Entanglement in Quantum Proofs

Zhengfeng Ji (UTS:QSI)

AQIS 2017, Singapore

UTS:QSI
CENTRE FOR QUANTUM SOFTWARE AND INFORMATION

UTS

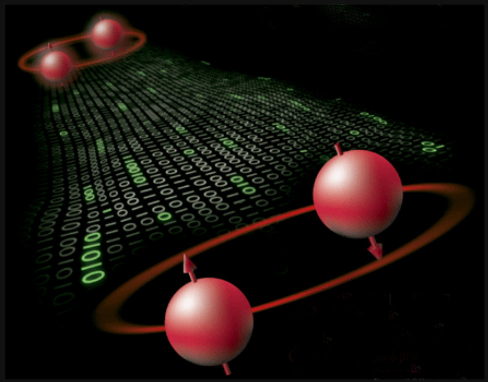
Outline

- ENTANGLEMENT and its features
- Classical and quantum PROOF systems
- Entanglement in quantum proofs
  1. Quantum Merlin Arthur (QMA)
  2. Quantum Interactive Proofs (QIP)
  3. Multiple Quantum Provers (QMIP, MIP*)
- Conclusions

ENTANGLEMENT

What is ENTANGLEMENT?

> “
> *..., then they can no longer be described in the same way as before, viz. by endowing each of them with a representative of its own. I would not call that one but rather* the characteristic trait *of quantum mechanics, the one that enforces its entire departure from classical lines of thought. By the interaction the two representatives [the quantum states] have become* ***entangled***.
>
> *— Erwin Schrödinger*



Entanglement as Correlation

- EPR paradox (Einstein-Podolsky-Rosen 1935)

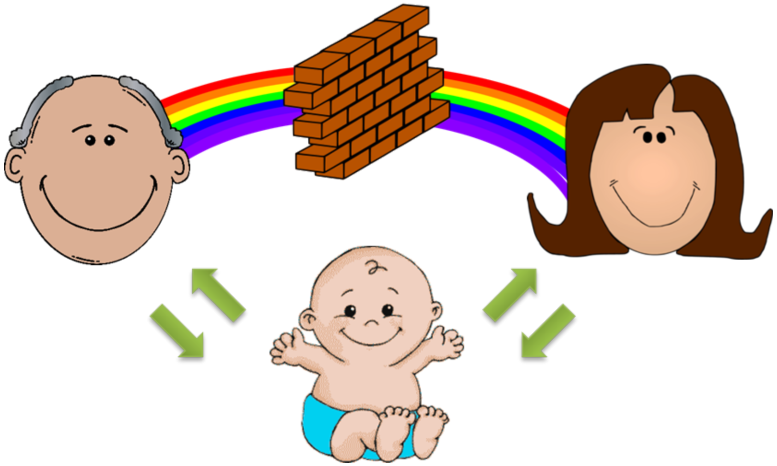
- Two ways to look at a qubit:

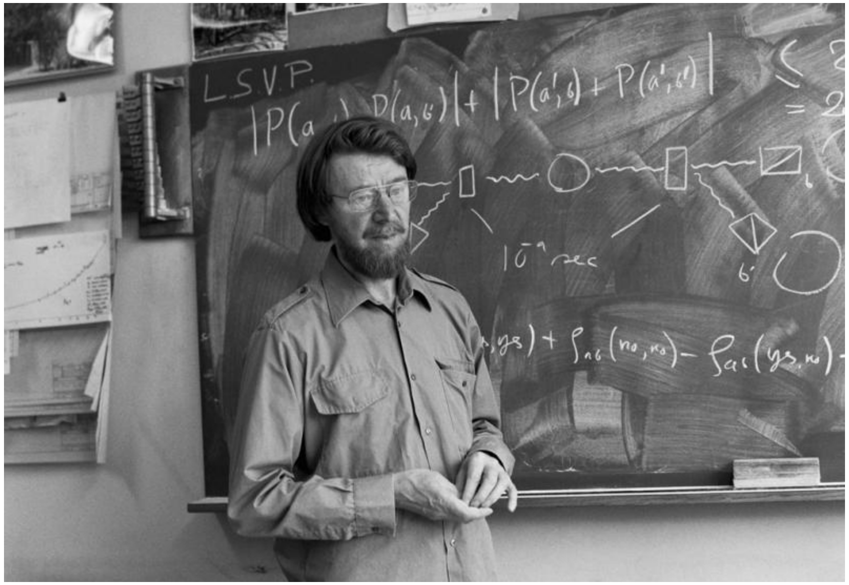
EPR State: $\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{|{+}{+}\rangle + |{-}{-}\rangle}{\sqrt{2}}.$

- Local realism, local hidden variables?

Nonlocality: Bell Inequalities

- No physical theory of local hidden variables can reproduce all of the predictions of quantum mechanics.
- CHSH game





$$\langle A_0 B_0 + A_0 B_1 + A_1 B_0 - A_1 B_1 \rangle \leq 2$$

Local versus Global Information

- Classically, complete knowledge of the global information implies that of the local
  - $x_1, x_2, x_3, \ldots, x_n = 0, 1, 0, \ldots, 1.$
  - Entropy: $S(AB) \geq S(A)$.

- Entangled state

For the EPR state $\frac{|00\rangle + |11\rangle}{\sqrt{2}}, S(AB) = 0, S(A) = 1.$

- Purification

For any state on A, there is a B system such that $S(AB) = 0$.

