COMPRESSION OF QUANTUM MULTI-PROVER INTERACTIVE PROOFS

ZHENGFENG JI

UNIVERSITY OF TECHNOLOGY SYDNEY

MY LAST SLIDE FOR LAST YEAR'S QIP

- Approximation of the entangled game value to inverse polynomial precision is **QMA**-hard
- A connection between Bell inequalities and Hamiltonian complexity
- How about approximation to constant precision?

  [Natarajan, Vidick 15]
- Can we reduce the number of players down to 2?
- Beyond **QMA**-hardness?

OUTLINE

1. Motivations
2. Proof Overview
3. Techniques
4. Conclusions

MOTIVATIONS

How Hard are Nonlocal Games?

> *You can't put a limit on anything. The more you dream, the farther you get.*
> *— Michael Phelps*

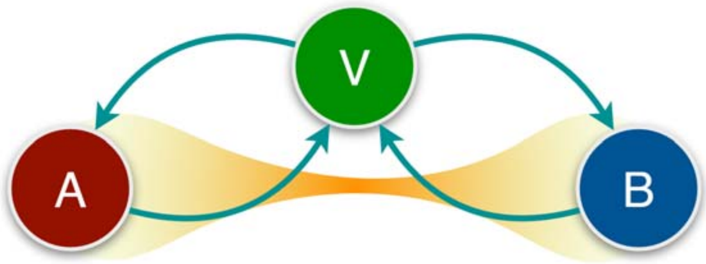
NONLOCAL GAMES

- Nonlocal games

  Bell inequalities + Multi-prover proofs

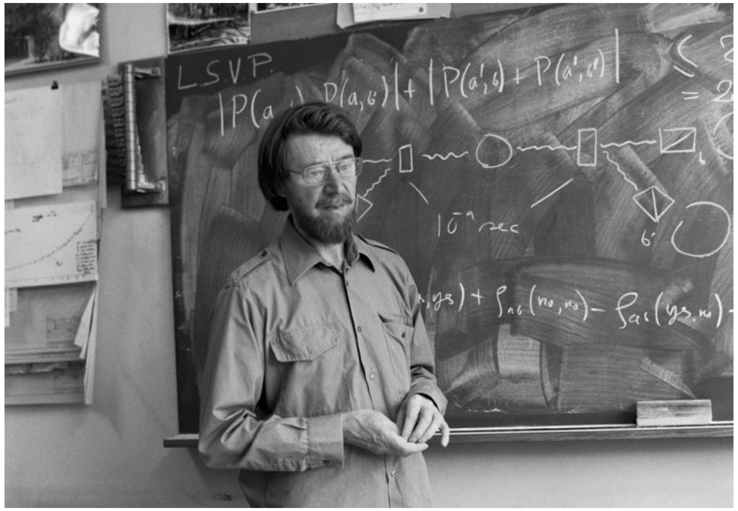
  Distribution π over $S \times T$

  Function $V : A \times B \times S \times T \to [0,1]$



- The nonlocal value ω^*

  The Nonlocal Game problem



- Nonlocal games vs. quantum multi-prover interactive proofs

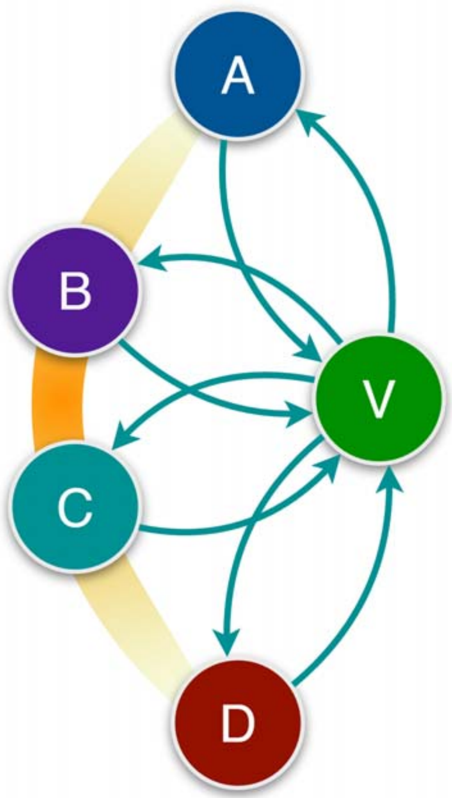
  Message size: $\log(n)$ vs. $\mathrm{poly}(n)$

