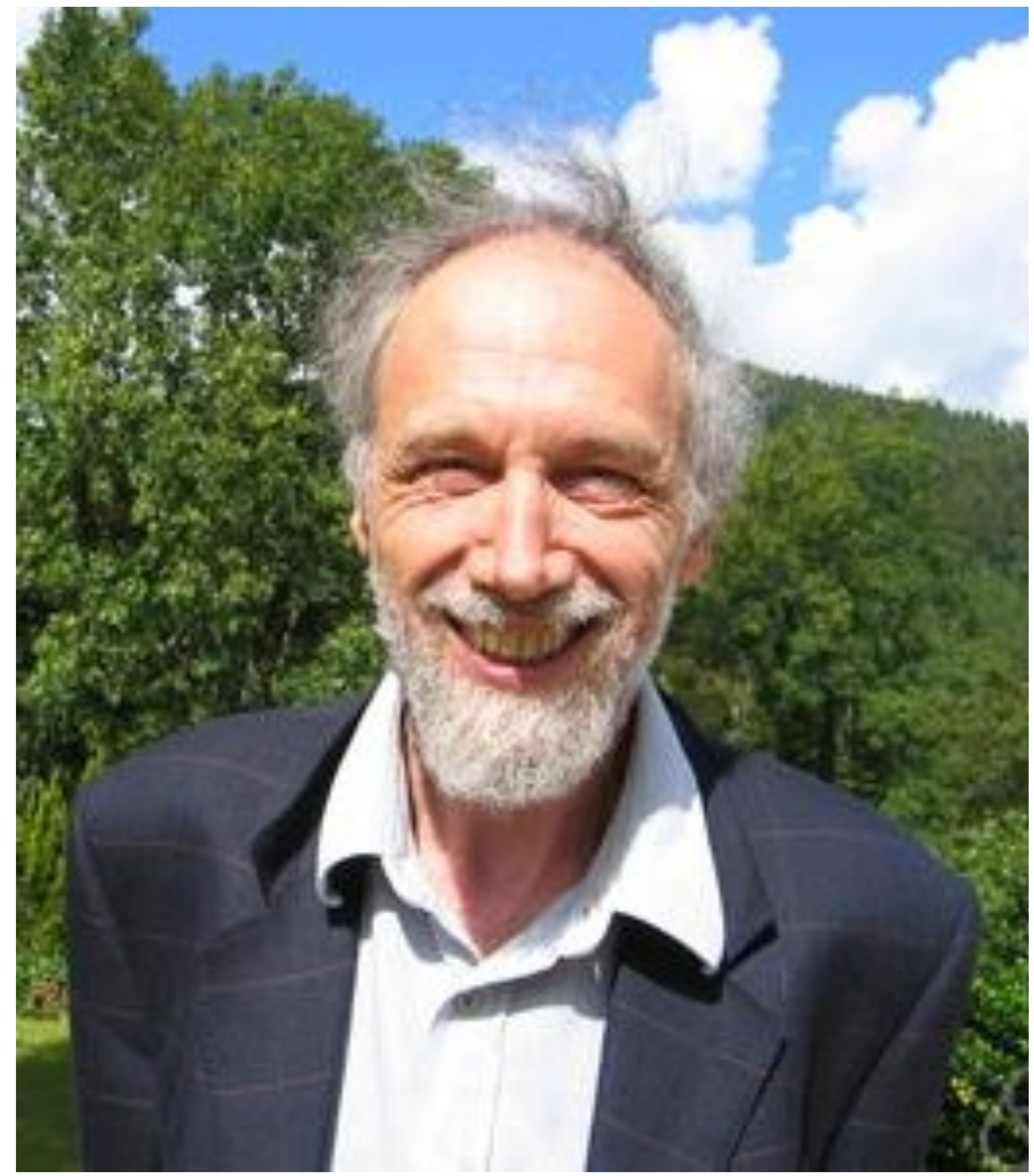
Tracial von Neumann algebras

- The algebras $M_2(\mathbb{C})$, $M_{2^N}(\mathbb{C})$, and $\mathscr{R}$ have some things in common:
  - You can add, multiply, scale, and take $*$ of the elements.
  - Closed under approxmation by "measurement probabilities."
  - Have a notion of trace:
    $$\mathrm{tr}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \frac{1}{2}(a+d).$$
- Such algebras are called *tracial von Neumann algebras*.

Connes' embedding problem (CEP)

The following quote appears in Connes' landmark 1976 paper:

"We now construct an approximate imbedding of N in $\mathscr{R}$. Apparently such an imbedding ought to exist for all II_1 factors because it does for the regular representation of free groups. However, the construction below relies on condition 6."



Connes Embedding Problem: Are all tracial von Neumann algebras "approximable" by $\mathscr{R}$?

A negative solution to CEP!