Monogamy of Entanglement

- Monogamy: entanglement between Alice and Bob limits Alice's ability to entangle with Charlie

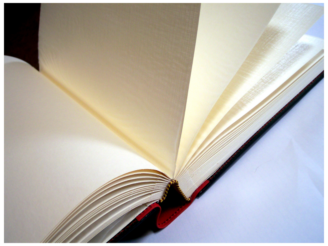
- Density Matrix Consistency

Is there a global state $\rho_{12\cdots n}$ whose local density matrix on $i, i+1$ is the EPR state?

Quantum Error Correcting Code

- Entanglement is necessary for QECC and the quantum codewords share many of the features of entanglement
- [4,2,2] code:

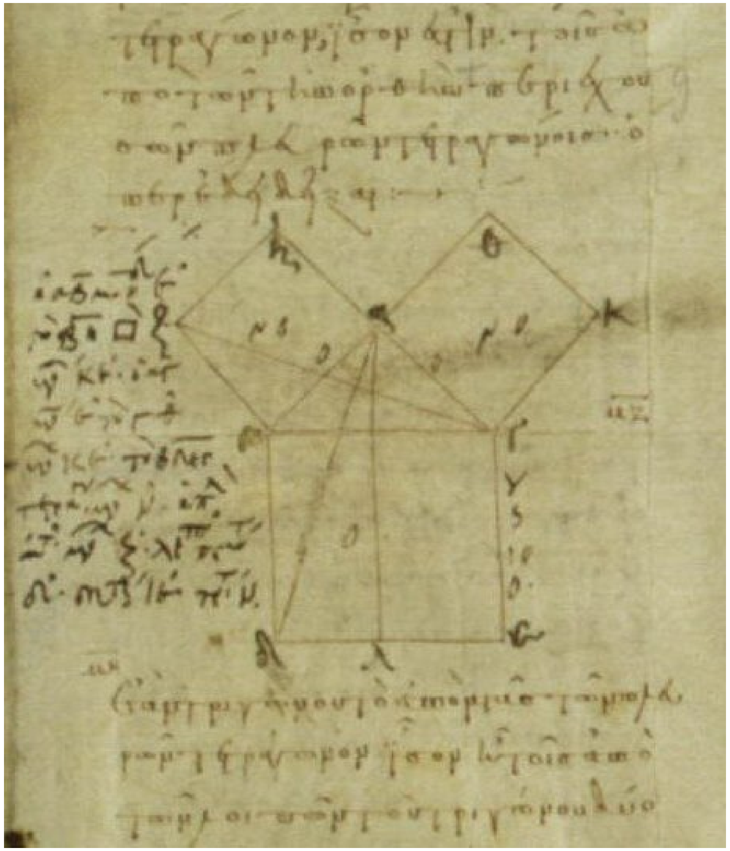
$$|0_{\mathrm{L}}\rangle = \frac{1}{2}\big(|0000\rangle + |1100\rangle + |0011\rangle + |1111\rangle\big),$$
$$|1_{\mathrm{L}}\rangle = \frac{1}{2}\big(|1010\rangle + |0110\rangle + |1001\rangle + |0101\rangle\big).$$



- Any state in the codespace is entangled
- A magic book with empty pages

PROOFS

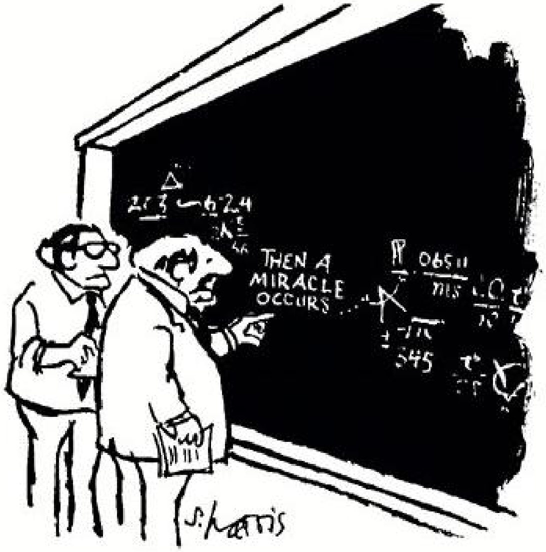
Mathematical Proofs



Mathematical logic: proofs using axioms and the rule of MP

Proofs Through the Computation Lens

NP, MA, IP, AM, MIP, ZK, PCP

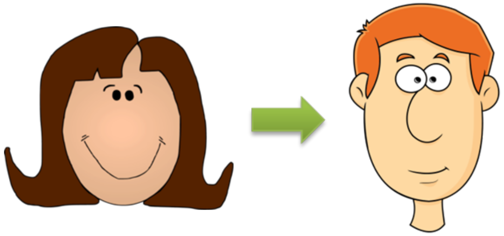


"I THINK YOU SHOULD BE MORE EXPLICIT HERE IN STEP TWO."

Efficient Proof Verification (NP)

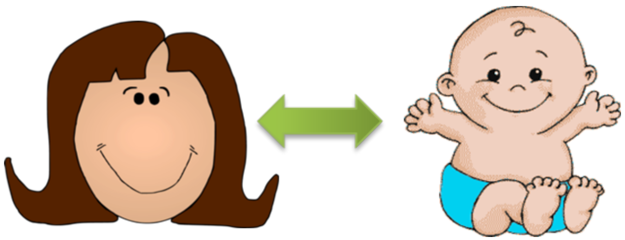
- Polynomial-time, deterministic verifier V_x such that
  - Completeness. If $x \in L$, there is a witness w such that V_x accepts w,
  - Soundness. If $x \notin L, V_x$ rejects all witnesses w.
- **Cook-Levin Theorem.** 3-SAT is NP-complete

$$(x_1 \vee x_2 \vee \neg x_4) \wedge (x_2 \vee x_3 \vee x_4) \wedge \cdots$$



Interactive Proofs (IP)

- Polynomial-time, randomized verifier, polynomial rounds of interaction



[Goldwasser, Micali and Rackoff '85]
[Babai '85]

- IP $=$ PSPACE!