IN LAST YEAR'S QIP

- A 4-player protocol for the Local Hamiltonian Problem
- Nonlocal games are QMA-hard
- Rigid nonlocal games for quantum error correcting codes
- Quantum complexity for quantum (nonlocal) games

- Dark cloud

  Unlike classical games which are NP-complete, there are no upper bounds known for nonlocal games!



MY LAST SLIDE FOR LAST YEAR'S QIP

- Approximation of the entangled game value to inverse polynomial precision is **QMA**-hard
- A connection between Bell inequalities and Hamiltonian complexity
- How about approximation to constant precision?

  [Natarajan, Vidick 15]
- Can we reduce the number of players down to 2?
- Beyond **QMA**-hardness?

HOW FARTHER CAN WE GET?

QMA(2)?

PP?

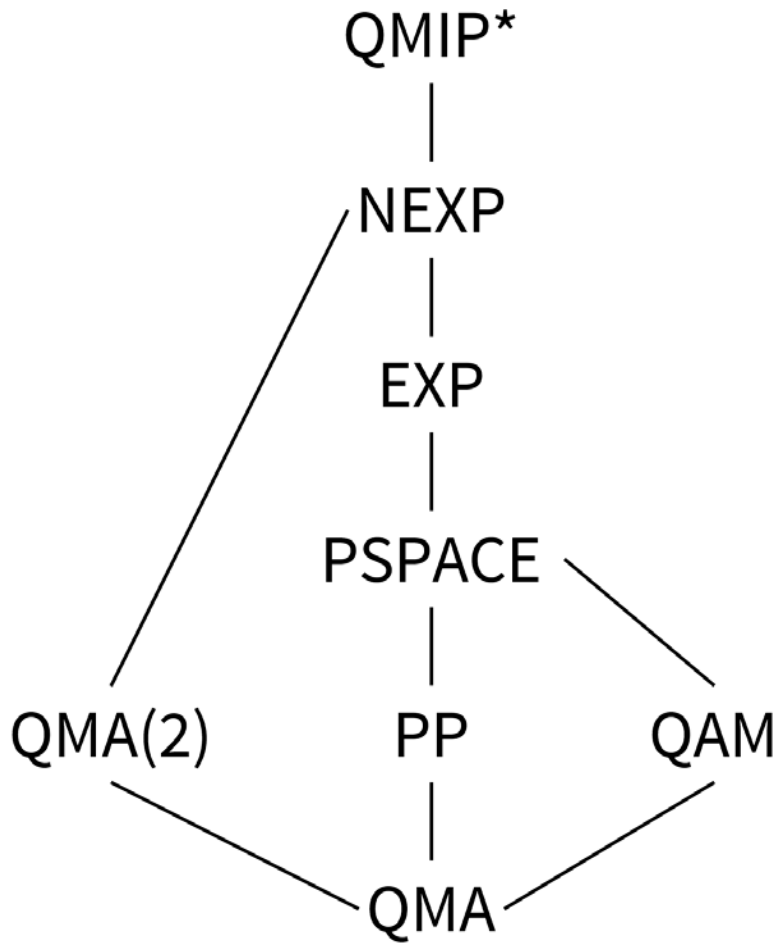
QAM?

PSPACE?

EXP?

NEXP?

QMIP*?!



PROOF OVERVIEW

A Combination of Good Old Ideas from Quantum Proofs

> *“There is no such thing as a new idea. It is impossible. We simply take a lot of old ideas and put them into a sort of mental kaleidoscope.*
> *— Mark Twain*

PSPACE?

