arXiv:1505.07432

Classical Verification of Quantum Proofs

Zhengfeng Ji

IQC, UWaterloo

arXiv:1505.07432

Classical Verification of Quantum Proofs

Zhengfeng Ji

IQC, UWaterloo

QCIS, UTS

Classical and quantum proof verification

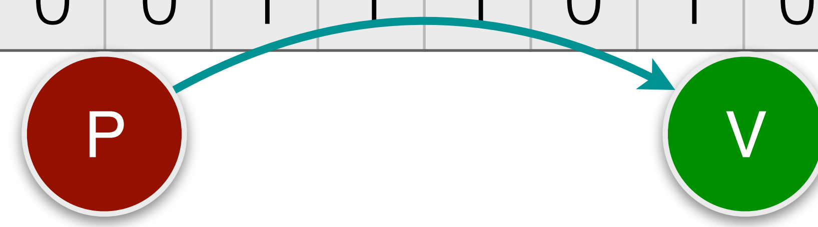
Classical and quantum proof verification

- Proof verification is a central concept in computer science
  - **NP**, **IP**, **MIP**, **PCP**, …

Classical and quantum proof verification

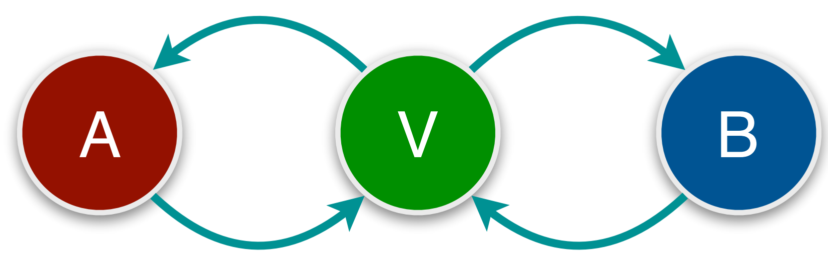
- Proof verification is a central concept in computer science
    - **NP**, **IP**, **MIP**, **PCP**, …

x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	$\dots$
1	0	0	1	1	1	0	1	0	$\dots$



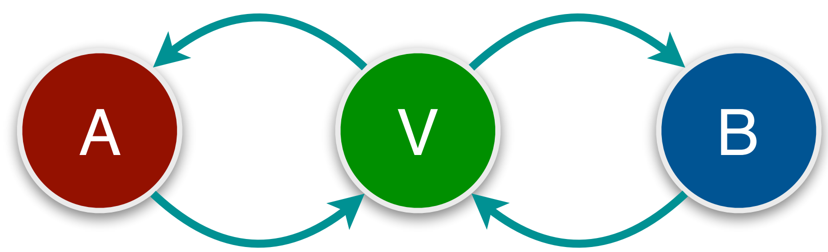
Classical and quantum proof verification

- Proof verification is a central concept in computer science
  - **NP**, **IP**, **MIP**, **PCP**, …



Classical and quantum proof verification

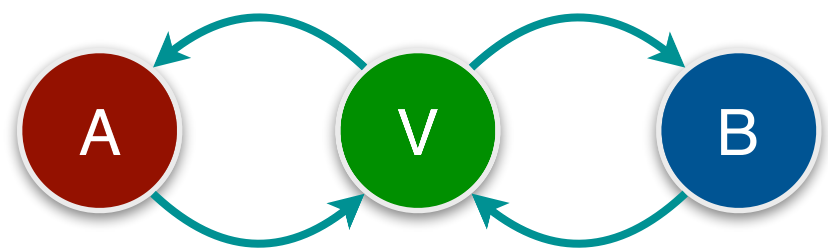
- Proof verification is a central concept in computer science
  - **NP**, **IP**, **MIP**, **PCP**, …



- Cook-Levin theorem: 3-SAT is **NP**-complete
  - 3-SAT, G3C, Ising

Classical and quantum proof verification

- Proof verification is a central concept in computer science
  - **NP**, **IP**, **MIP**, **PCP**, …

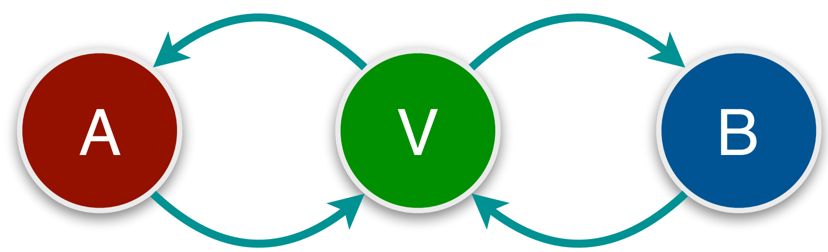


- Cook-Levin theorem: 3-SAT is **NP**-complete
  - 3-SAT, G3C, Ising

$$(x_1 \vee x_3 \vee x_5) \wedge (x_2 \vee \neg x_3 \vee \neg x_5) \wedge \ldots$$

Classical and quantum proof verification

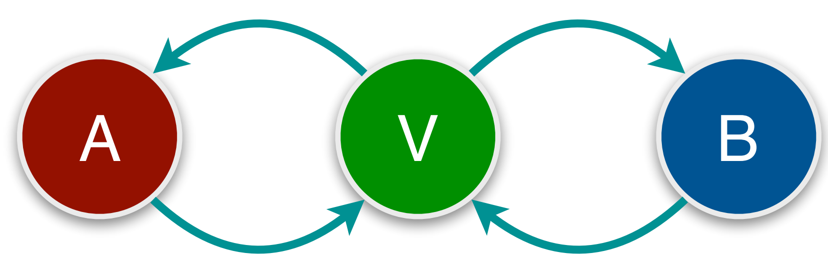
- Proof verification is a central concept in computer science
  - **NP**, **IP**, **MIP**, **PCP**, …



- Cook-Levin theorem: 3-SAT is **NP**-complete
  - 3-SAT, G3C, Ising $(x_1 \vee x_3 \vee x_5) \wedge (x_2 \vee \neg x_3 \vee \neg x_5) \wedge \ldots$
- Quantum proof verification
  - **QMA**, **QIP**, **MIP***, **QMIP**, Quantum **PCP**?

Classical and quantum proof verification

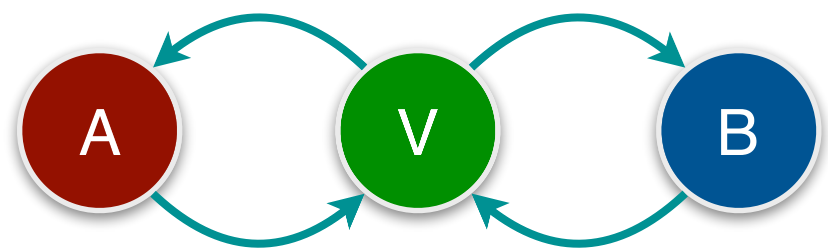
- Proof verification is a central concept in computer science
  - **NP**, **IP**, **MIP**, **PCP**, …



- Cook-Levin theorem: 3-SAT is **NP**-complete
  - 3-SAT, G3C, Ising $(x_1 \vee x_3 \vee x_5) \wedge (x_2 \vee \neg x_3 \vee \neg x_5) \wedge \ldots$
- Quantum proof verification
  - **QMA**, **QIP**, **MIP***, **QMIP**, Quantum **PCP**?
- Local Hamiltonian problem

Classical and quantum proof verification

- Proof verification is a central concept in computer science
    - **NP**, **IP**, **MIP**, **PCP**, …



- Cook-Levin theorem: 3-SAT is **NP**-complete
    - 3-SAT, G3C, Ising

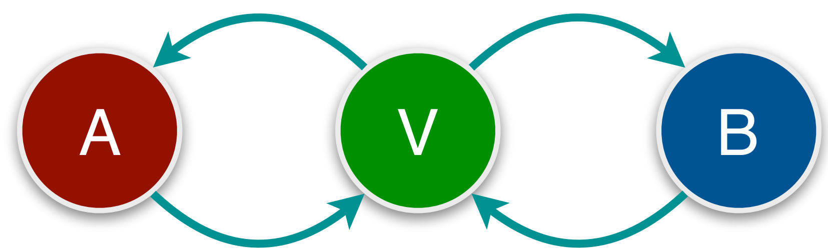
$$(x_1 \vee x_3 \vee x_5) \wedge (x_2 \vee \neg x_3 \vee \neg x_5) \wedge \ldots$$

- Quantum proof verification
    - **QMA**, **QIP**, **MIP***, **QMIP**, Quantum **PCP**?
- Local Hamiltonian problem

$$H = \sum_{j=1}^{m} H_j$$

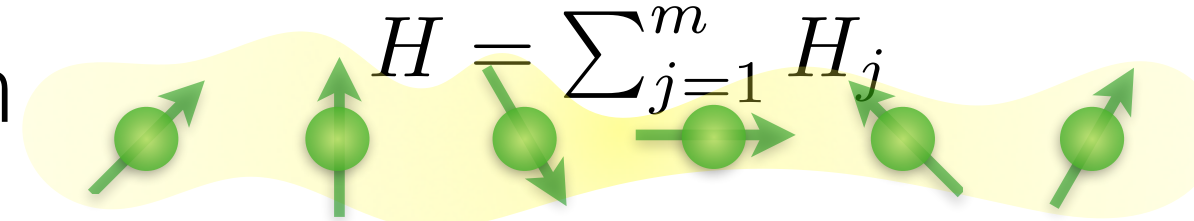
Classical and quantum proof verification

- Proof verification is a central concept in computer science
    - **NP**, **IP**, **MIP**, **PCP**, …



- Cook-Levin theorem: 3-SAT is **NP**-complete
    - 3-SAT, G3C, Ising $(x_1 \vee x_3 \vee x_5) \wedge (x_2 \vee \neg x_3 \vee \neg x_5) \wedge \ldots$
- Quantum proof verification
    - **QMA**, **QIP**, **MIP***, **QMIP**, Quantum **PCP**?
- Local Hamiltonian problem

$$H = \sum_{j=1}^{m} H_j$$



Multi-player one-round games for NP

Multi-player one-round games for NP

- Proof verification without seeing the whole proof

$$(x_1 \vee x_3 \vee x_5) \wedge (x_2 \vee \neg x_3 \vee \neg x_5) \wedge \ldots$$

x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	$\ldots$
-	0	0	-	1	-	-	-	-	$\ldots$

Multi-player one-round games for NP

- Proof verification without seeing the whole proof

$$(x_1 \vee x_3 \vee x_5) \wedge \boxed{(x_2 \vee \neg x_3 \vee \neg x_5)} \wedge \ldots$$

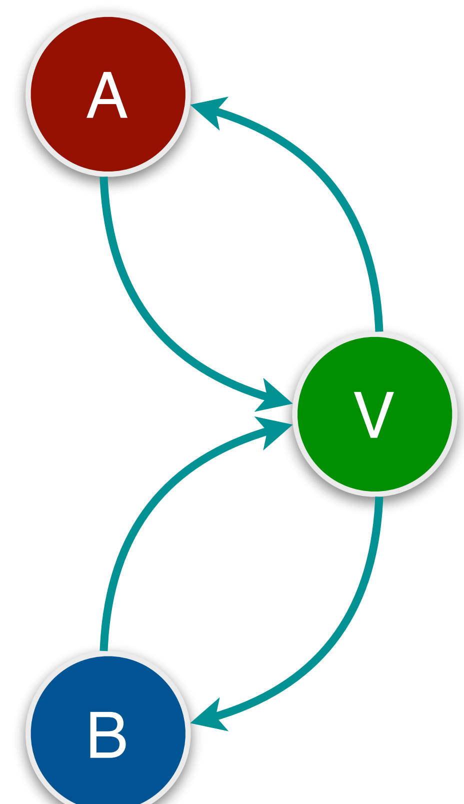
x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	…
-	0	0	-	1	-	-	-	-	…

Multi-player one-round games for NP

- Proof verification without seeing the whole proof

$$(x_1 \vee x_3 \vee x_5) \wedge \boxed{(x_2 \vee \neg x_3 \vee \neg \boxed{x_5})} \wedge \ldots$$

x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	...
-	0	0	-	1	-	-	-	-	...



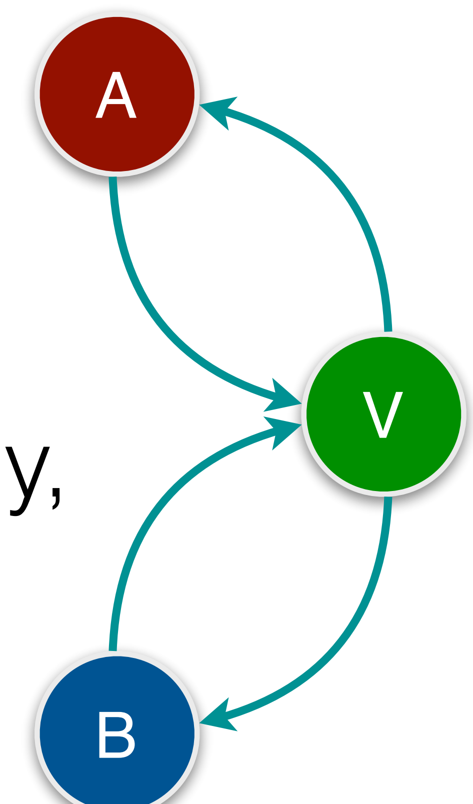
Multi-player one-round games for NP

- Proof verification without seeing the whole proof

$$(x_1 \vee x_3 \vee x_5) \wedge (x_2 \vee \neg x_3 \vee \neg x_5) \wedge \ldots$$

x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	$\ldots$
-	0	0	-	1	-	-	-	-	$\ldots$

- The power of the second prover
  - Query a variable in the clause randomly, check consistency (oracularization)



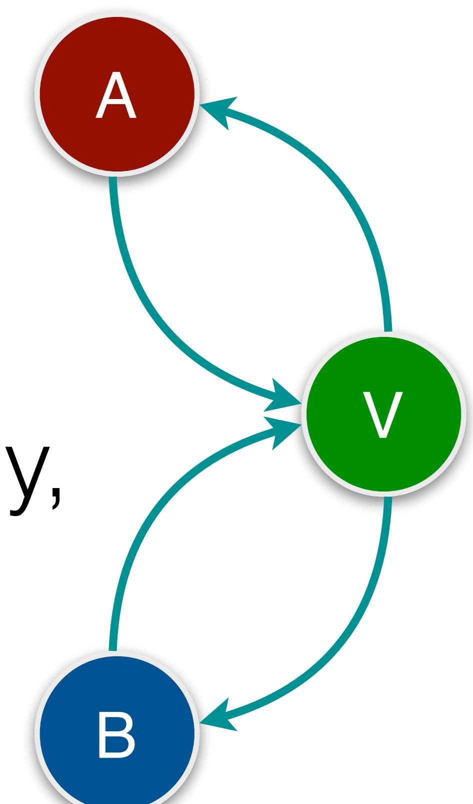
Multi-player one-round games for NP

- Proof verification without seeing the whole proof

$$(x_1 \vee x_3 \vee x_5) \wedge \boxed{(x_2 \vee \neg x_3 \vee \neg \boxed{x_5})} \wedge \ldots$$

x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	$\ldots$
-	0	0	-	1	-	-	-	-	$\ldots$

- The power of the second prover
  - Query a variable in the clause randomly, check consistency (oracularization)
- **NP**-hardness of multi-player games

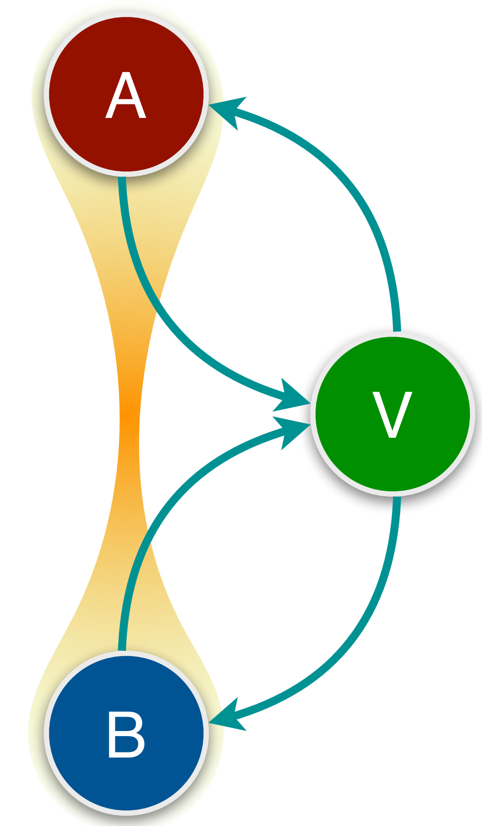


The power of multiple entangled provers

The power of multiple entangled provers

- Bell inequalities
- Entanglement can either weaken or strengthen the expressive power