[Lund, Fort, Karloff and Nisan '90]
[Shamir '92]

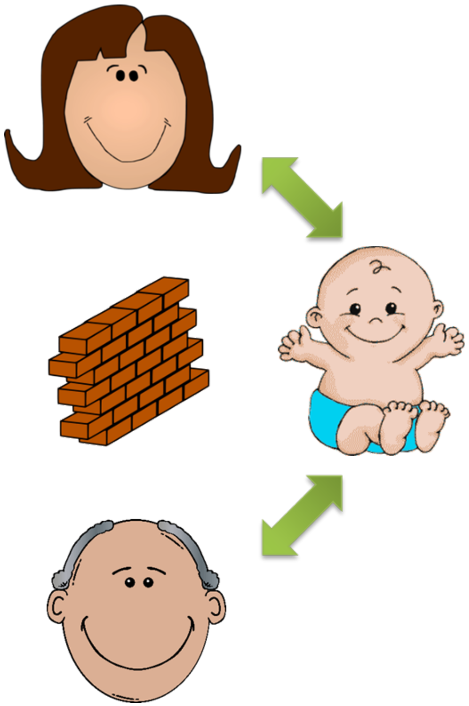
Multi-Prover Interactive Proofs (MIP)

- Multiple provers try to convince the verifier of certain statement
- The power of an extra prover: oracularization

  $$(x_1 \vee x_2 \vee \neg x_4) \wedge (x_2 \vee x_3 \vee x_4) \wedge \cdots$$

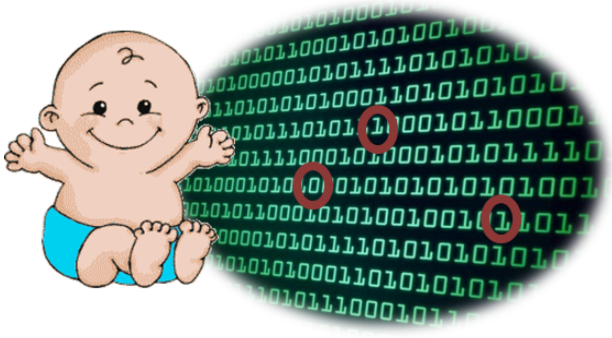
  Send a random clause $x_2 \vee x_3 \vee x_4$ to Alice and a random variable in the clause to Bob
- Unexpectedly powerful: MIP $=$ NEXP $\neq$ NP

[Babai, Fortnow and Lund '90]



Probabilistically Checkable Proofs (PCP)

- The verifier flips r random coins and queries q bits from the proof: PCP (r, q)
- Alternative characterization of NP



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

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

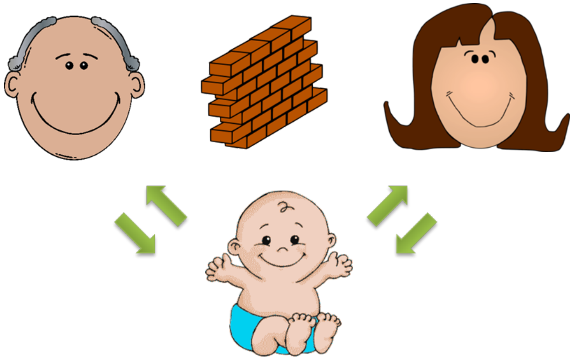
NP $\rightarrow$ IP $\rightarrow$ MIP $\rightarrow$ PCP $\rightarrow$ NP

One-Round Multi-Player Games

- One-round two-player games

  Distribution π over $S \times T$

  Predicate $V : A \times B \times S \times T \to \{0,1\}$



- The classical value ω
- NP-completeness to approximate to inverse polynomial precision via the oracularization technique
- Games are multi-prover interactive proofs with small message sizes

MIP's vs. Games	Message Size	Rounds	Gap	Hardness
Multi-Prover Proofs	poly	poly	constant	NEXP
Multi-Player Games	$\log$	1	poly^{-1}, or constant	NP

PCP Theorem. It is NP-hard to approximate the classical value of a one-round two-player game to constant precision.

QUANTUM Proofs

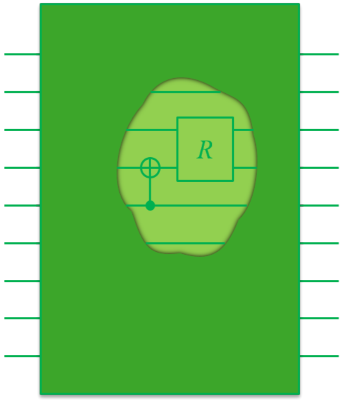
Interaction + Quantumness

Quantum Merlin Arthur (QMA)

QMA: A Quantum Analog of NP

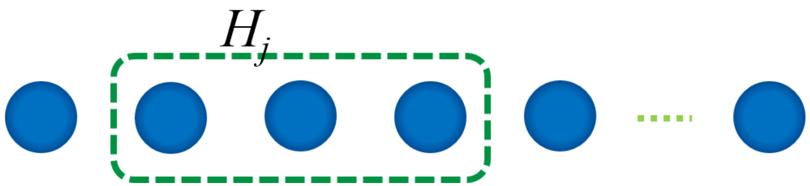
- Polynomial-time quantum verifier of quantum witness state
- Previously known as BQNP, changed to QMA by Watrous

  Arthur is the verifier and Merlin is the prover
- QMA contains NP, and conjectured to be more powerful than NP
- One of the core concepts in Hamiltonian complexity theory



Quantum Cook-Levin Theorem

- Local Hamiltonian problem
  - Input: A k-local Hamiltonian $H = \sum_j H_j$, real numbers a, b.
  - Question: Is $\lambda_{\min}(H)$ smaller than a (or larger than b)?