An intermediate goal to illustrate the ideas

FROM QMA TO QMAM (QMA MODIFIED)

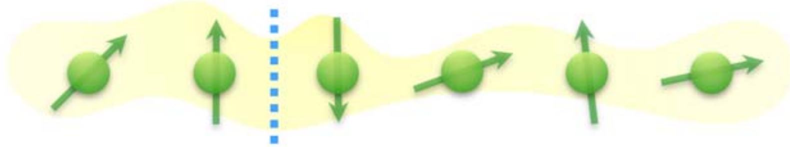
- QMA

  A quantum analog of NP.

  [Kitaev '99]

- QMAM

  [Marriott and Watrous '05]



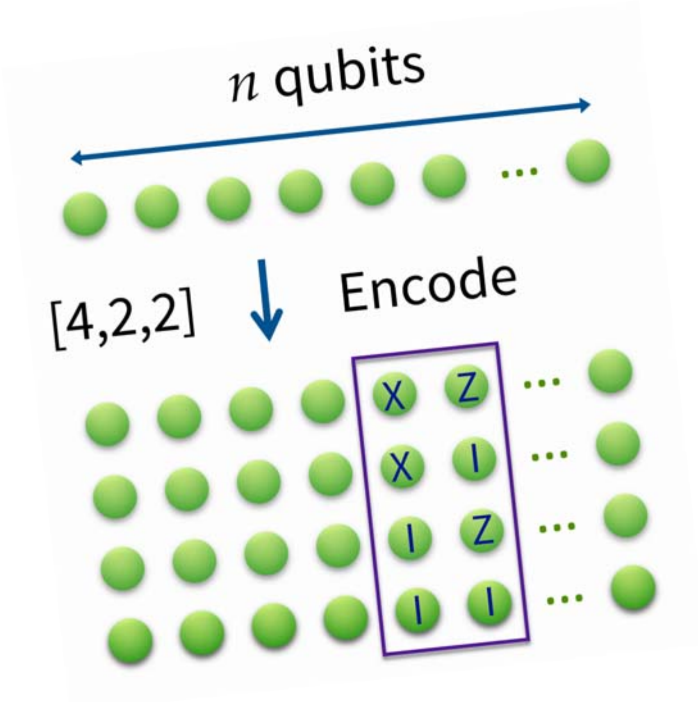
  Merlin sends the first half of the proof state to Arthur; Arthur sends a random bit b to Merlin; Merlin sends the second half; Arthur decides acceptance.

  A quantum characterization of PSPACE.

- Uhlmann's theorem

  Merlin applies unitary transform W if $b = 1$.

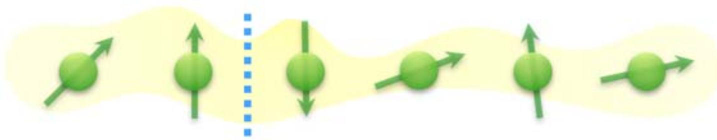
- Are we done?