[Cleve et al. 04]



The power of multiple entangled provers

- Bell inequalities
- Entanglement can either weaken or strengthen the expressive power

[Cleve et al. 04]

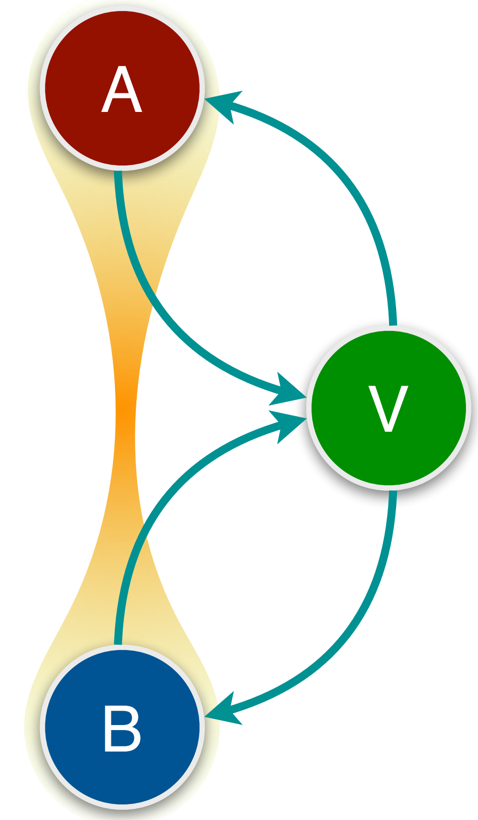
- **NP**-hardness

[Kempe et al. 08]

[Ito, Kobayashi, Matsumoto 09]

- **NEXP**-hardness, at least as powerful as classical

[Ito, Vidick 12]



The power of multiple entangled provers

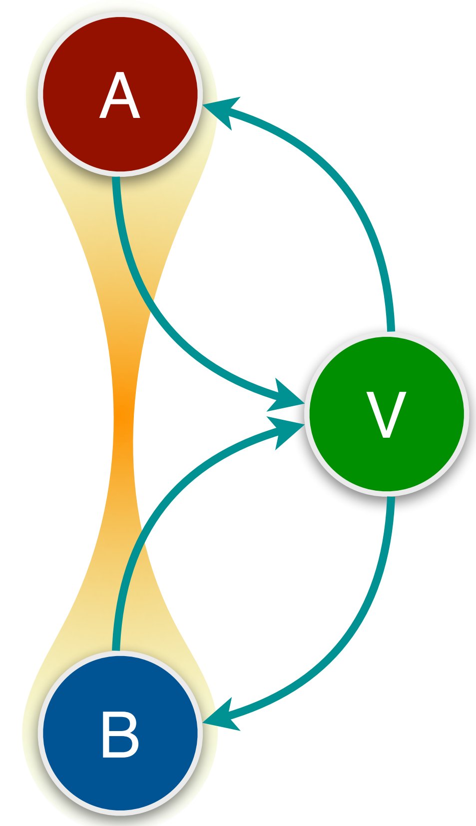
- Bell inequalities
- Entanglement can either weaken or strengthen the expressive power

  [Cleve et al. 04]
- **NP**-hardness

  [Kempe et al. 08]

  [Ito, Kobayashi, Matsumoto 09]
- **NEXP**-hardness, at least as powerful as classical

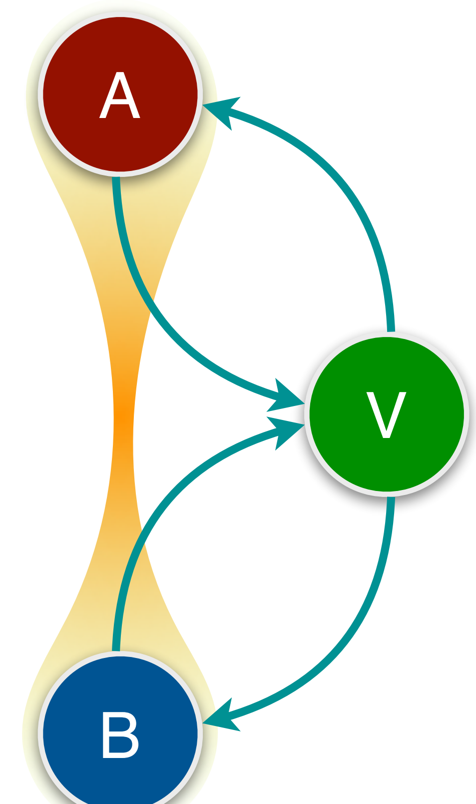
  [Ito, Vidick 12]
- Entanglement-resistant techniques



The power of multiple entangled provers

- Bell inequalities
- Entanglement can either weaken or strengthen the expressive power
  [Cleve et al. 04]
- **NP**-hardness
  [Kempe et al. 08]
  [Ito, Kobayashi, Matsumoto 09]
- **NEXP**-hardness, at least as powerful as classical
  [Ito, Vidick 12]
- Entanglement-resistant techniques

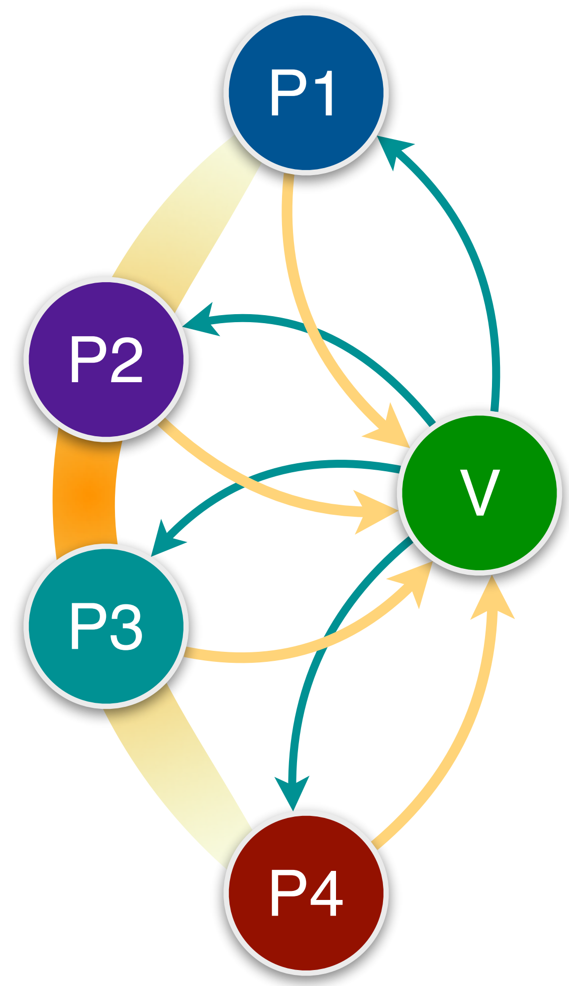
“Quantum hardness” for entangled games?



Multi-player games for QMA

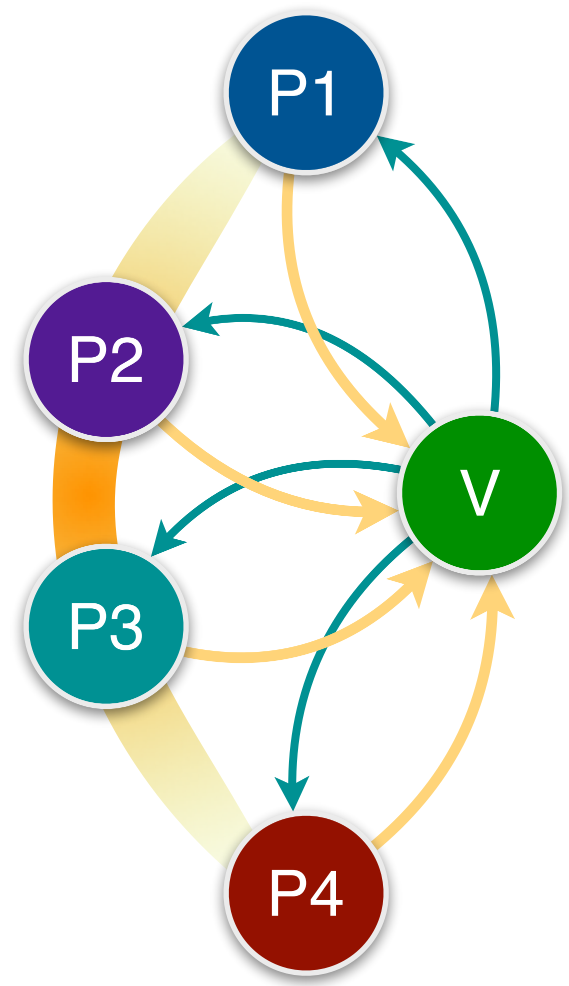
Multi-player games for QMA

- Fitzsimons-Vidick protocol



Multi-player games for QMA

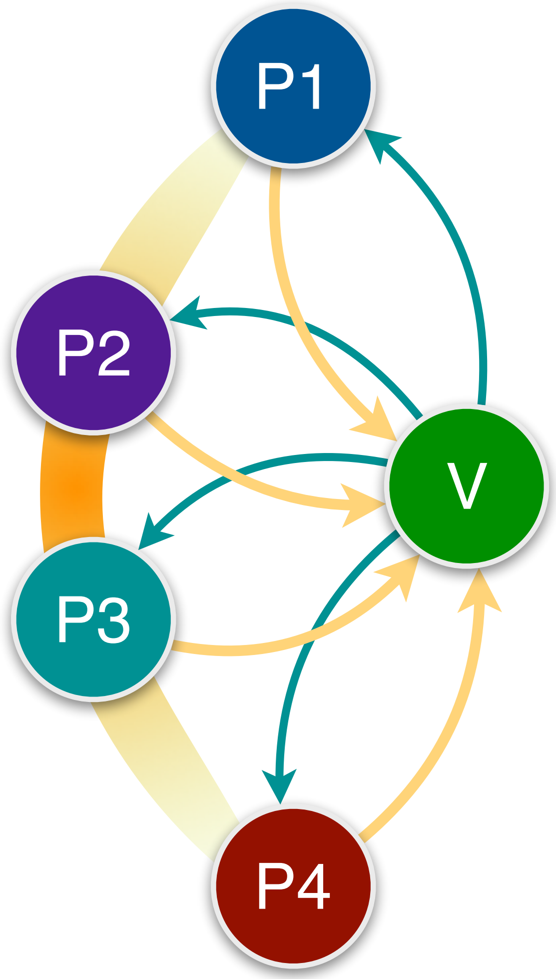
- Fitzsimons-Vidick protocol
- Encode the proof using the 4-qubit quantum error detecting code and do the following with equal probability:
  - Perform the encoding check
  - Perform the energy check



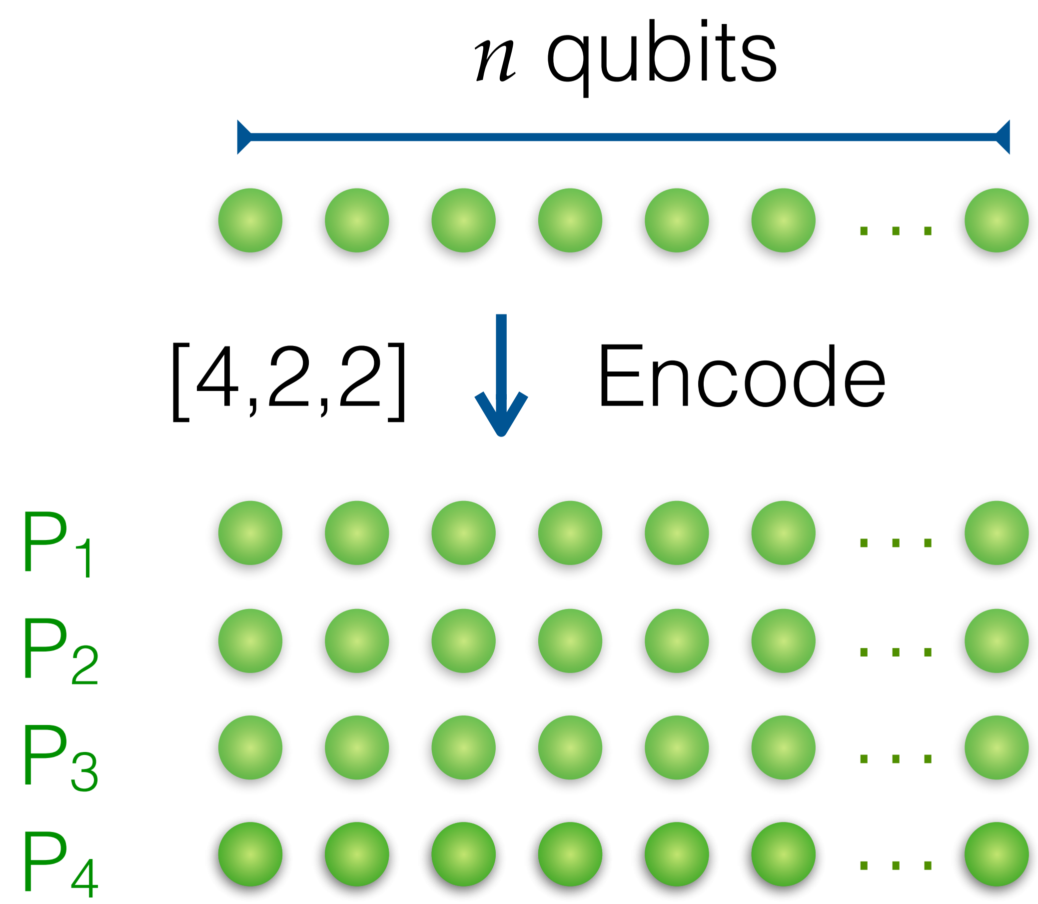
Multi-player games for QMA

- Fitzsimons-Vidick protocol
- Encode the proof using the 4-qubit quantum error detecting code and do the following with equal probability:
  - Perform the encoding check
  - Perform the energy check
- Quantum oracularization
  - Classical oracularization as an error detecting code