- An analogue of SAT problems

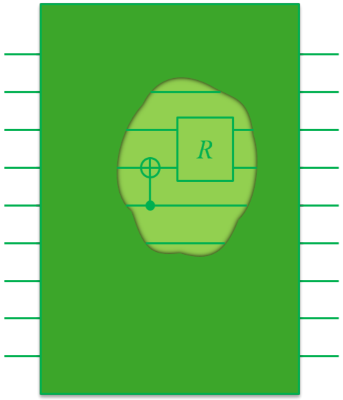
Clause $x_2 \vee x_3 \vee x_4$ corresponds to a Hamiltonian term $H_j = |000\rangle\langle 000|$ acting on qubits $2, 3, 4$.

Theorem (Kitaev). The Local Hamiltonian problem is QMA-complete.

Propagation Check

- The key idea in the proof of the classical Cook-Levin: Computation is Local.

  One can locally check the configuration history of the verification procedure step by step



- How can we check the propagation of quantum computation?

  Trivial computation: identity check?

  Is $|\psi_{t-1}\rangle$ the same as $|\psi_t\rangle$?

- **CANNOT** do this locally, because of entanglement!

  There are orthogonal entangled states that are locally the same.

Entangle with the Clock

- **Entangle** the history qubits with the clock!
- Consider the history state of the form

$$\frac{1}{\sqrt{T+1}}\sum_{t=0}^{T}|t\rangle_{\text{clock}}\otimes|\psi_t\rangle_{\text{history}}.$$

- Propagation checking term becomes local:

$$|t-1\rangle\langle t-1|\otimes I+|t\rangle\langle t|\otimes I$$
$$-|t-1\rangle\langle t|\otimes U_t^{\dagger}-|t\rangle\langle t-1|\otimes U_t$$

- Use X measurement to check the trivial propagation
- In general, measure X under the conjugation of a controlled U_t gate

Quantum Interactive Proofs (QIP)

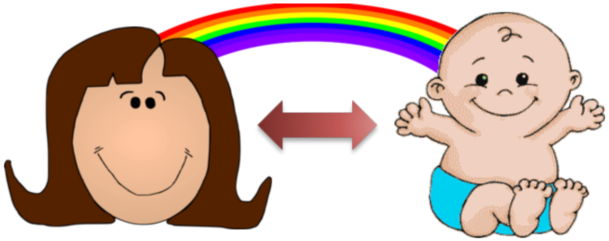
QIP: Quantum Interactive Proofs

- Polynomial-time quantum verifier, polynomially many rounds of quantum message exchange

  Trivially contains IP, and therefore PSPACE.

- Entanglement everywhere between the verifier and the prover makes the analysis much harder

  Does this ensure stronger expressiveness power?

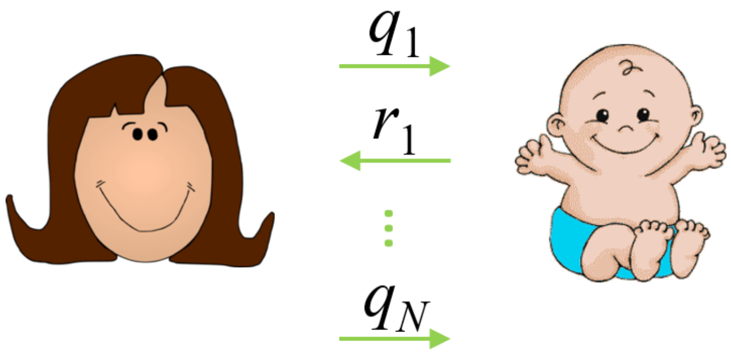


Temporal Dependence in Interactive Proofs

- A possible history of an IP protocol for PSPACE:
  $q_1, r_1, q_2, r_2, \ldots, q_N, r_N$

  $r_i \in \mathbb{F}$ is chosen at random, q_i is a degree-d polynomial over $\mathbb{F}$.

  Temporal dependence: q_i cannot depend on $r_i, q_{i+1}, r_{i+1}, \ldots, r_N$.
- Cannot first select $r_1, r_2, \ldots, r_N$ and ask for $q_1, q_2, \ldots, q_N$.



Temporal Dependence Check Using Entanglement

- Watrous: PSPACE has a 3-message quantum interactive proof.

$$\sum_R \{|R\rangle|Q(R)\rangle\}_{\text{verifier}} \otimes \{|R\rangle\}_{\text{prover}}$$

  Sends $|\overline{Q(R)}^u\rangle$ and u back to the prover and check whether the prover can disentangle $|\overline{R}^u\rangle$ for a random $u \in \{1, 2, \ldots, N\}$.

- Strengthened to QIP $=$ QIP(3), which in turn helped in the proof of QIP $=$ PSPACE *[Jain, J., Upadhyay and Watrous, 2009]*
- Same power, but more efficient in terms of round complexity. Unlikely to happen classically!