5.3

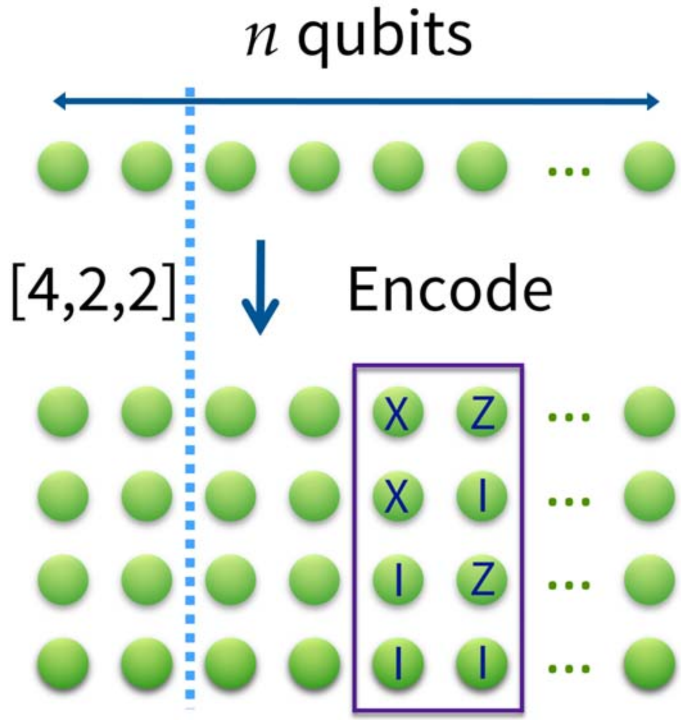
TRANSVERSALITY VERSUS UNIVERSALITY

- Need rigid nonlocal games that can enforce the players to first perform the unitary W and then measure X, Z



- The encoding and distribution of quantum proofs

  Need transversality even for the honest players to follow the protocol



- But no universal set of transversal gates exists for any quantum code!

  [Zeng, Cross and Chuang '07], [Eastin and Knill '09]

TWO IDEAS FOR THE TRANSVERSALITY PROBLEM

1. The computation can be classical on the prover side for QIP(3)

   [Watrous '99]

   No transversal gates known even for universal classical computation on quantum codes

2. A new distribution of the proof state without encoding

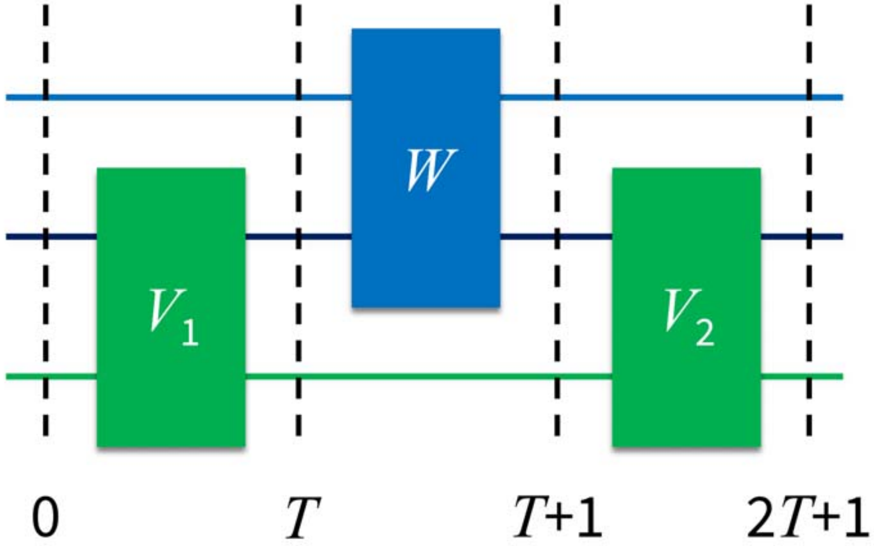
   Propagation games and constraint propagation games

   Rigidity without encoding

STEP 1. AN HONEST-PLAYER GAME FOR QIP(3)

- Plays the role of the Local Hamiltonian Problem for QMA
- History state of the interaction

$$\sum_{t=0}^{2T+1} |t\rangle \otimes U_t U_{t-1} \cdots U_1 |\psi\rangle$$



- Referee possesses the clock and the verifier register, prover possesses a copy of clock and both the message and prover register
  - Verifier propagation check: Both the Hadamard and Toffoli propagations can be checked by Pauli X and Z measurements
  - Prover propagation check: Extended EPR game

STEP 2. AN EXTENDED NONLOCAL GAME FOR QIP(3)

Use the rigidity of a constraint propagation game to remove the requirement that the prover measures honestly in the honest-player game for QIP(3)

STEP 3. A NONLOCAL GAME FOR QIP(3)