$0 \mapsto 00,\ 1 \mapsto 11$

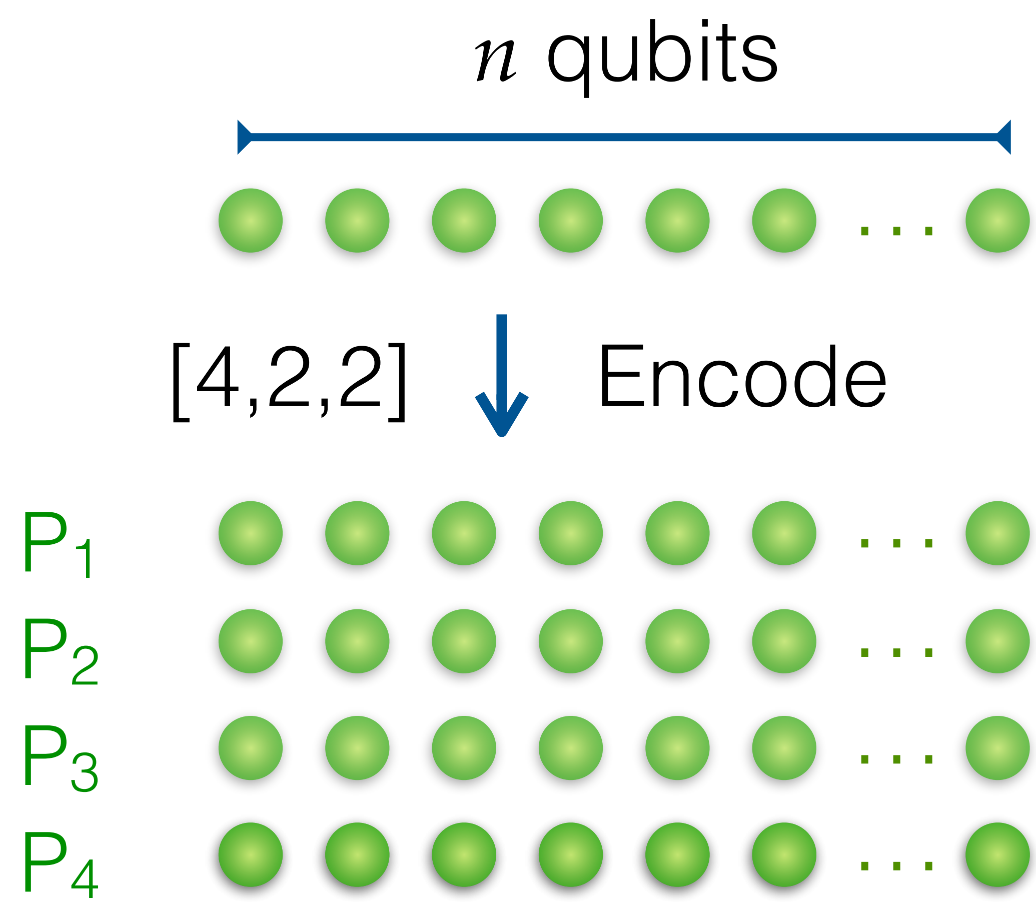


Fitzsimons-Vidick protocol



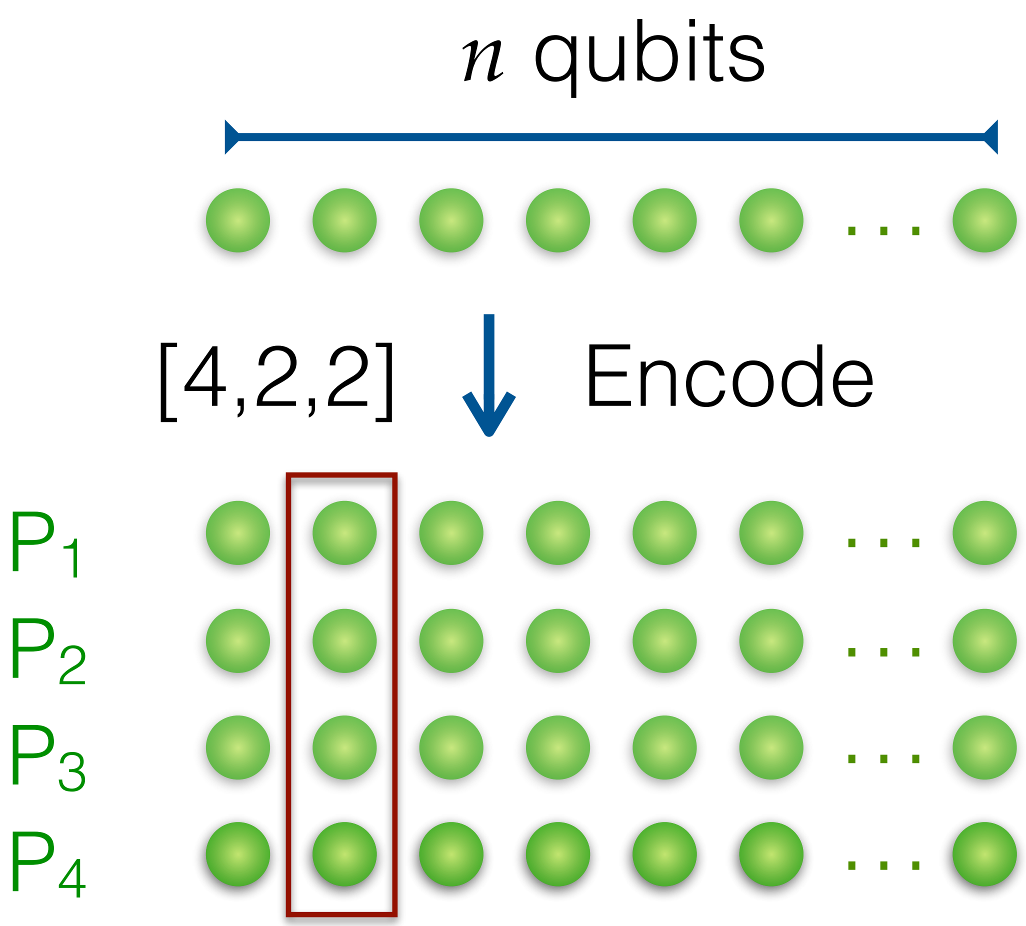
Fitzsimons-Vidick protocol

- Encode and distribute among the four provers



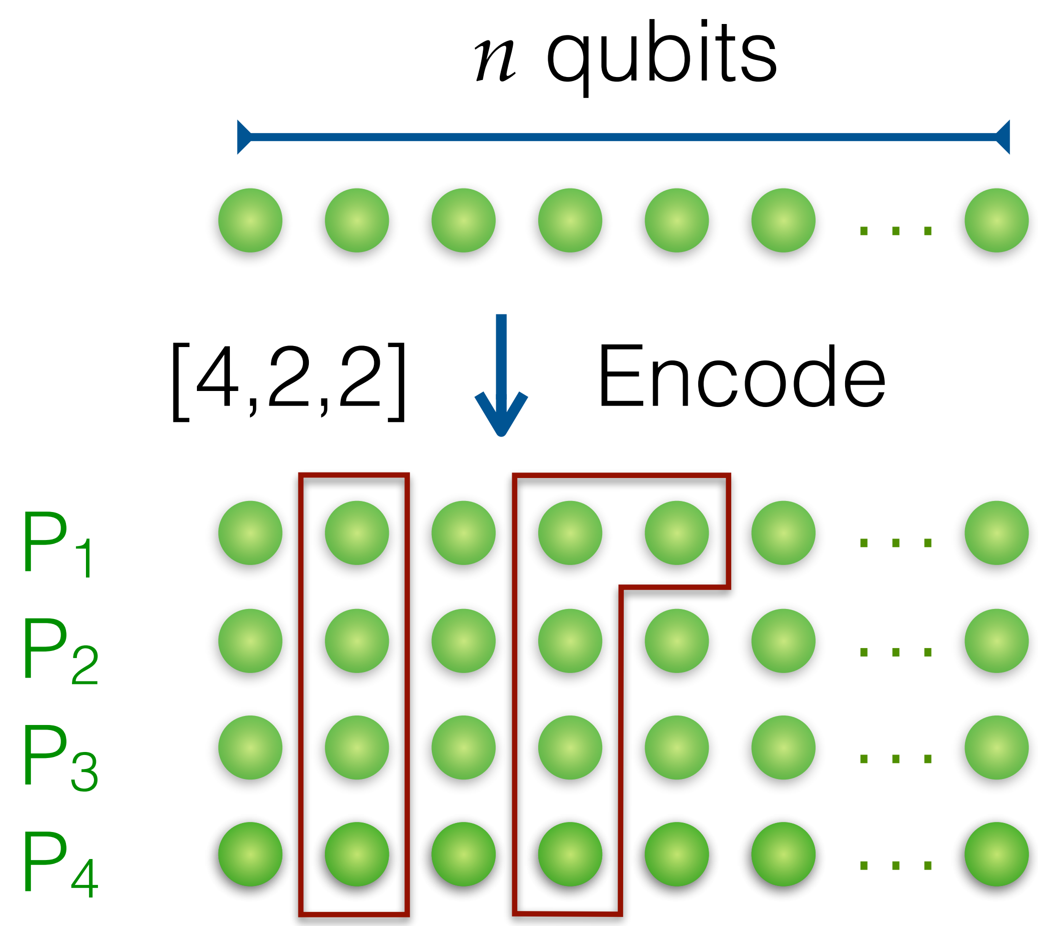
Fitzsimons-Vidick protocol

- Encode and distribute among the four provers
- Encoding check



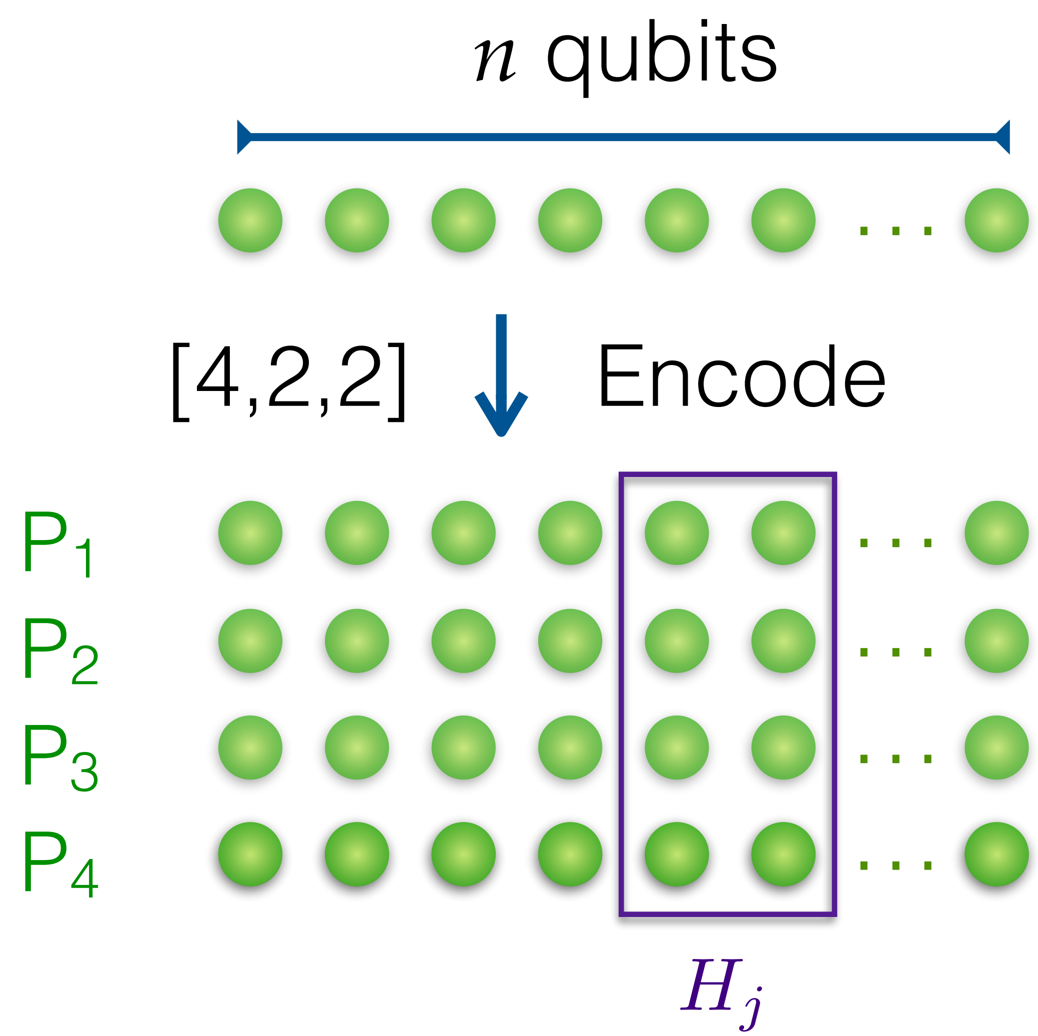
Fitzsimons-Vidick protocol

- Encode and distribute among the four provers
- Encoding check



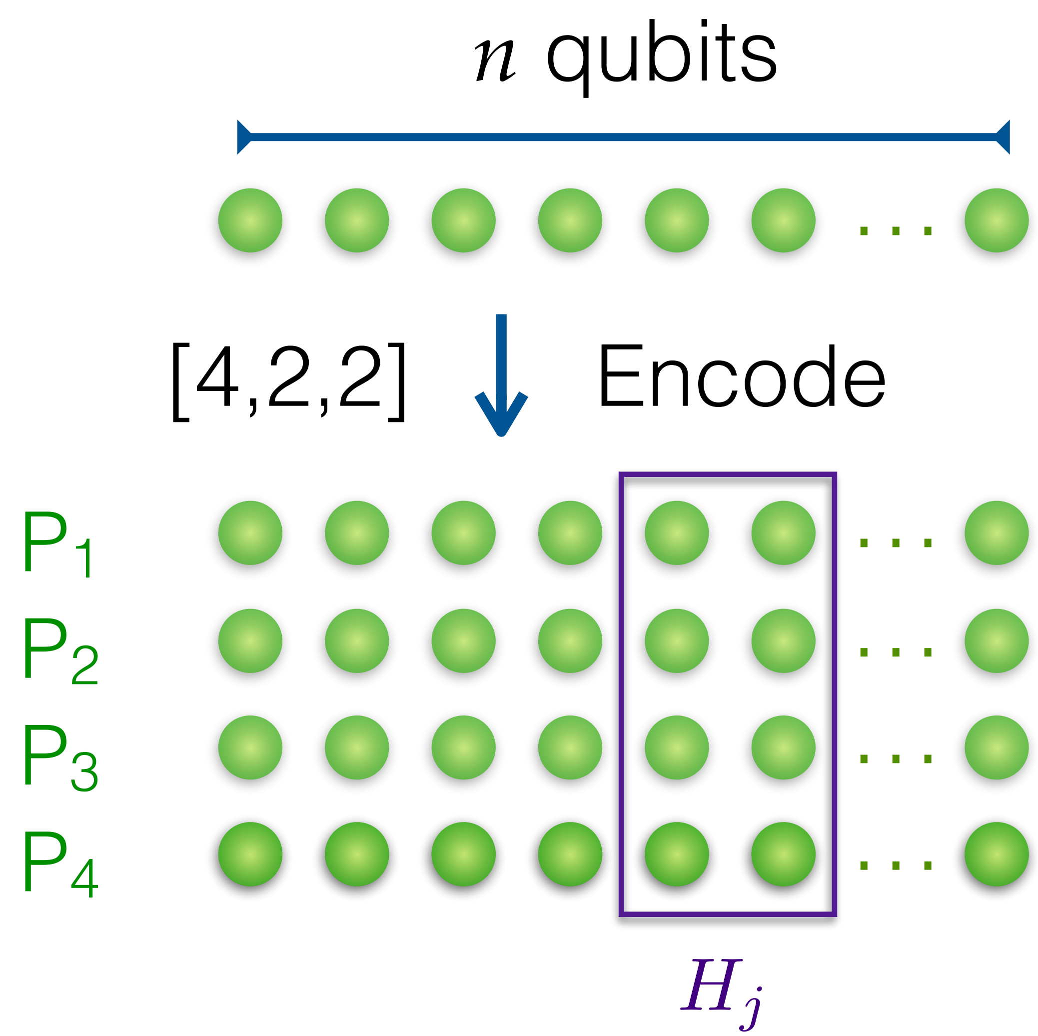
Fitzsimons-Vidick protocol

- Encode and distribute among the four provers
- Encoding check
- Energy check



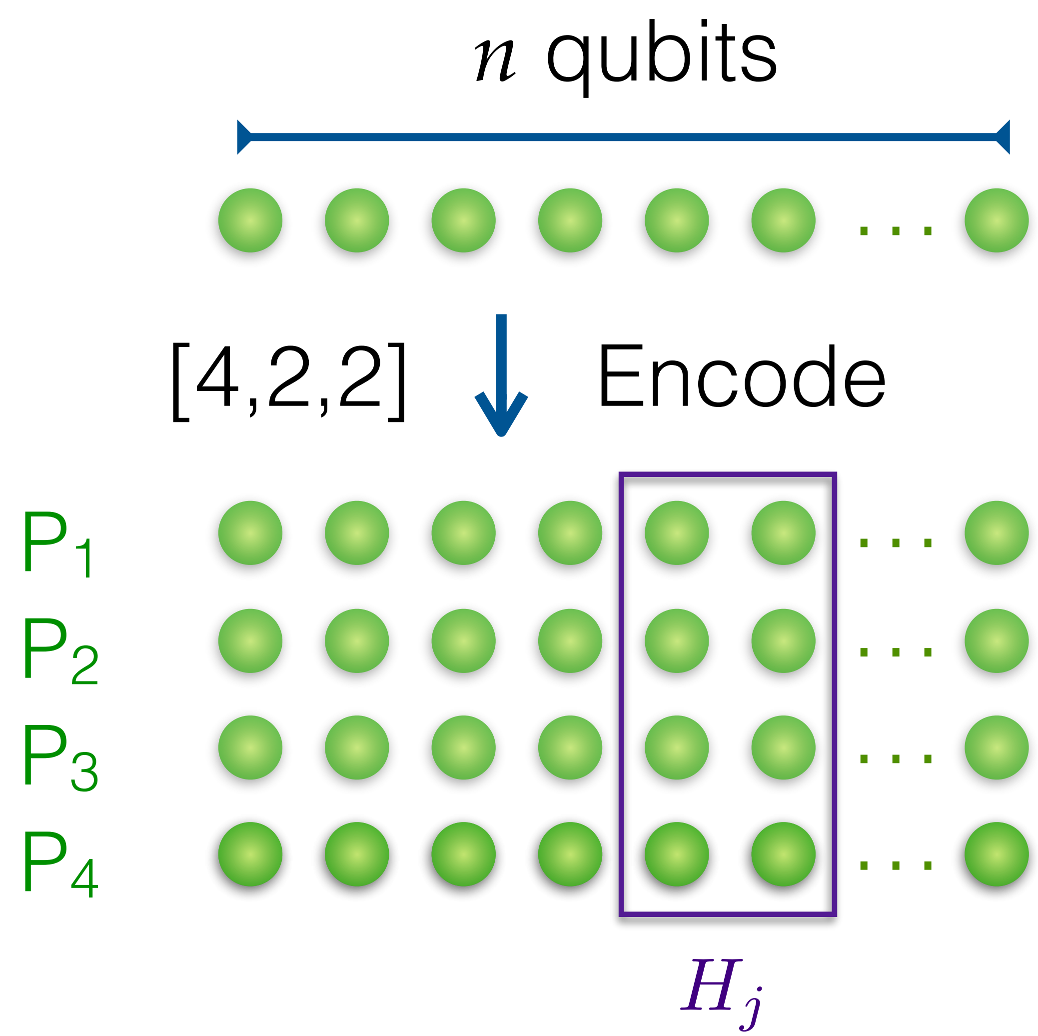
Fitzsimons-Vidick protocol

- Encode and distribute among the four provers
- Encoding check
- Energy check
- Questions: $O(\log n)$ bits
- Answers: $O(1)$ qubits