Many Provers, Entangled (QMIP*, Nonlocal Games)

Quantum Multi-Prover Interactive Proofs

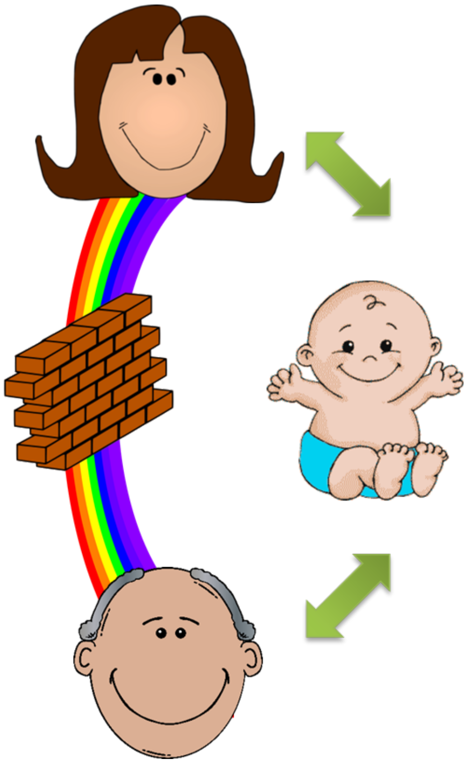
- Entanglement among provers

  Entanglement vs. shared randomness

- Exchange classical or quantum messages with the verifier (QMIP* $=$ MIP*)

  [Reichardt, Unger and Vazirani '12]

- No upper bound known!



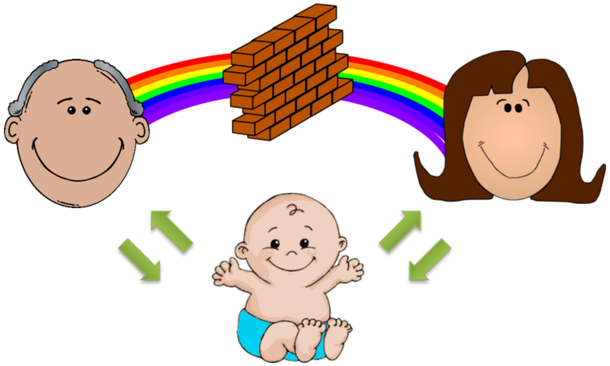
Nonlocal Games

- Nonlocal games

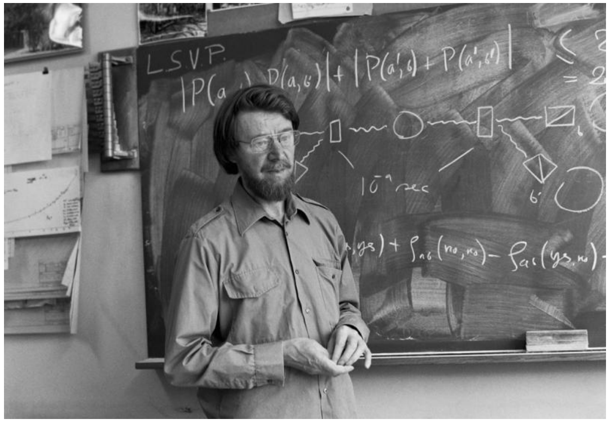
  Distribution π over $S \times T$

  Predicate $V : A \times B \times S \times T \to \{0,1\}$

  Strategy $(\rho, \{A_s^a\}, \{B_t^b\})$



- Bell inequalities *[Bell '64]*
- The nonlocal value ω^* and the Nonlocal Game problem
- Quantum multi-prover interactive proofs with small message sizes

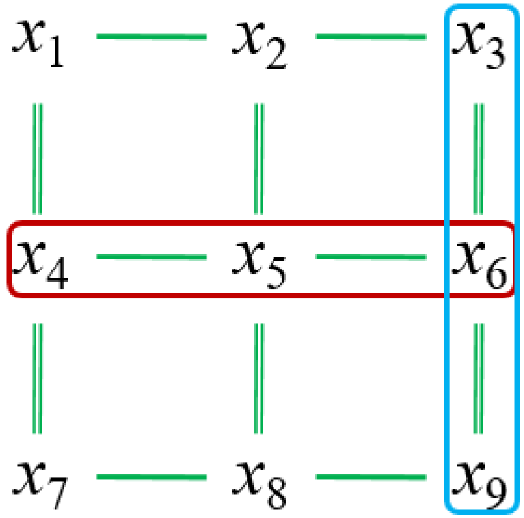


Entanglement and the Soundness Problem

- Entanglement causes soundness problems in classically sound interactive proofs

  [Cleve, Høyer, Toner and Watrous '04]

- Mermin-Peres magic square game
  - An instance of 3-SAT of 9 variables and 24 clauses
  - With two shared EPRs, Alice and Bob win the game with certainty
  - No soundness anymore!
- Is it a bug or a feature?



- Two-player XOR games:

  Referee's decision depends only on the parity of the two players' answer bits

  $\bigoplus$MIP*(2,1) $\subseteq$ QIP(2) $\subseteq$ PSPACE

  [Wehner '06]

  $\bigoplus$MIP(2,1) $=$ NEXP

  [Håstad '01]

- Unique games with entangled provers are easy

  [Kempe, Regev and Toner '07]

- Unfixable bug...