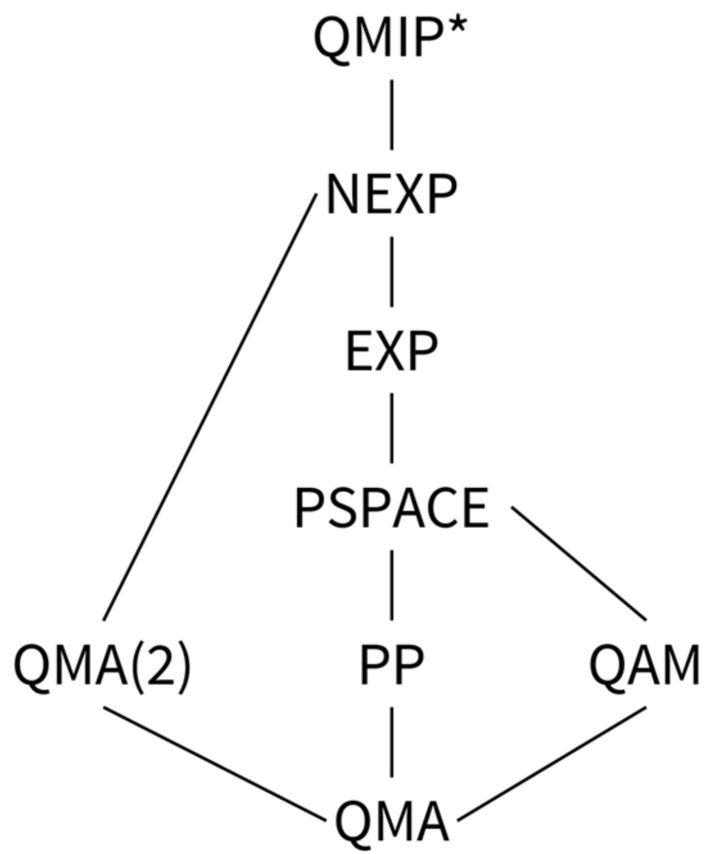
Make sure that the referee only performs Pauli X, Z measurements and delegate the measurements to additional provers

BEYOND PSPACE AND IMPLICATIONS

- Parallelization works for quantum multi-prover interactive proofs

  [Kempe, Kobayashi, Matsumoto and Vidick '08]

- The Nonlocal Game problem (with inverse polynomial precision) is QMIP*-complete, and hence NEXP-hard.
- Nonlocal games are provably harder than classical games (NP-hard).
- A strong indication that approximation precision matters for the complexity of Nonlocal Games.



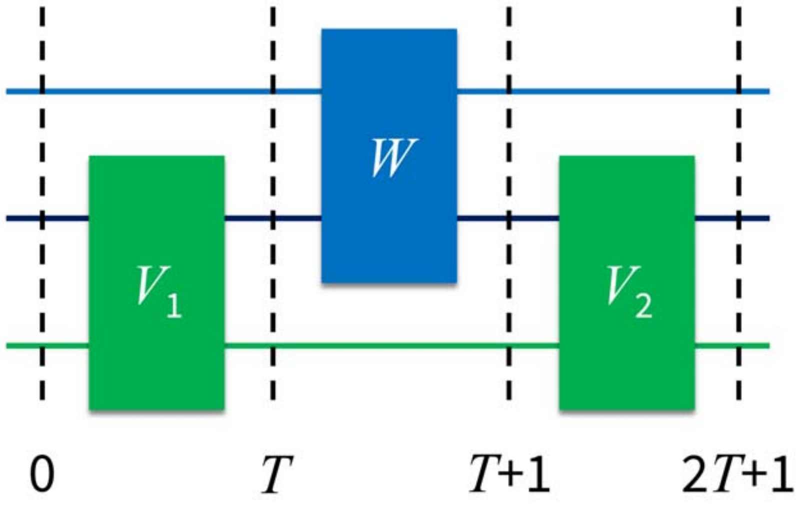
TECHNIQUES

Rigidity by Extended Nonlocal Games

> “ *Example is leadership.*
> *— Albert Schweitzer*

THE POWER OF EXTENDED NONLOCAL GAMES

- Easier and more flexible to achieve rigidity with Extended Nonlocal Games
  - Allow the distribution of raw qubits (without encoding) to the players while retaining control over the players' behavior (rigidity)
  - Check the prover's propagation in QIP(3)