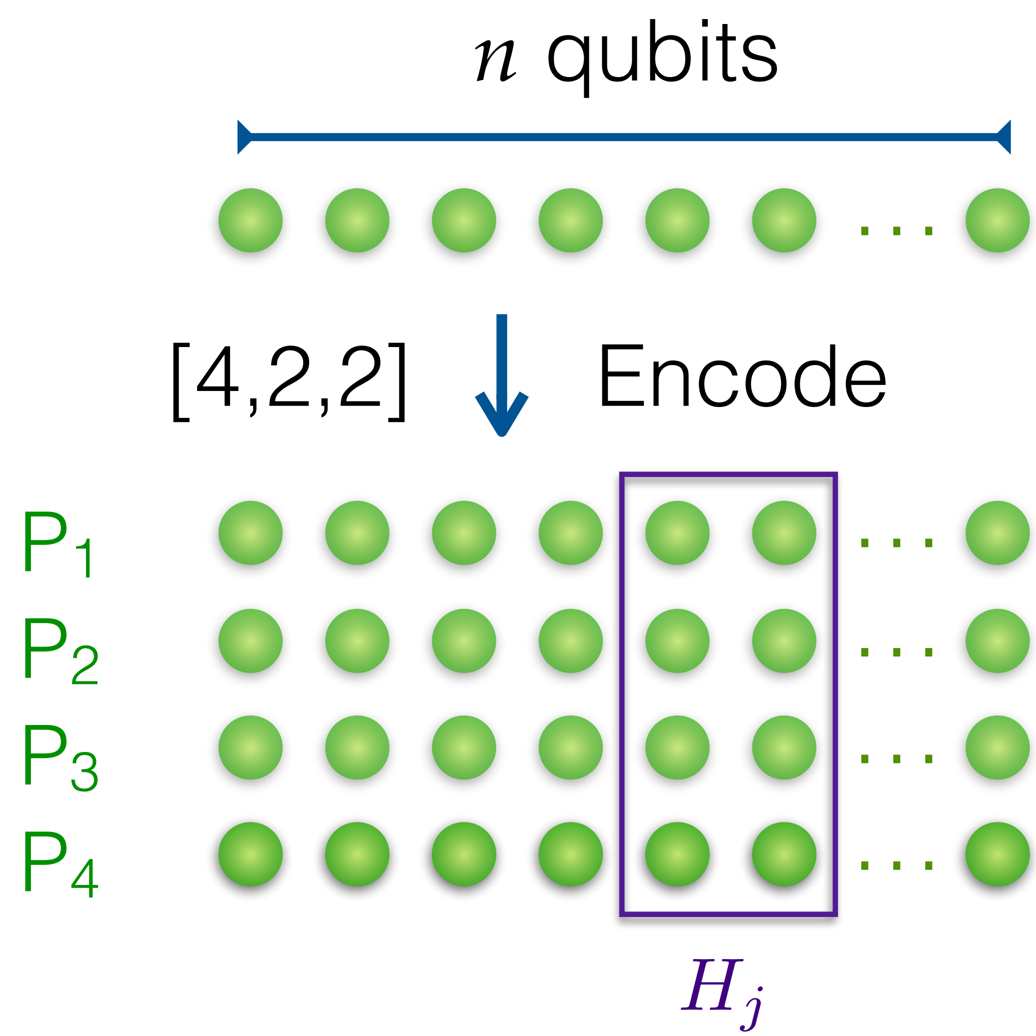
Fitzsimons-Vidick protocol

- Encode and distribute among the four provers
- Encoding check
- Energy check
- Questions: $O(\log n)$ bits
- Answers: $O(1)$ ~~q~~ubits



Fitzsimons-Vidick protocol

- Encode and distribute among the four provers
- Encoding check
- Energy check
- Questions: $O(\log n)$ bits
- Answers: $O(1)$ ~~q~~ubits
- De-quantization of both the answer messages and verifier

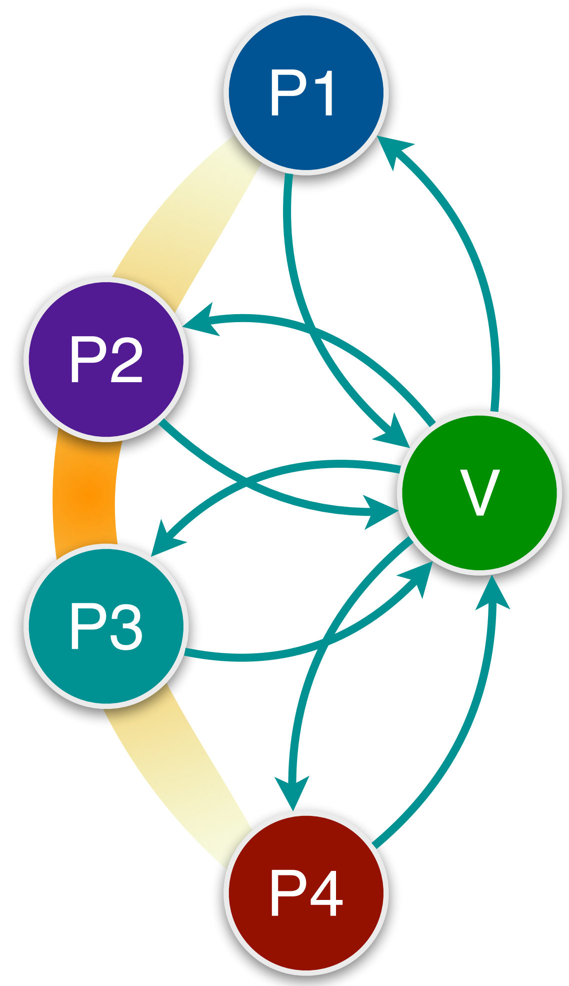


Main results

Main results

- A 4-player protocol for the local Hamiltonian problem

Questions: logarithmic number of bits,
Answers: constant number of bits

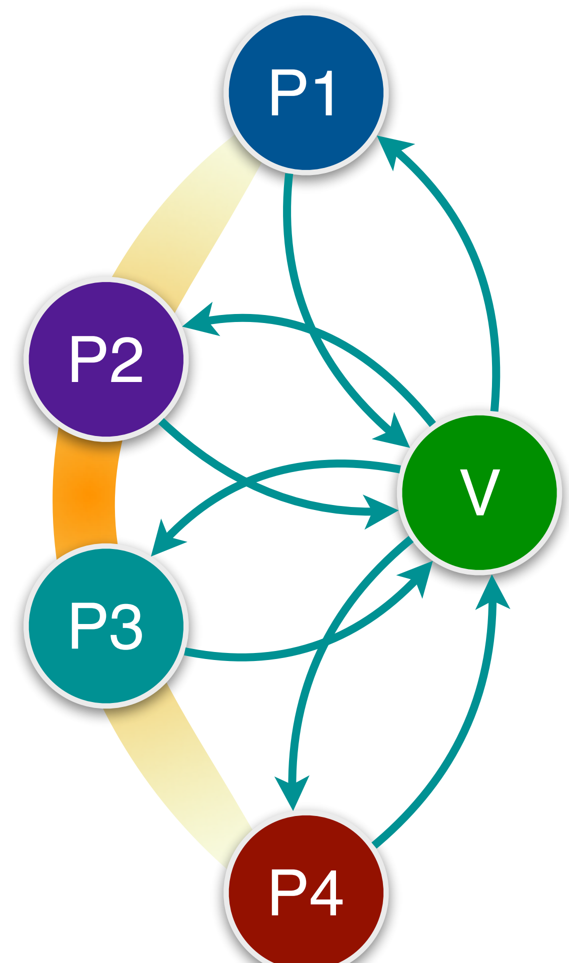


Main results

- A 4-player protocol for the local Hamiltonian problem

  Questions: logarithmic number of bits,
  Answers: constant number of bits

- Entangled games are **QMA**-hard, an improvement of the known **NP**-hardness results



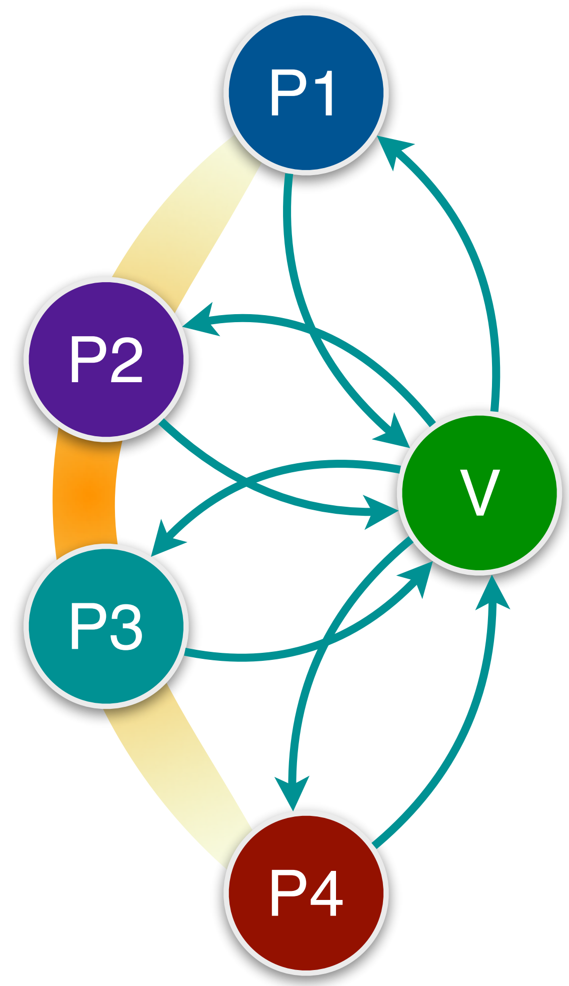
Main results

- A 4-player protocol for the local Hamiltonian problem

  Questions: logarithmic number of bits,
  Answers: constant number of bits

- Entangled games are **QMA**-hard, an improvement of the known **NP**-hardness results

- Essential use the shared entanglement, quantum hardness of entangled games



Main results

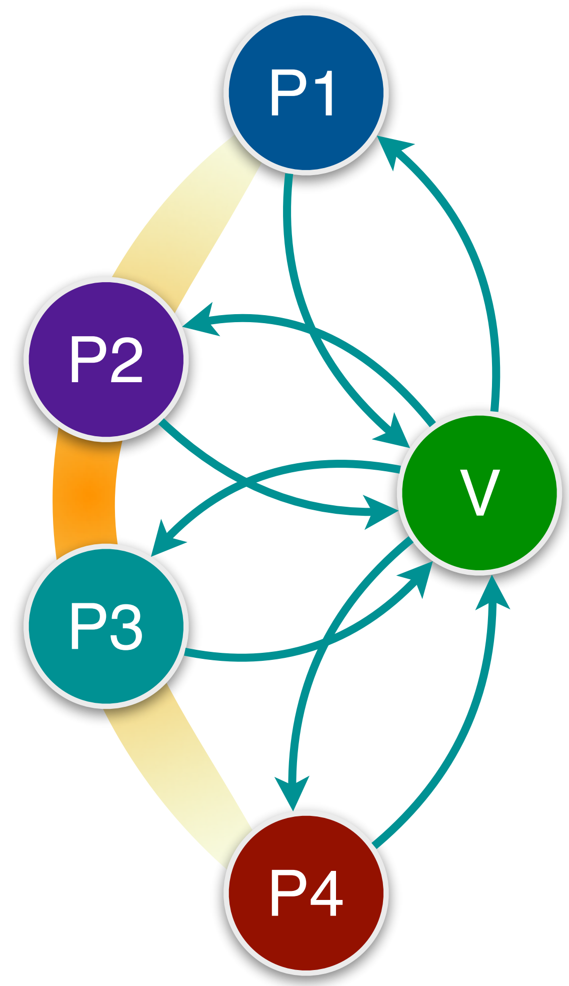
- A 4-player protocol for the local Hamiltonian problem

  Questions: logarithmic number of bits,
  Answers: constant number of bits

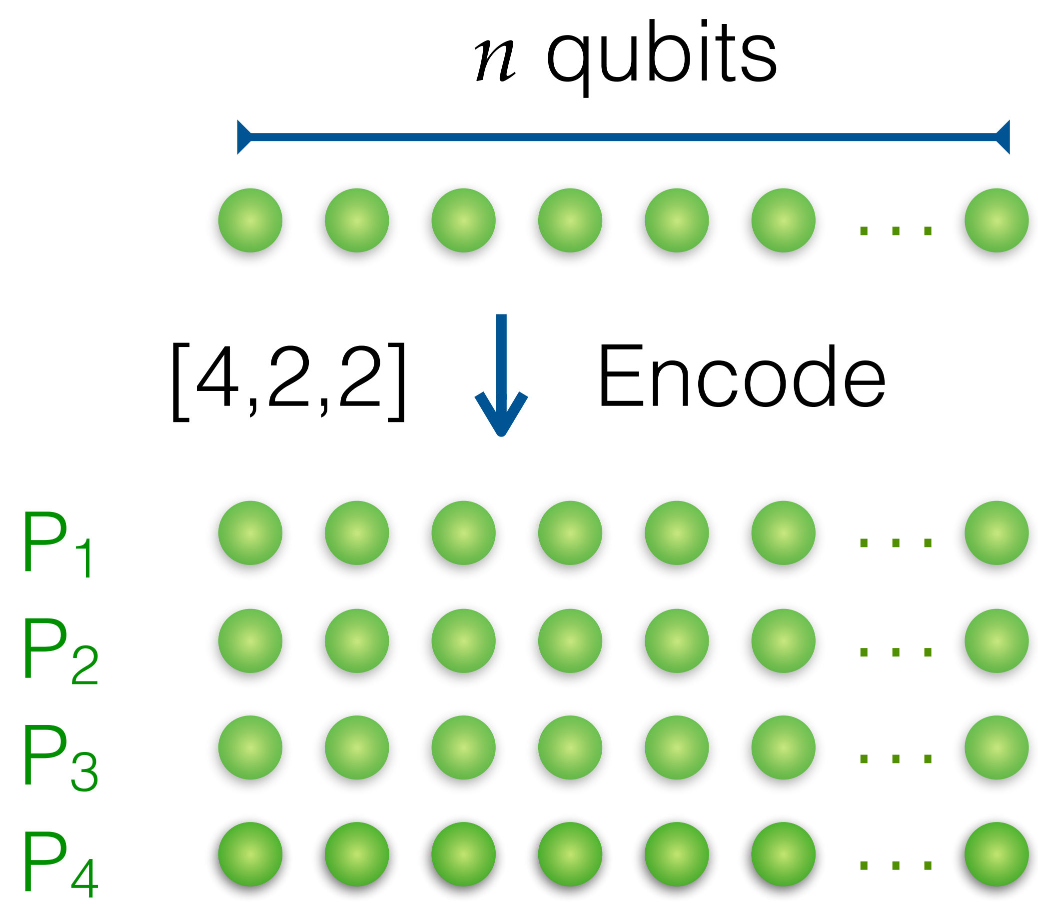
- Entangled games are **QMA**-hard, an improvement of the known **NP**-hardness results