Entanglement Resistant Techniques

- Limit the power of entanglement
  - Consistency check

    Same answer for the same question

  - Confusion check
  - A third player (using monogamy)
    - Bob’ or 2-out-of-3
  - Naturally immune to entanglement: linearity and multilinearity tests

- Nonlocal games are NP-hard
  - 3-players *[Kempe, Kobayashi, Matsumoto, Toner and Vidick '08]*
  - 2-players *[Ito, Kobayashi and Matsumoto '09]*
  - Quantum Constraint Satisfaction Problems *[J. '13]*
- NEXP $\subseteq$ MIP* *[Ito and Vidick '12]*

  Entangled proves are at least as powerful as classical provers!
- Bug fixed!

Using Entanglement for Good

- Can the verifier make use of the shared entangled between provers?
- We have to go beyond the entanglement resistant approach and design protocols that classical provers cannot follow!

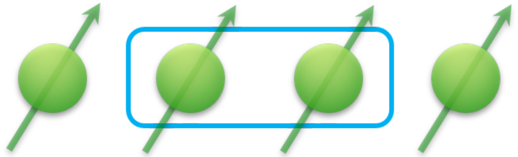
Nonlocal Games are QMA-hard

- Nonlocal games for QMA

[Fitzsimons and Vidick '15], [J. '15]

  - Density matrix consistency example: cannot simply query the $i-1, i$-th qubits and check if it is the EPR state
  - Solution: quantum error detecting code

    Quantum oracularization



  - Stabilizer game

    Nonlocality in quantum error detecting codes

    Rigidity + Encoding

- Feature, not bug!

How Farther Can We Get?

QMA(2)?

PP?

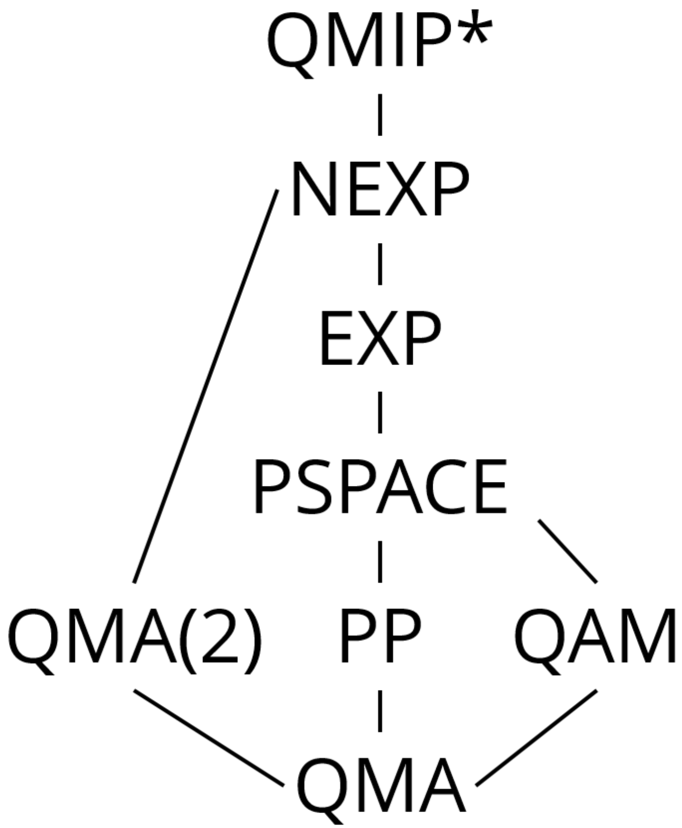
QAM?

PSPACE?

EXP?

NEXP?

QMIP*?!



Nonlocal Games are QMIP*-complete

- From QMIP* protocols to nonlocal games

[J. '17]

	MIP	**Classical Games**	**MIP***	**Nonlocal Games**
Msg size	poly	log	poly	log
Hardness	NEXP	NP	QMIP*	QMIP*

- Nonlocal Game is QMIP*-complete, and hence NEXP-hard
- Unconditionally harder than classical games
- A fundamental difference between classical and quantum proofs

$$\text{NP} \to \text{IP} \to \text{MIP} \to \text{PCP} \to \text{NP?}$$

Propagation Checking for QMIP*

- Verifier propagation check

  Assumption: the players will measure honestly (Local Hamiltonian Problems in QMA)

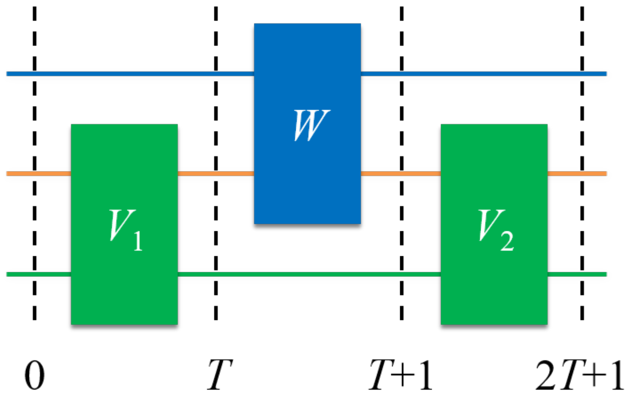
- Prover propagation check

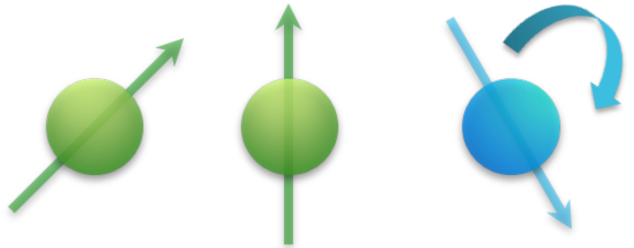
  Purification: $\rho_B = \mathrm{Tr}_A(|\psi\rangle\langle\psi|_{AB})$