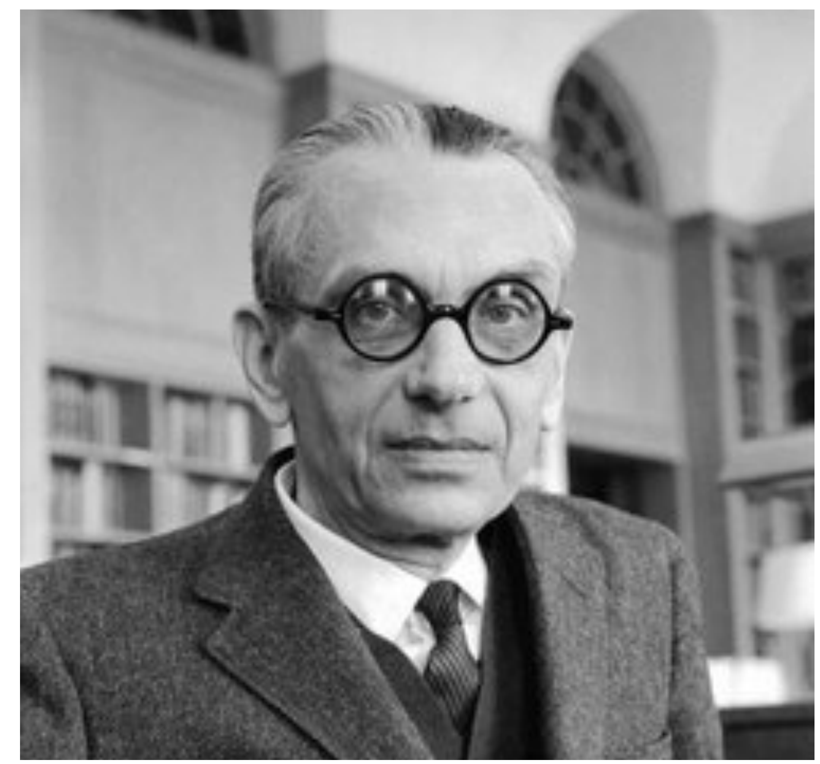
- $\mathrm{MIP}^* = \mathrm{RE}$ implies that CEP is false!!!
- But how?
- Theorem (Kirchberg, 1992): CEP is equivalent to the so-called QWEP problem.
- Theorem (Fritz, Junge et. al.): QWEP is equivalent to Tsirelson's problem.
- But we just saw that Tsirelson's problem is false!! QED.

Huh?

Enter logic!!