- Essential use the shared entanglement, quantum hardness of entangled games

- For exponentially small gapped c,s, **MIP**$\subsetneq$**MIP***(4,1,c,s) under assumptions

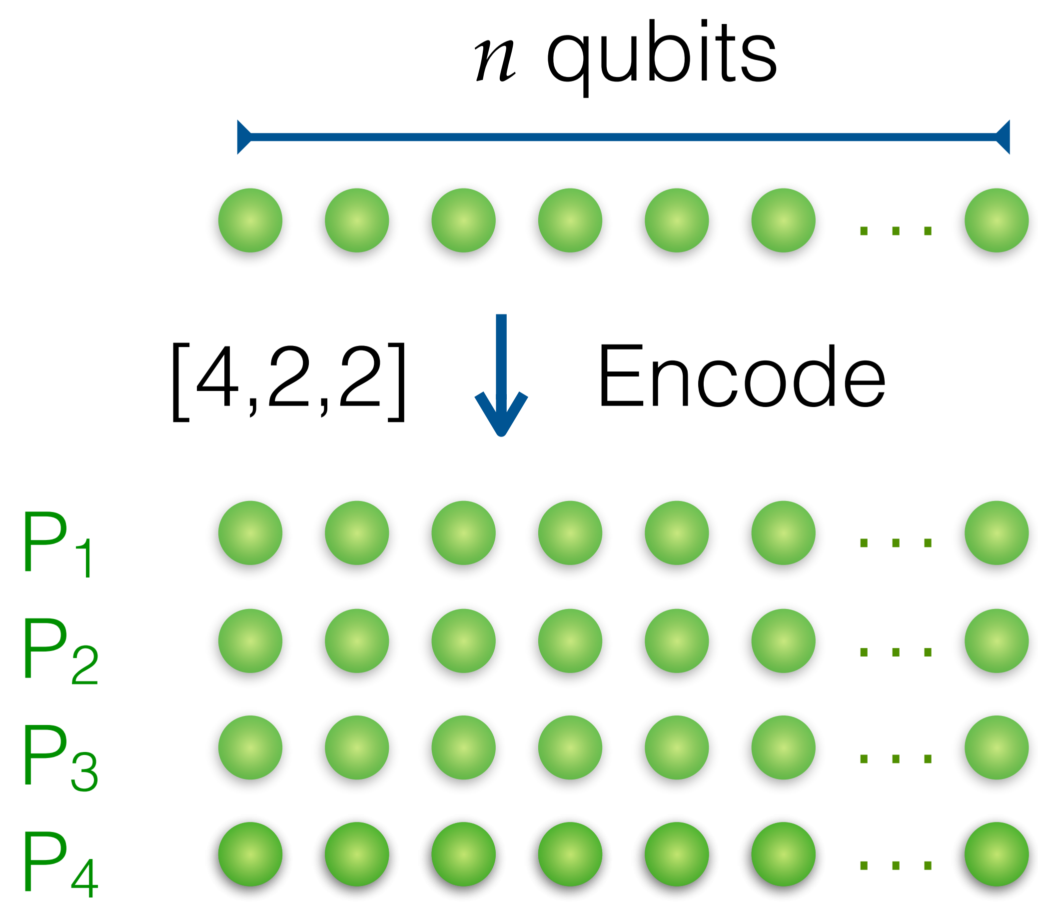


Overview of the protocol



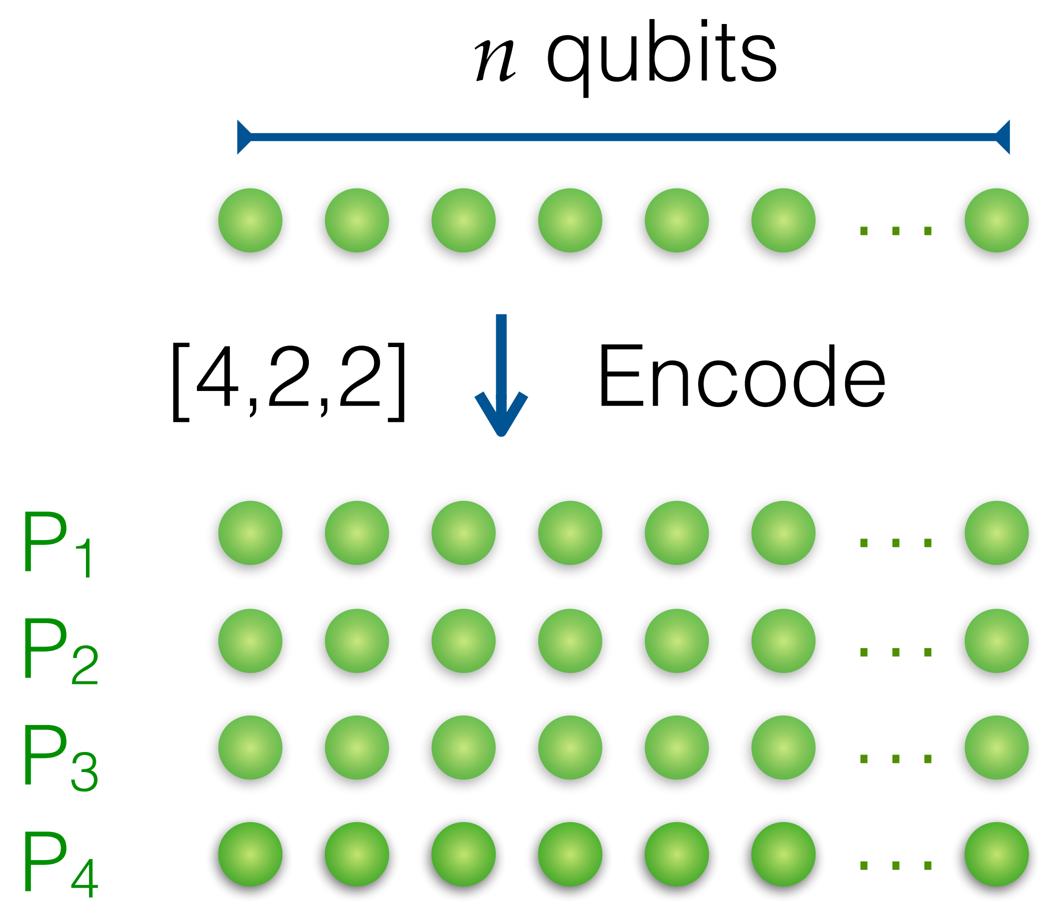
Overview of the protocol

- Follows Fitzsimons-Vidick protocol very closely



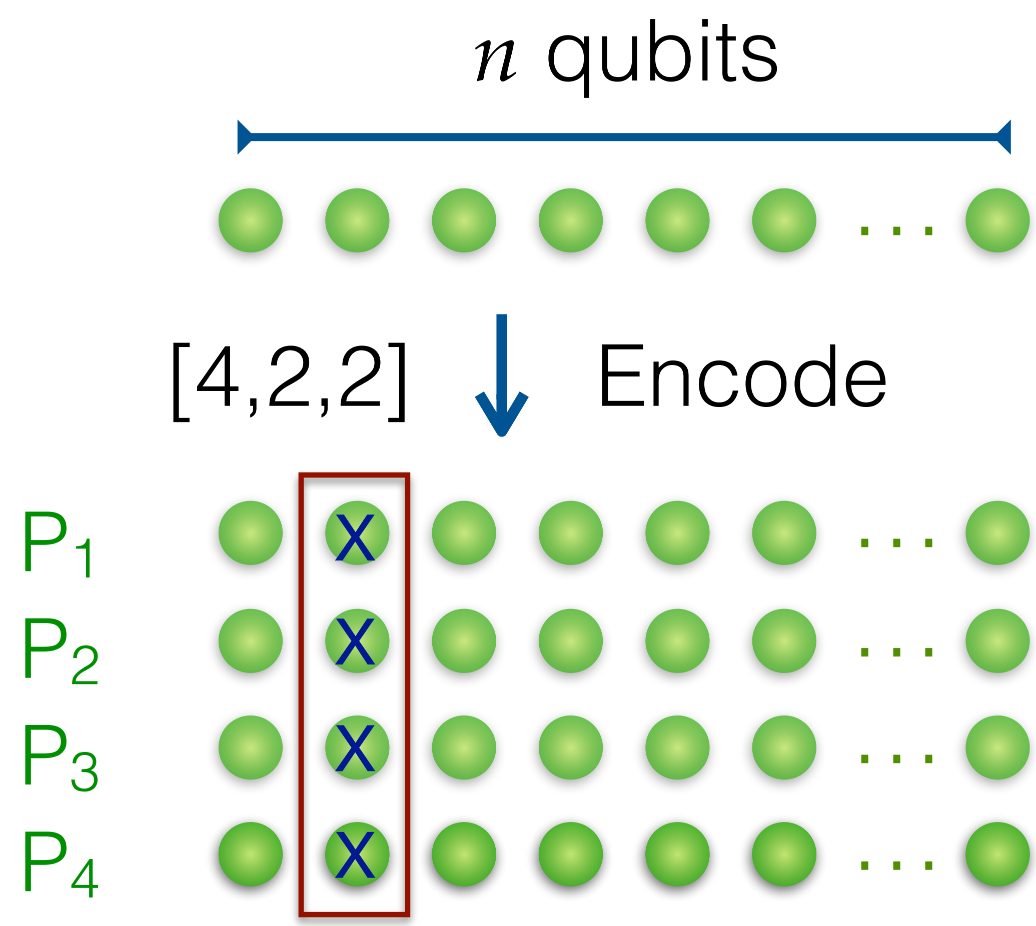
Overview of the protocol

- Follows Fitzsimons-Vidick protocol very closely
- Sends measurement specifications and asks for the outcome instead of asking for qubits from the provers



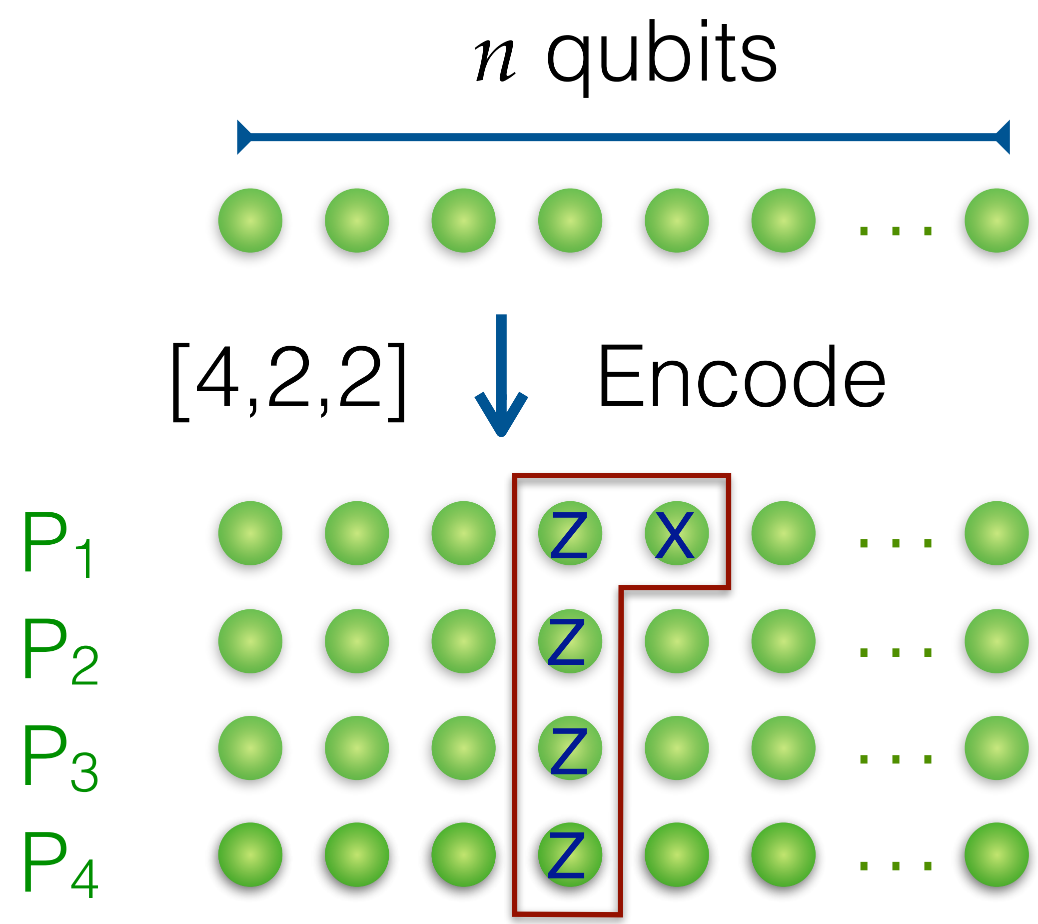
Overview of the protocol

- Follows Fitzsimons-Vidick protocol very closely
- Sends measurement specifications and asks for the outcome instead of asking for qubits from the provers



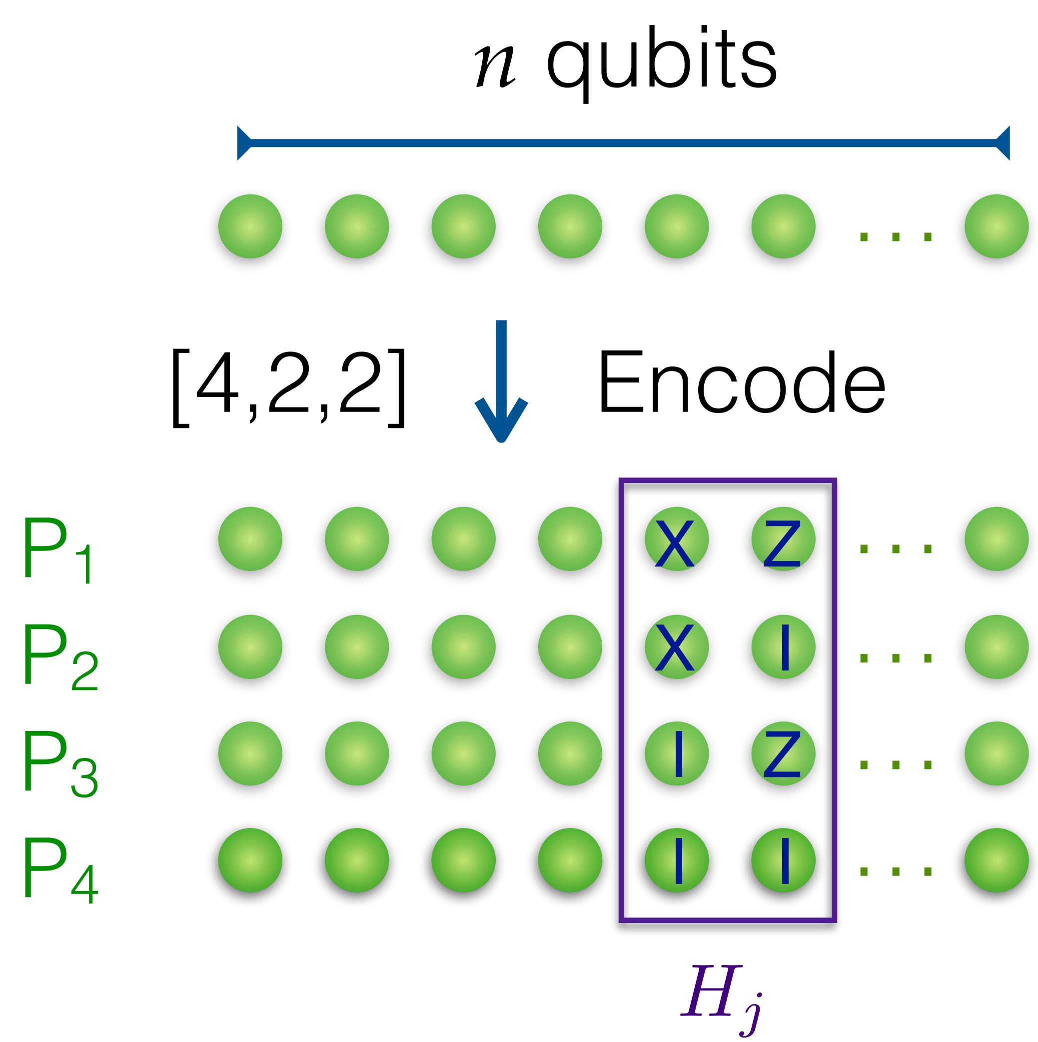
Overview of the protocol

- Follows Fitzsimons-Vidick protocol very closely
- Sends measurement specifications and asks for the outcome instead of asking for qubits from the provers