  Uhlmann's Theorem

  As in the proof of QIP(3) = QIP

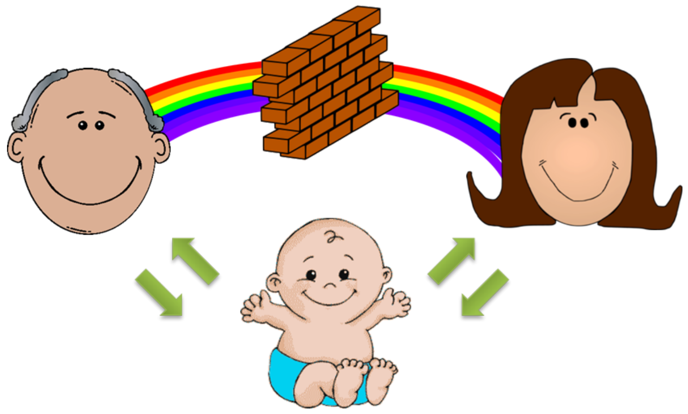
- Rigidity





Rigidity for CHSH

- V randomly samples $s, t \in \{0, 1\}$ and accepts if and only if $a \oplus b = s \wedge t$.



- Optimal strategy

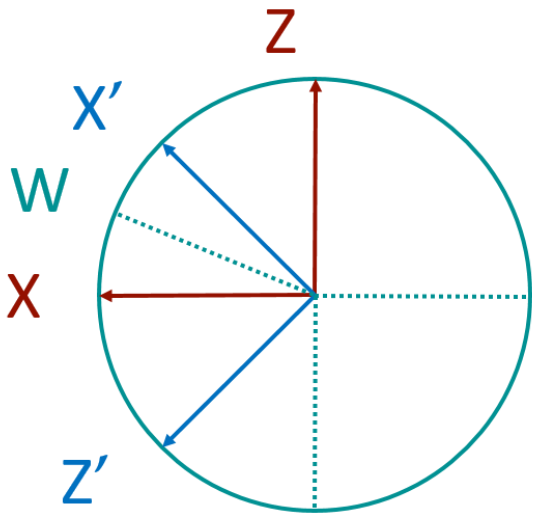
  Alice: X, Z; Bob: X', Z'; on EPR.

- Game values: 0.75 vs. 0.85

- Rigidity

  Alice has to measure X, Z; Bob has to measure X', Z'

  Jordan's Lemma



Rigid Games for Quantum Codes

- Nonlocality in quantum codes

EPR	XX, ZZ
[4,1,2] code	$XXXX, ZZZZ$

- Rigidity + Encoding
- Rigidity for stabilizer game

  Must measure X, Z on an encoded state
- Entanglement in stabilizer codes

Eight-player Stabilizer Game

- An eight-qubit code with the following stabilizer generators

X	X	X	X	X	X	X	X
X	Z	X	Z	X	Z	X	Z
Y	Y	I	I	I	I	I	I
I	I	Y	Y	I	I	I	I
I	I	I	I	Y	Y	I	I
I	I	I	I	I	I	Y	Y

+	X	X	X	X	X	X	X	X
-	Z	Z	X	X	X	X	X	X
+	X	Z	X	Z	X	Z	X	Z
+	Z	X	X	Z	X	Z	X	Z

- Consider stabilizer operators without Y's
- Anti-commutativity from the products

Let Ξ be the subset of stabilizer operators of XZ-form for the eight-qubit code. The stabilizer game for the eight-qubit code is the eight-player nonlocal game defined as follows.

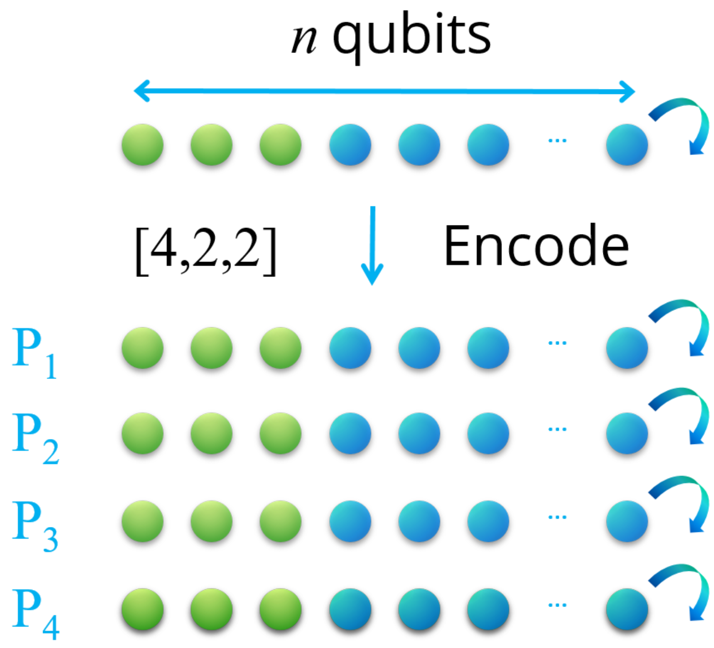
+	X	X	X	X	X	X	X	X
-	Z	Z	X	X	X	X	X	X
+	X	Z	X	Z	X	Z	X	Z
+	Z	X	X	Z	X	Z	X	Z

1. The referee selects one of the 32 operators from Ξ uniformly at random. Let $D^{(i)} \in \{X, Z\}$, $s \in \{0, 1\}$ be the i-th tensor factor and the sign of the chosen operator respectively.
2. For $i \in [8]$, the referee sends $D^{(i)}$ to player (i) and receive a bit $a^{(i)}$ back;
3. Accepts if $\bigoplus_{i=1}^{8} a^{(i)} = s$ and rejects otherwise.