EXTENDED NONLOCAL GAMES

- Nonlocal Games and Extended Nonlocal Games

  Question sets S, T, answer sets A, B, distribution π over $S \times T$ and a function V that specifies the acceptance rule of the referee

Nonlocal Games	$V : A \times B \times S \times T \to [0, 1]$
Extended Nonlocal Games	$V : A \times B \times S \times T \to [0, I]$

[Johnston, Mittal, Russo and Watrous '16]
[Tomamichel, Fehr, Kaniewski and Wehner '13]

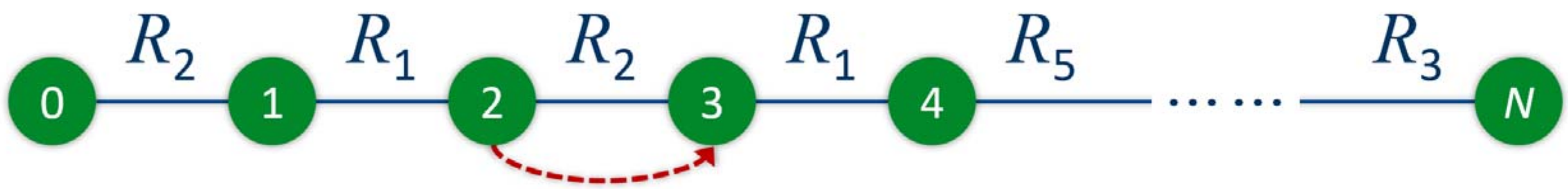
- Equivalently, the referee possesses a quantum system which the players choose how to initialize; the referee may measure and then decide

- Single-player extended nonlocal games are already interesting

6.3

PROPAGATION GAMES (SIMPLE VERSION)

- Reflections $R_1, R_2, \ldots, R_n$. A sequance $\mathfrak{R} = (R_{\zeta_i})_{i=1}^{N}$ of reflections with indices $\zeta_i \in [n]$



The propagation game is an extended nonlocal game in which the referee possesses a quantum system $\mathbb{C}^{N+1}$ and

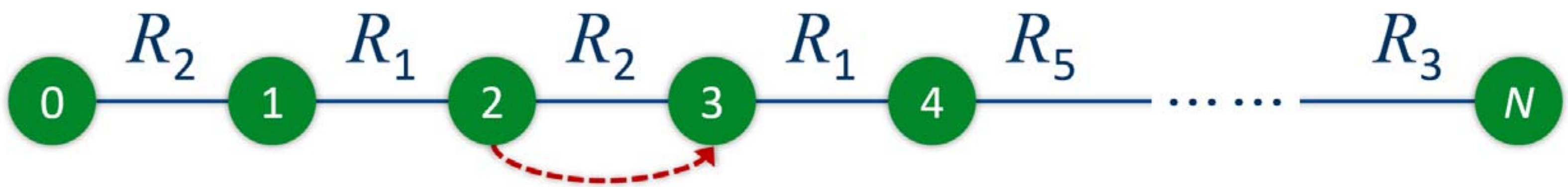
1. Selects an $i \in [N]$ uniformly at random and sends the index $j = \zeta_i \in [n]$ to the player and receives an answer bit a;
2. Performs the projective measurement Π_i on his system and accepts if the outcome is 2 or equals to a.

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 $V_{\mathfrak{R}} \rho V_{\mathfrak{R}}^*$.