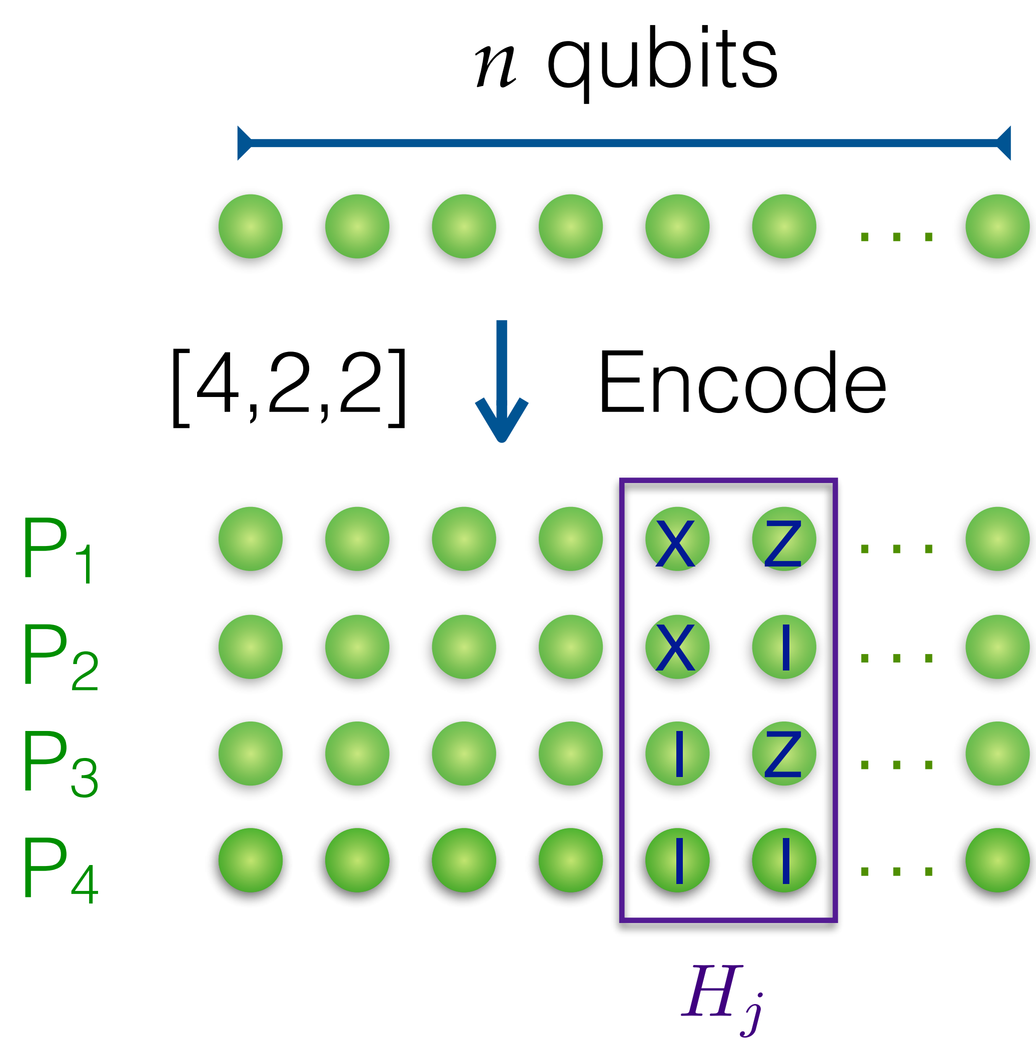
Overview of the protocol

- Follows Fitzsimons-Vidick protocol very closely
- Sends measurement specifications and asks for the outcome instead of asking for qubits from the provers



Overview of the protocol

- Follows Fitzsimons-Vidick protocol very closely
- Sends measurement specifications and asks for the outcome instead of asking for qubits from the provers
- How can we trust the provers?



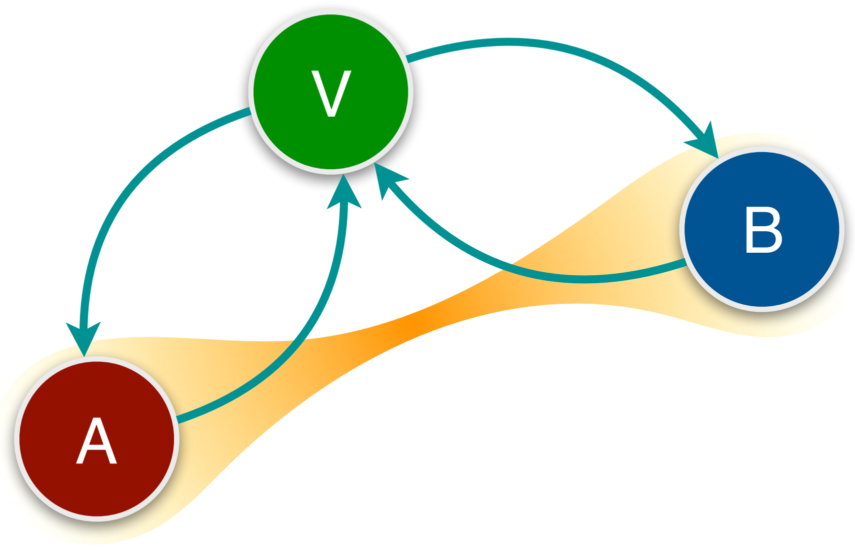
Where are the qubits?

Where are the qubits?

- The classical verifier can only collect information about Pr[answers $a,b,c,\ldots$ | questions $s,t,u,\ldots$]

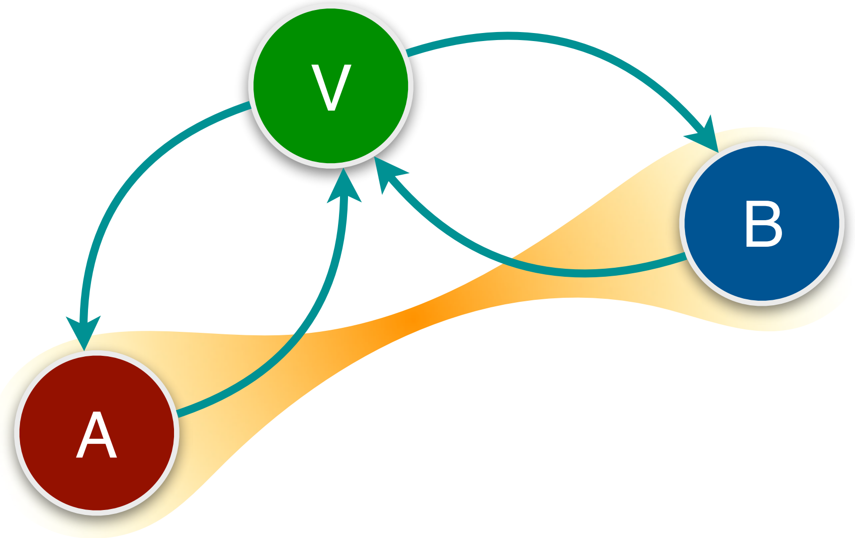
Where are the qubits?

- The classical verifier can only collect information about Pr[answers $a,b,c,\ldots$ | questions $s,t,u,\ldots$]
- Alice and Bob want to prove that they have jointly prepared a quantum state



Where are the qubits?

- The classical verifier can only collect information about Pr[answers $a,b,c,\ldots$ | questions $s,t,u,\ldots$]
- Alice and Bob want to prove that they have jointly prepared a quantum state
- Example I: EPR

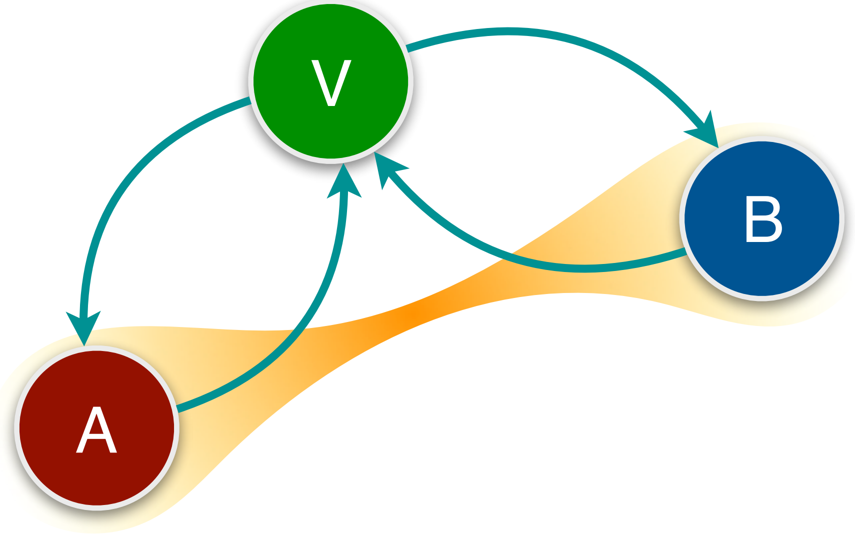


Where are the qubits?

- The classical verifier can only collect information about Pr[answers $a,b,c,\ldots$ | questions $s,t,u,\ldots$]

- Alice and Bob want to prove that they have jointly prepared a quantum state
- Example I: EPR
  - Use CHSH rigidity

[Reichardt, Unger, Vazirani 13]



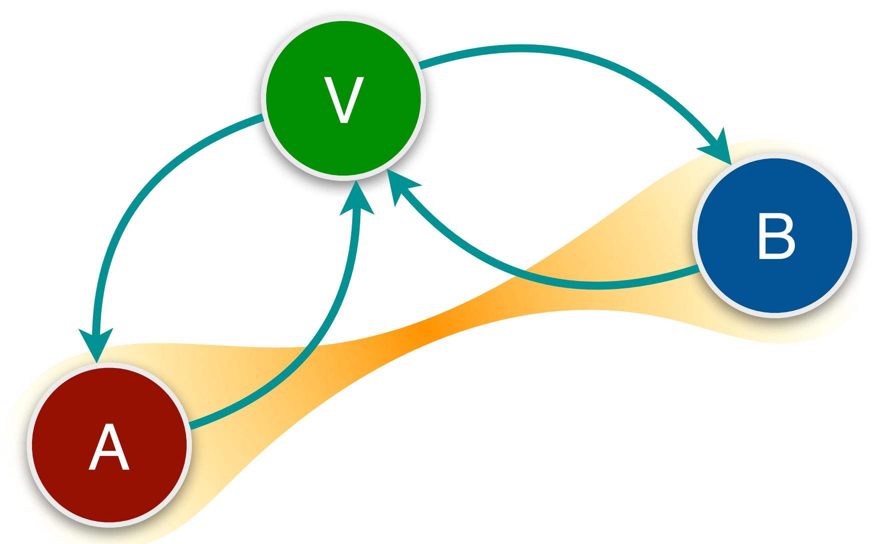
Where are the qubits?

- The classical verifier can only collect information about Pr[answers $a,b,c,\ldots$ | questions $s,t,u,\ldots$]

- Alice and Bob want to prove that they have jointly prepared a quantum state
- Example I: EPR
    - Use CHSH rigidity

[Reichardt, Unger, Vazirani 13]

- Example II: Werner states



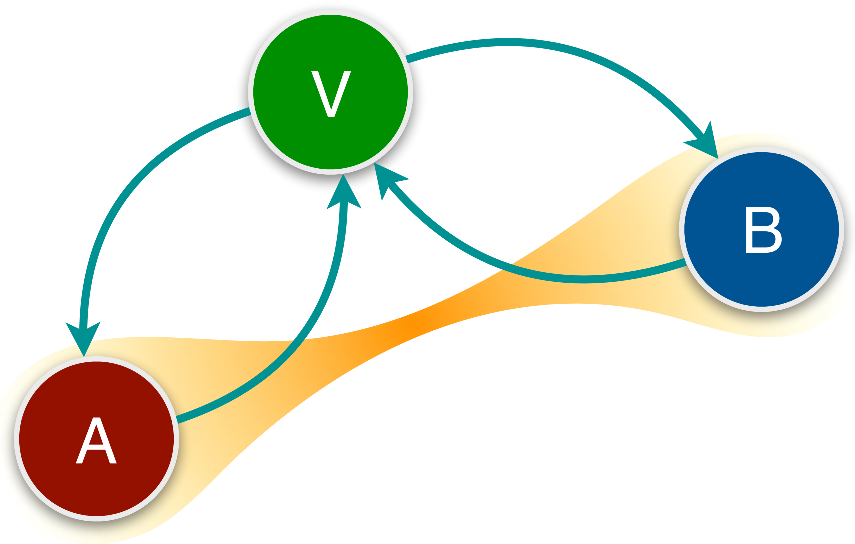
Where are the qubits?

- The classical verifier can only collect information about Pr[answers $a,b,c,\ldots$ | questions $s,t,u,\ldots$]
- Alice and Bob want to prove that they have jointly prepared a quantum state
- Example I: EPR
  - Use CHSH rigidity

[Reichardt, Unger, Vazirani 13]

- Example II: Werner states
  - Impossible!

[Werner 89]



Where are the qubits?

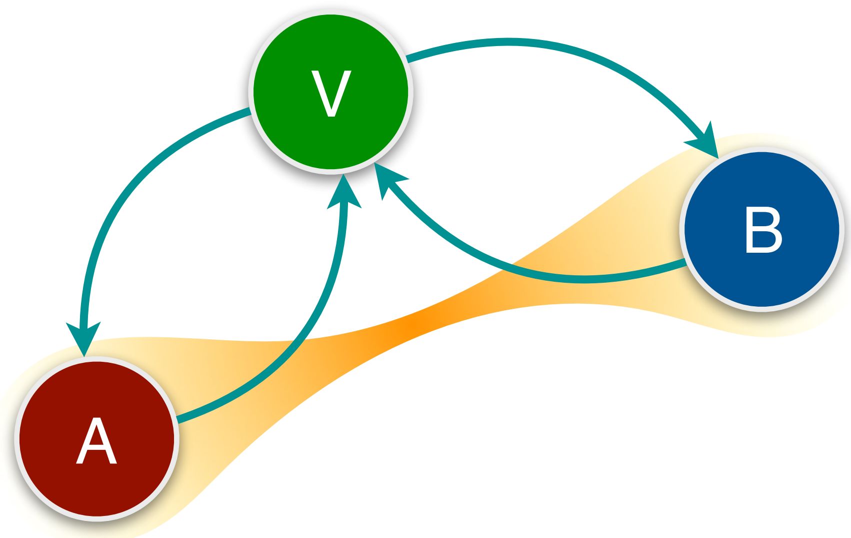
- The classical verifier can only collect information about Pr[answers $a,b,c,\ldots$ | questions $s,t,u,\ldots$]
- Alice and Bob want to prove that they have jointly prepared a quantum state
- Example I: EPR
  - Use CHSH rigidity

[Reichardt, Unger, Vazirani 13]

- Example II: Werner states
  - Impossible!