Rigid Games for History State Subspace

- Transversality vs. Universality
- Rigid games on the history state subspace, with quantum verifier
- Remove the honest-player assumption
- Entanglement in history states has a loose and flexible structure
- Propagation games and constraint propagation games

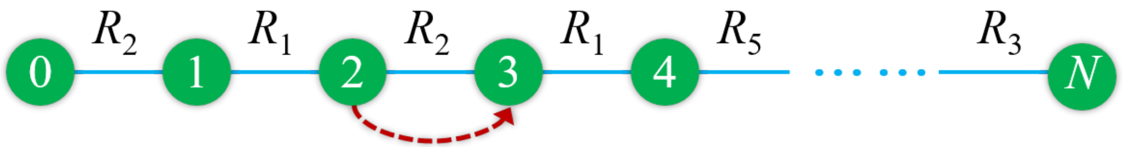
Measure honestly on the history state



$$\frac{1}{\sqrt{T+1}}\sum_{t=0}^{T}|t\rangle \otimes U_t \cdots U_1|\phi\rangle$$

Propagation Games (Simple Version)

- Reflections $R_1, R_2, \ldots, R_n$ and a sequence $\mathfrak{R} = (R_{\zeta_i})_{i=1}^N$ of reflections with indices $\zeta_i \in [n]$
- Propagation graph $G = (V, E)$ is the chain

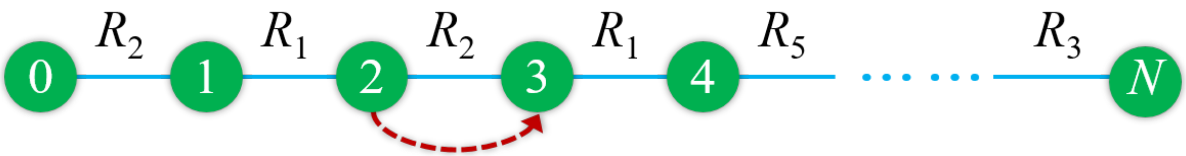


- The propagation game is an extended nonlocal game where the referee possesses quantum system $\mathbb{C}^V$, randomly samples an edge $e \in E$ and checks the propagation for this edge

Rigidity for Propagation Games

- The history state isometry for sequence $\mathfrak{R}$ is defined as

$$V_{\mathfrak{R}} \propto \sum_{t=0}^{N} |t\rangle \otimes R_{\zeta_t} R_{\zeta_{t-1}} \cdots R_{\zeta_1}.$$



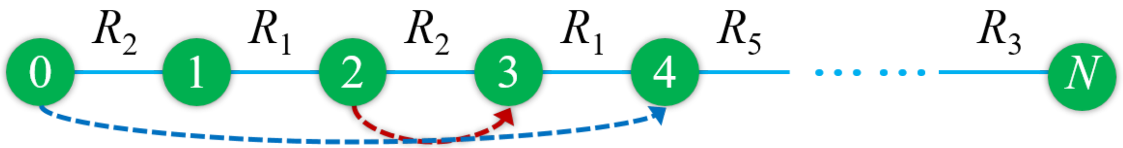
- History states are states for the form $V_{\mathfrak{R}} \rho V_{\mathfrak{R}}^*$
- **Theorem**. Any strategy that has value at least $1 - \epsilon$ must use shared state that is $N^{3/2}\epsilon^{1/2}$-close to a history state for $\hat{\mathfrak{R}}$ in trace distance.

Constraint Propagation Games

- Reflections $R_1, R_2, \ldots, R_n$; Constraints $C_1, C_2, \ldots, C_m$

$$R_{j_1} R_{j_2} \cdots R_{j_{n_i}} = (-1)^{\tau_i} I.$$

- Two chains G_{prop} and G_{cons}:



The referee possesses a quantum system $\mathbb{C}^{V(G_{\text{prop}})}$ and randomly performs the following two checks

1. (Propagation Check). Propagation game for G_{prop};
2. (Constraint Check). Propagation game for G_{cons} (no need to interact with the player);

Rigidity for Constraint Propagation Games

- For strategy $\left(\rho, \{\hat{R}_j\}\right)$, define

$$\hat{C}_i = \hat{R}_{i,1}\hat{R}_{i,2}\cdots\hat{R}_{i,n_i}.$$

- **Theorem**. If the strategy has value at least $1-\epsilon$, then the constraints are approximately satisfied. That is, for some constant κ and state $\rho_0 \propto \langle 0|\rho|0\rangle$,

$$\operatorname{Re}\operatorname{Tr}_{\rho_0}\hat{C}_i \approx_{N^\kappa \epsilon^{1/\kappa}} (-1)^{\tau_i}.$$

Conclusions

- Entanglement and its features
- Its interesting role in quantum proofs
- 成也萧何，败也萧何
- Open problems:
  - What is the power of entangled provers?
  - Is there a multi-prover variant of the quantum PCP theorem?
  - Can entanglement help a classical verifier to check more?
  - QMA(2): What is the power of UNENTANGLEMENT?
  - Quantum prover interactive proofs (QPIP): Is QPIP $=$ BQP?
  - Generalize the arithmetization technique to the quantum setting?


Thank You!