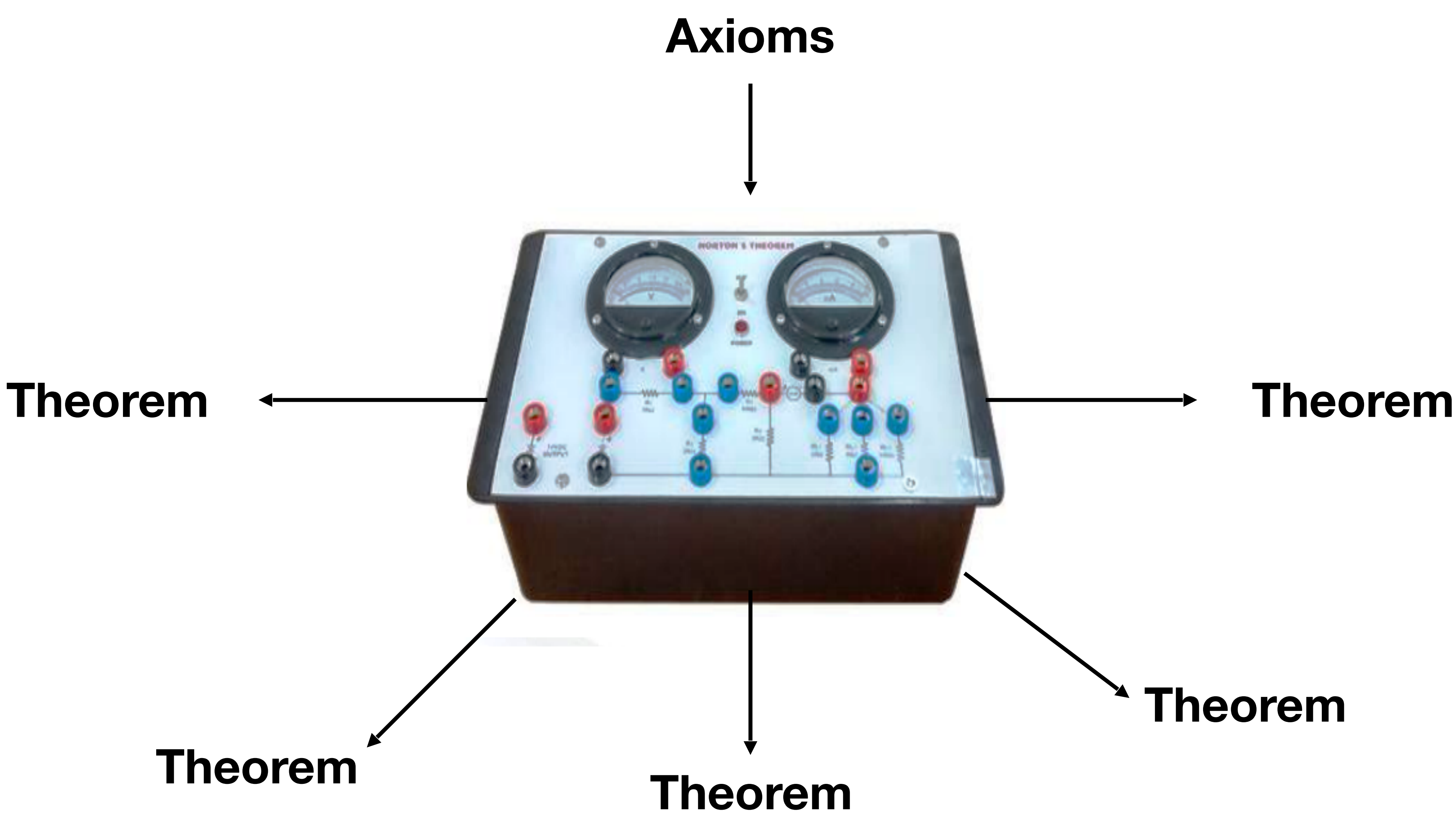
Gödel's Completeness Theorem

- Theorem: $\sum_{v \in V} \deg(v) = 2 \cdot |E|$.
- What does it mean for this to be a "theorem" of graph theory?
  - Interpretation #1: It is true in every graph.
  - Interpretation #2: It can be formally derived from the axioms of a graph.
- Gödel's Completeness Theorem says these two interpretations of "theorem" are always equivalent!



Theorem proving machines!

Interpretation #2 of the word “theorem” has the advantage of being “mechanical”.



$\mathrm{MIP}^* = \mathrm{RE}$ implies failure of CEP redux (with Bradd Hart)

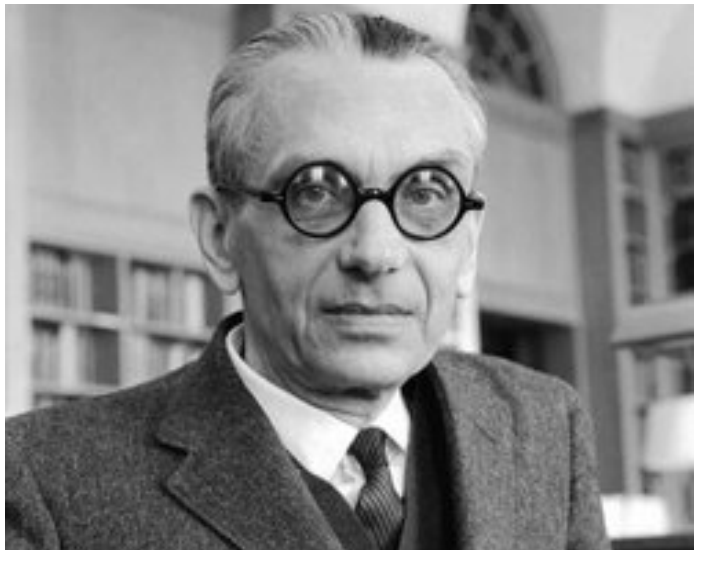
- If $\mathrm{val}^*(\mathfrak{G}) \leq r$, then *assuming CEP*, we can show that this can be expressed as a "fact" F true in all tracial von Neumann algebras.

- By the Completeness Theorem, this fact F will eventually turn up in our "theorem proving machine".

- We can thus effectively approximate $\mathrm{val}^*(\mathfrak{G})$ from above, contradicting $\mathrm{MIP}^* = \mathrm{RE}$.

Gödel's Incompleteness Theorem

- Hilbert's Program (1920s): Can one "axiomatize" arithmetic?
- Silly solution: make all theorems axioms!
- Better: can one find an "effective" set of axioms so that it is decidable whether a given statement is true or fale?
- No! Gödel's Incompleteness Theorem: given any effective set of axioms, there will be true facts of arithmetic you cannot derive from these axioms.



A Gödelian refutation of CEP

- Perhaps it is too arrogant to assume all tracial von Neumann algebras are “approximable” by $\mathscr{R}$.

- Maybe only those with certain extra properties are “approximable” by $\mathscr{R}$.

- Our proof shows that this is not the case: for any effective set of properties, there is a tracial von Neumann algebra with those properties that is not “approximable” by $\mathscr{R}$.

- We can use this Gödelian refutation of CEP to prove some extra results that the “standard” proof cannot.

Thank you!

References

- Isaac Goldbring, *The Connes embedding problem: a guided tour*, Bulletin of the AMS, Volume 59 (2022), 503-560.
- Isaac Goldbring and Bradd hart, *A computability-theoretic approach to the Connes embedding problem*, Bulletin of the Association for Symbolic Logic, Volume 22 (2016), 238-248.
- Isaac Goldbring and Bradd hart, *The universal theory of the hyperfinite II_1 factor is not computable*, to appear in the Bulletin of the Association for Symbolic Logic.
- Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen, MIP*=RE, arXiv 2001.04383.