[Werner 89]

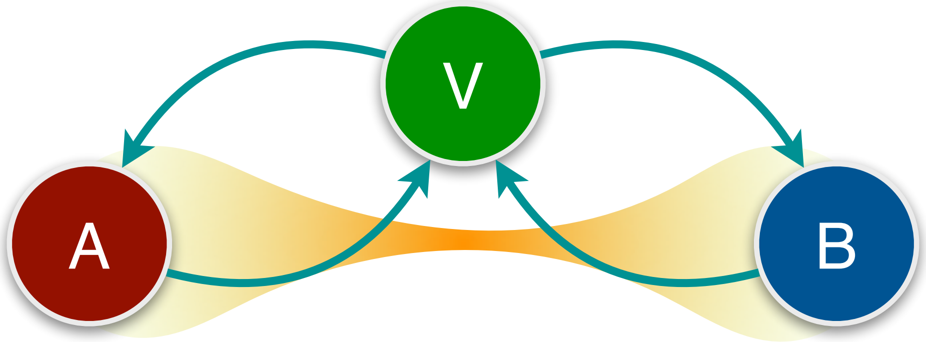
- Stabilizer games



CHSH game in terms of stabilizers

CHSH game in terms of stabilizers

CHSH: $a \oplus b \stackrel{?}{=} s \wedge t$

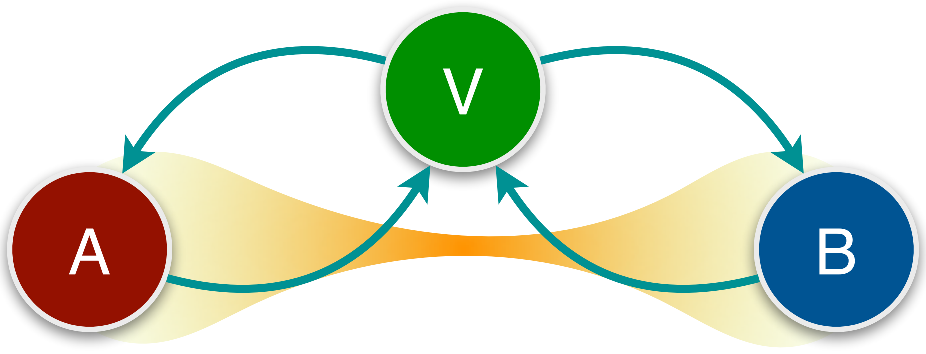


CHSH game in terms of stabilizers

- The EPR state as a stabilizer

X	X
Z	Z

CHSH: $a \oplus b \stackrel{?}{=} s \wedge t$



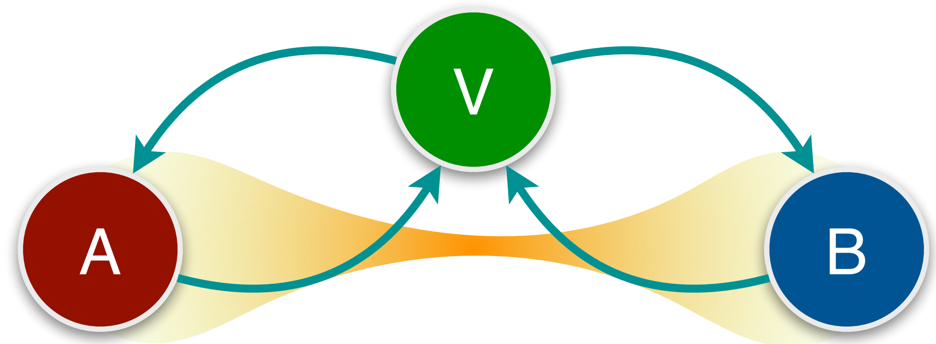
CHSH game in terms of stabilizers

- The EPR state as a stabilizer

X	X
Z	Z

$$\langle XX + ZZ \rangle = 2$$

CHSH: $a \oplus b \stackrel{?}{=} s \wedge t$



CHSH game in terms of stabilizers

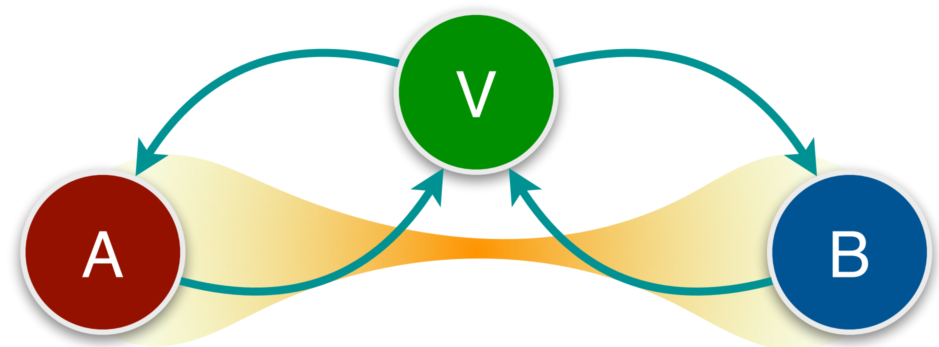
- The EPR state as a stabilizer

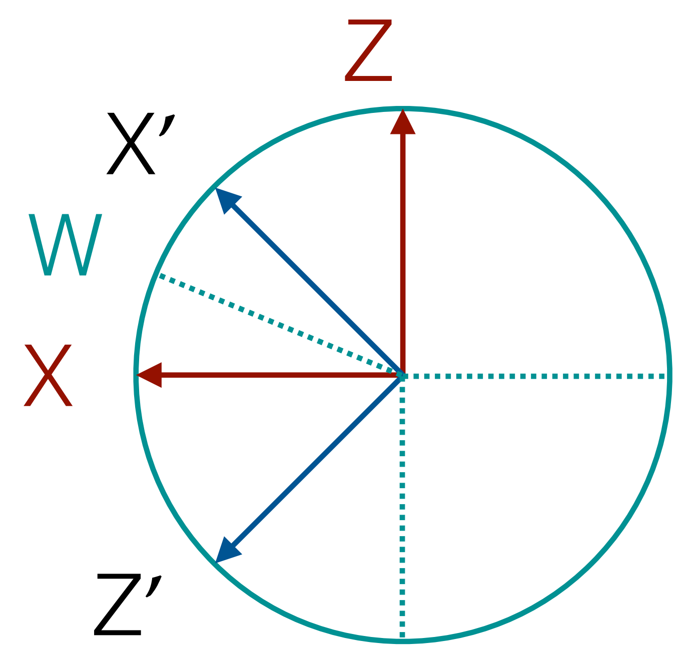
X	X
Z	Z

$$\langle XX + ZZ \rangle = 2$$

$$X = \frac{X' + Z'}{\sqrt{2}} \qquad Z = \frac{X' - Z'}{\sqrt{2}}$$

CHSH: $a \oplus b \stackrel{?}{=} s \wedge t$

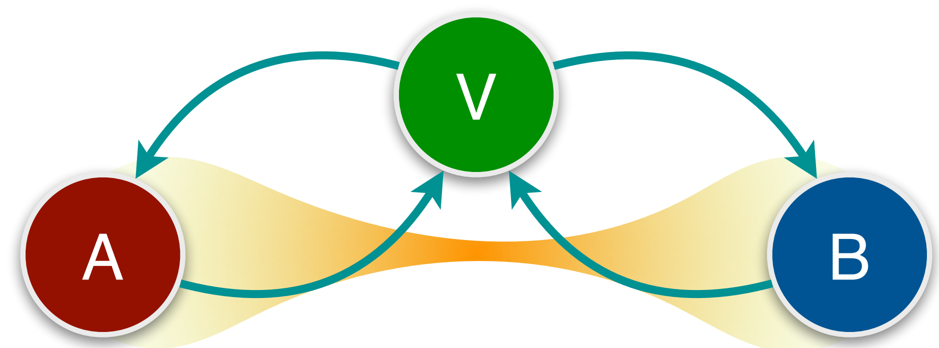




CHSH game in terms of stabilizers

- The EPR state as a stabilizer

CHSH: $a \oplus b \stackrel{?}{=} s \wedge t$



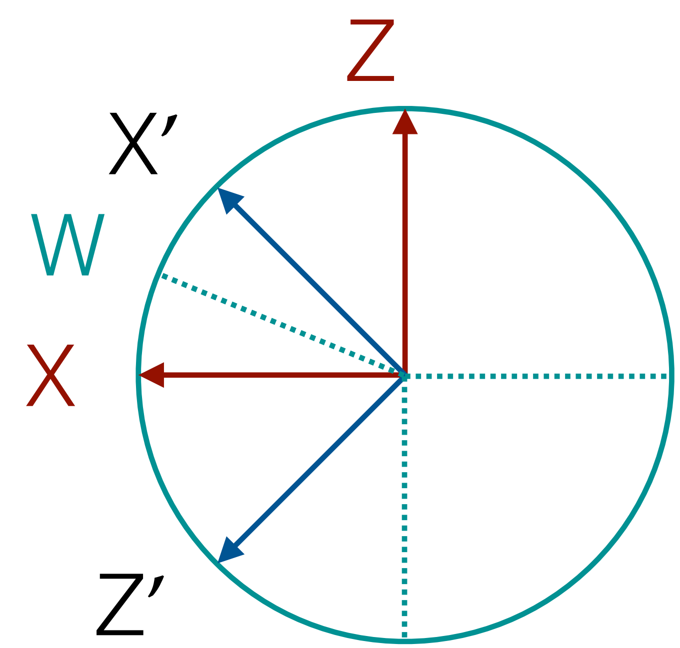
X	X
Z	Z

$$\langle XX + ZZ \rangle = 2$$

$$X = \frac{X' + Z'}{\sqrt{2}} \qquad Z = \frac{X' - Z'}{\sqrt{2}}$$

$$\langle XX' + XZ' + ZX' - ZZ' \rangle = 2\sqrt{2}$$

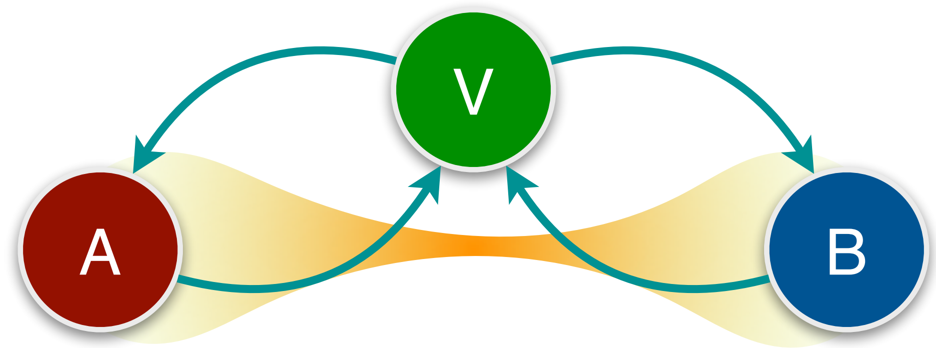
$$\langle X(X' + Z') + Z(X' - Z') \rangle \leq 2$$



CHSH game in terms of stabilizers

- The EPR state as a stabilizer

CHSH: $a \oplus b \stackrel{?}{=} s \wedge t$



X	X
Z	Z

$$\langle XX + ZZ \rangle = 2$$

$$X = \frac{X' + Z'}{\sqrt{2}} \qquad Z = \frac{X' - Z'}{\sqrt{2}}$$

$$\langle XX' + XZ' + ZX' - ZZ' \rangle = 2\sqrt{2}$$

$$\langle X(X' + Z') + Z(X' - Z') \rangle \leq 2$$

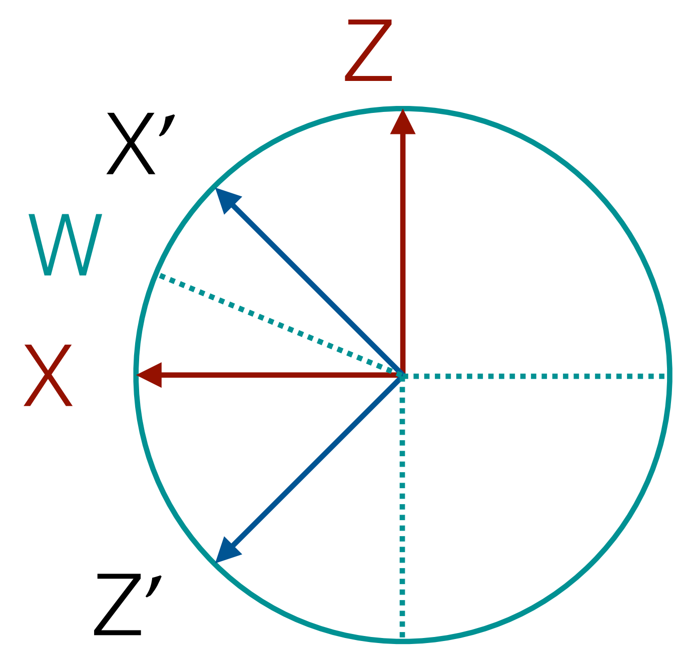
X	X
Z	Z

$\longrightarrow$

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

$\longrightarrow$

+	0	0
+	0	1
+	1	0
-	1	1



Stabilizer games with a special player

Stabilizer games with a special player

- Apply the 45-degree rotation trick to the stabilizers of the [4,2,2] code

X	X	X	X
Z	Z	Z	Z

$\longrightarrow$

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

Stabilizer games with a special player

- Apply the 45-degree rotation trick to the stabilizers of the [4,2,2] code

X	X	X	X
Z	Z	Z	Z

→

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

→

+	0	0	0	2
+	0	0	0	3
+	1	1	1	2
-	1	1	1	3

Stabilizer games with a special player

- Apply the 45-degree rotation trick to the stabilizers of the [4,2,2] code

X	X	X	X
Z	Z	Z	Z

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

+	0	0	0	2
+	0	0	0	3
+	1	1	1	2
-	1	1	1	3

Parity Questions

Stabilizer games with a special player

- Apply the 45-degree rotation trick to the stabilizers of the [4,2,2] code

X	X	X	X
Z	Z	Z	Z

→

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

→

+	0	0	0	2
+	0	0	0	3
+	1	1	1	2
-	1	1	1	3

Parity Questions

- Special player: the 4-th player

Stabilizer games with a special player

- Apply the 45-degree rotation trick to the stabilizers of the [4,2,2] code

X	X	X	X
Z	Z	Z	Z

→

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

→

+	0	0	0	2
+	0	0	0	3
+	1	1	1	2
-	1	1	1	3

Parity Questions

- Special player: the 4-th player

- No full rigidity, but partial rigidity: the special player must measure honestly

Partial rigidity of the special player stabilizer game

Lemma (Partial Rigidity). For any strategy $\mathcal{S} = (\rho, \{R_w^{(i)}\})$ of the special player stabilizer game whose value is at least $\omega_{\rm sps}^* - \varepsilon$ there exists an isometry $V : \mathcal{H}_4 \to \mathbb{C}^2 \otimes \hat{\mathcal{H}}_4$ such that

$$R_3^{(4)} = V^\dagger (Z' \otimes I) V,$$

$$R_2^{(4)} \approx_{\sqrt{\varepsilon}} V^\dagger (X' \otimes I) V.$$

Partial rigidity of the special player stabilizer game

Lemma (Partial Rigidity). For any strategy $\mathcal{S} = (\rho, \{R_w^{(i)}\})$ of the special player stabilizer game whose value is at least $\omega^*_{\rm sps} - \varepsilon$ there exists an isometry $V : \mathcal{H}_4 \to \mathbb{C}^2 \otimes \hat{\mathcal{H}}_4$ such that

$$R_3^{(4)} = V^\dagger (Z' \otimes I) V,$$
$$R_2^{(4)} \approx_{\sqrt{\varepsilon}} V^\dagger (X' \otimes I) V.$$

Proof of the lemma uses the Jordan's lemma and a proof technique for the CHSH rigidity from [Reichardt, Unger, Vazirani 13]

Stabilizer games

Stabilizer games

- The stabilizer game is a 4-player game with 2-bit questions and single-bit answers

Stabilizer games

- The stabilizer game is a 4-player game with 2-bit questions and single-bit answers
- With equal probability, the verifier performs

Stabilizer games

- The stabilizer game is a 4-player game with 2-bit questions and single-bit answers
- With equal probability, the verifier performs
  - Random special-player games

+	0	0	2	0
+	0	0	3	0
+	1	1	2	1
-	1	1	3	1

Stabilizer games

- The stabilizer game is a 4-player game with 2-bit questions and single-bit answers
- With equal probability, the verifier performs
  - Random special-player games
  - Direct checking of encoding

+	0	0	2	0
+	0	0	3	0
+	1	1	2	1
-	1	1	3	1

+	0	0	0	0
+	1	1	1	1

Stabilizer games

- The stabilizer game is a 4-player game with 2-bit questions and single-bit answers
- With equal probability, the verifier performs
  - Random special-player games
  - Direct checking of encoding
- Optimal strategy:
  - Share any state in the code space
  - Measure honestly

+	0	0	2	0
+	0	0	3	0
+	1	1	2	1
-	1	1	3	1

+	0	0	0	0
+	1	1	1	1

Stabilizer games

- The stabilizer game is a 4-player game with 2-bit questions and single-bit answers
- With equal probability, the verifier performs
  - Random special-player games
  - Direct checking of encoding
- Optimal strategy:
  - Share any state in the code space
  - Measure honestly
- Full rigidity! Device independence

+	0	0	2	0
+	0	0	3	0
+	1	1	2	1
-	1	1	3	1

+	0	0	0	0
+	1	1	1	1

Stabilizer games

- The stabilizer game is a 4-player game with 2-bit questions and single-bit answers
- With equal probability, the verifier performs
  - Random special-player games
  - Direct checking of encoding
- Optimal strategy:
  - Share any state in the code space
  - Measure honestly
- Full rigidity! Device independence
- Encoded Werner states are certifiable!