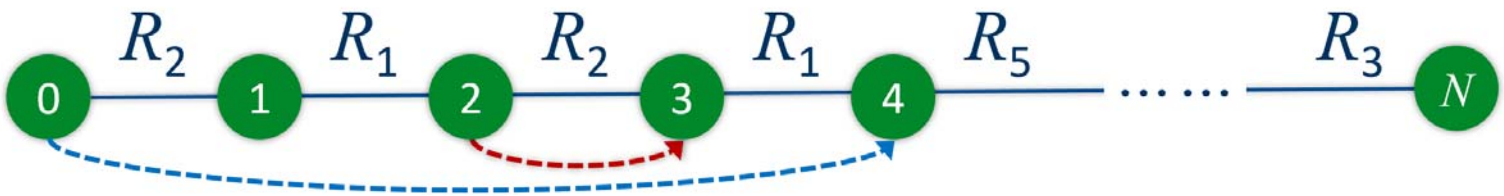
- **Theorem**. Any strategy that has value at least $1-\epsilon$ must use shared state that is $N^{3/2}\epsilon^{1/2}$-close to a history state for $\hat{\mathfrak{R}}$ in trace distance.

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 $\mathbb{C}^{V(G_{\mathrm{prop}})}$ and performs the following two checks with equal probability:

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

6.6

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 $\rho_0 \propto \langle 0|\rho|0\rangle$,

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

MULTI-QUBIT RIGIDITY WITHOUT CONSISTENCY

- Two enhancements to Propagation Games and Constraint Propagation Games

  1. Allow the confusion questions $R_{j|q}$ where $j \in q \subseteq [n]$

     Relate the Single qubit Pauli to Multi-qubit Pauli

  2. Allow the controlled questions $\Lambda_c(R_j)$

     Rearranging operators without consistency

- Multi-Qubit Rigidity

  The player must measure the constant-weight Pauli operators up to some isometry

REASONS TO ENHANCE CONSTRAINT PROPAGATION GAMES

- The rigidity theorem for constraint propagation games allows us to enforce useful conditions such as approximate commutativity and approximate anti-commutativity

$$\mathrm{Re}\,\mathrm{Tr}_{\rho_0}\left(\hat{R}_0\hat{R}_1\hat{R}_0\hat{R}_1\right) \approx \pm 1$$

- However, approximate commutativity and anti-commutativity are not sufficient to guarantee the multi-qubit rigidity

[Chao, Reichardt, Sutherland and Vidick '17]

CHECKING PROVER PROPAGATION

- Consider only the prover propagation part and check that the state is of the form

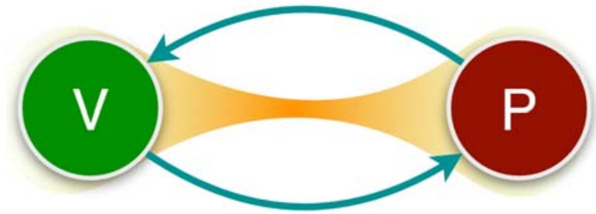
$$|00\rangle|\phi\rangle + |11\rangle(I \otimes W)|\phi\rangle$$

- Extended EPR Game

X	X
Z	Z

+	X	0
+	Z	1

X	X
Z	Z
X	X
Z	Z



- Anti-commutativity and rigidity
- A theory of approximate stabilizers
- To achieve close-to-optimal value, the player must initialize the EPR state and measure honestly

CONCLUSION AND OPEN PROBLEMS

- We proved that any r-player quantum multi-prover interactive protocol can be compressed to a nonlocal game in which messages are of $O(\log n)$ bits
- Nonlocal Games are QMIP*-complete and NEXP-hard
- A combination of ideas in quantum proofs
  - History state and propagation checking
  - Parallelization of quantum proofs
  - Rigidity of nonlocal games
- Exact case versus approximate case *[Slofstra '17]*
- Open problems
  - What is the hardness of the constant precision approximation problem for nonlocal games?
  - Tradeoff between precision and complexity
  - Characterization of QMIP*

THANKS!