+	0	0	2	0
+	0	0	3	0
+	1	1	2	1
-	1	1	3	1

+	0	0	0	0
+	1	1	1	1

Rigidity of the stabilizer game

Lemma (Rigidity). For any strategy $\mathcal{S} = (\rho, \{R_w^{(i)}\})$ of the stabilizer game whose value is at least $\omega_{\mathrm{sg}}^* - \varepsilon$ there exist isometries $V_i : \mathcal{H}_i \to \mathbb{C}^2 \otimes \hat{\mathcal{H}}_i$ for all i such that

$$
\begin{aligned}
R_3^{(i)} &= V_i^\dagger (Z' \otimes I) V_i, \\
R_2^{(i)} &\approx_{\sqrt{\varepsilon}} V_i^\dagger (X' \otimes I) V_i, \\
R_1^{(i)} &\approx_{\sqrt[4]{\varepsilon}} V_i^\dagger (Z \otimes I) V_i, \\
R_0^{(i)} &\approx_{\sqrt[4]{\varepsilon}} V_i^\dagger (X \otimes I) V_i.
\end{aligned}
$$

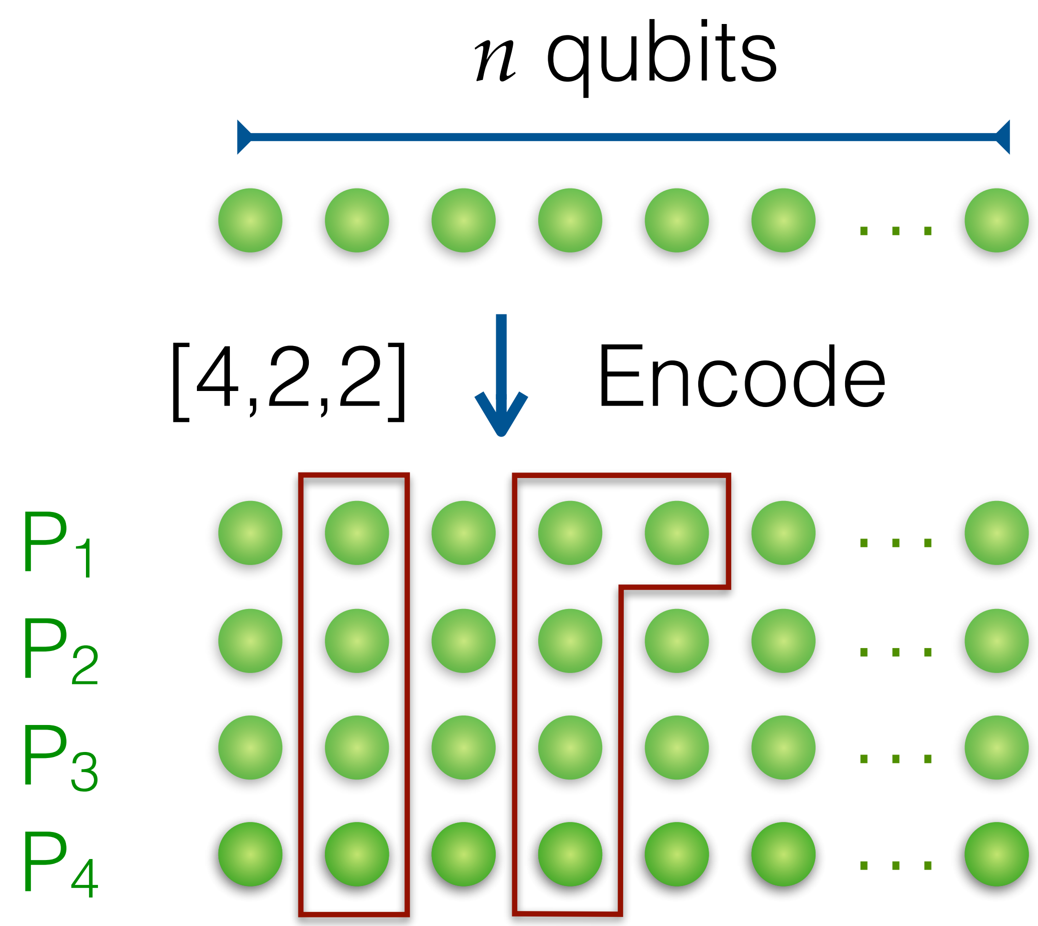
Rigidity of the stabilizer game

Lemma (Rigidity). For any strategy $\mathcal{S} = (\rho, \{R_w^{(i)}\})$ of the stabilizer game whose value is at least $\omega_{\mathrm{sg}}^* - \varepsilon$ there exist isometries $V_i : \mathcal{H}_i \to \mathbb{C}^2 \otimes \hat{\mathcal{H}}_i$ for all i such that

$$
\begin{aligned}
R_3^{(i)} &= V_i^\dagger (Z' \otimes I) V_i, \\
R_2^{(i)} &\approx_{\sqrt{\varepsilon}} V_i^\dagger (X' \otimes I) V_i, \\
R_1^{(i)} &\approx_{\sqrt[4]{\varepsilon}} V_i^\dagger (Z \otimes I) V_i, \\
R_0^{(i)} &\approx_{\sqrt[4]{\varepsilon}} V_i^\dagger (X \otimes I) V_i.
\end{aligned}
$$

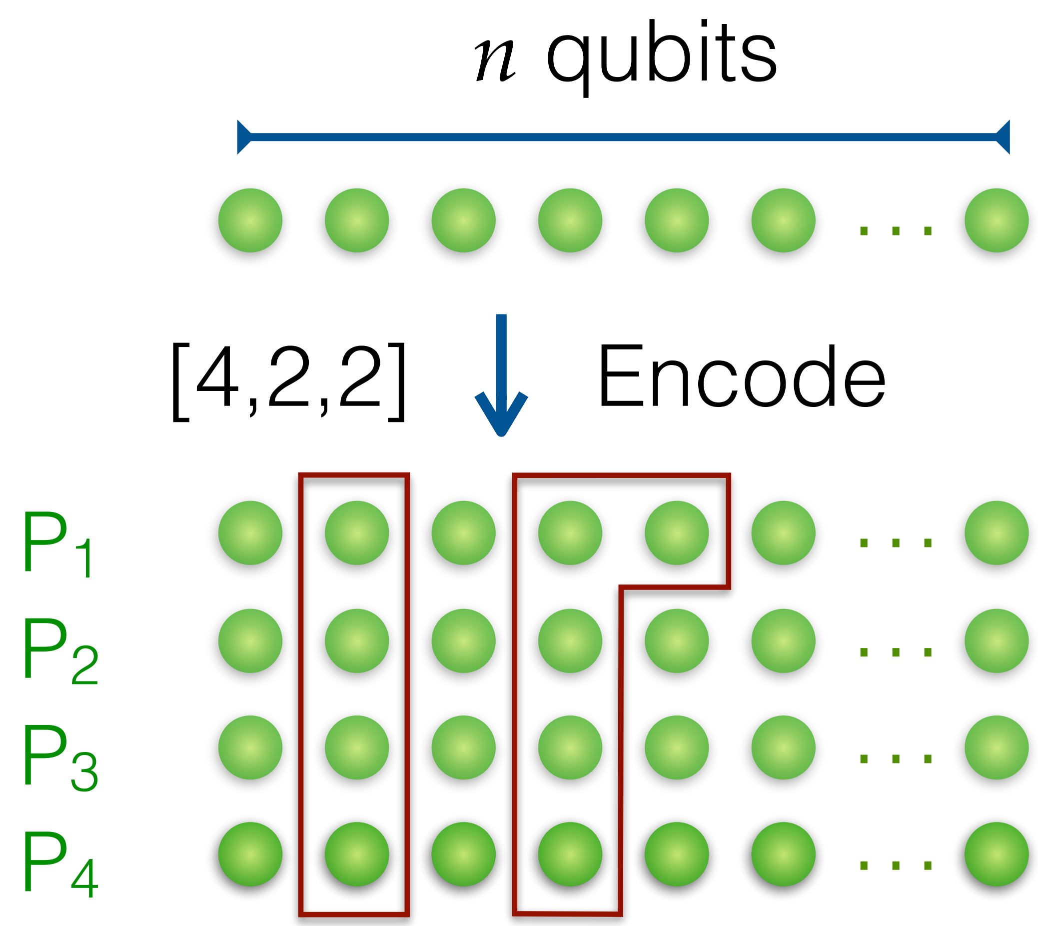
The proof uses the consistency properties of the game

Multi-qubit stabilizer game



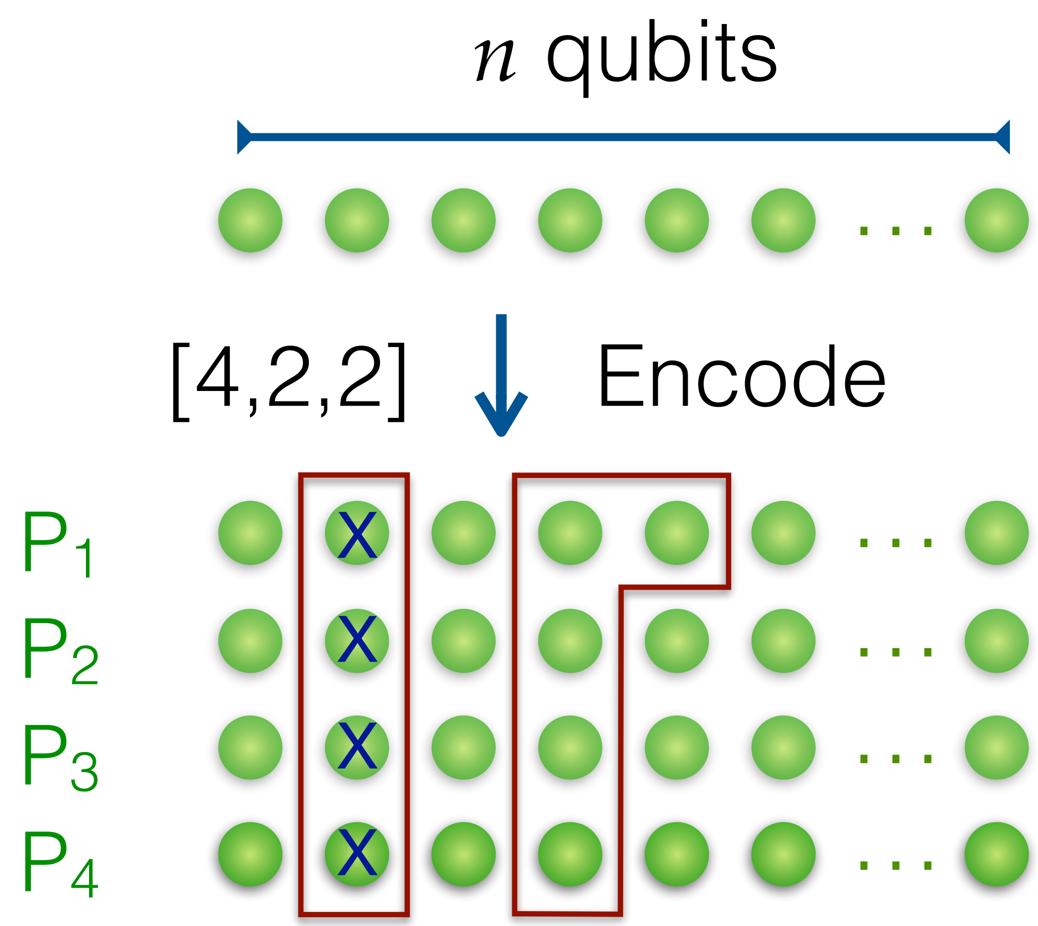
Multi-qubit stabilizer game

- For both types of the encoding checks, the verifier plays the corresponding stabilizer game



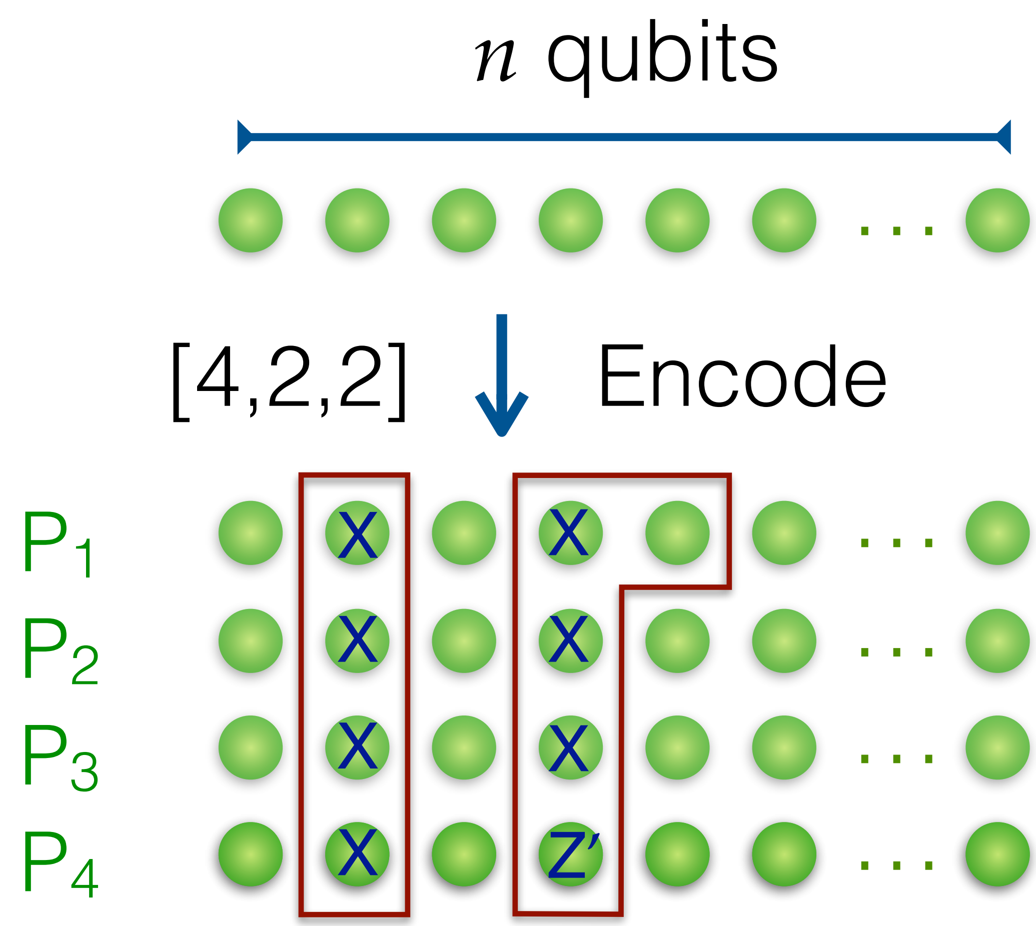
Multi-qubit stabilizer game

- For both types of the encoding checks, the verifier plays the corresponding stabilizer game



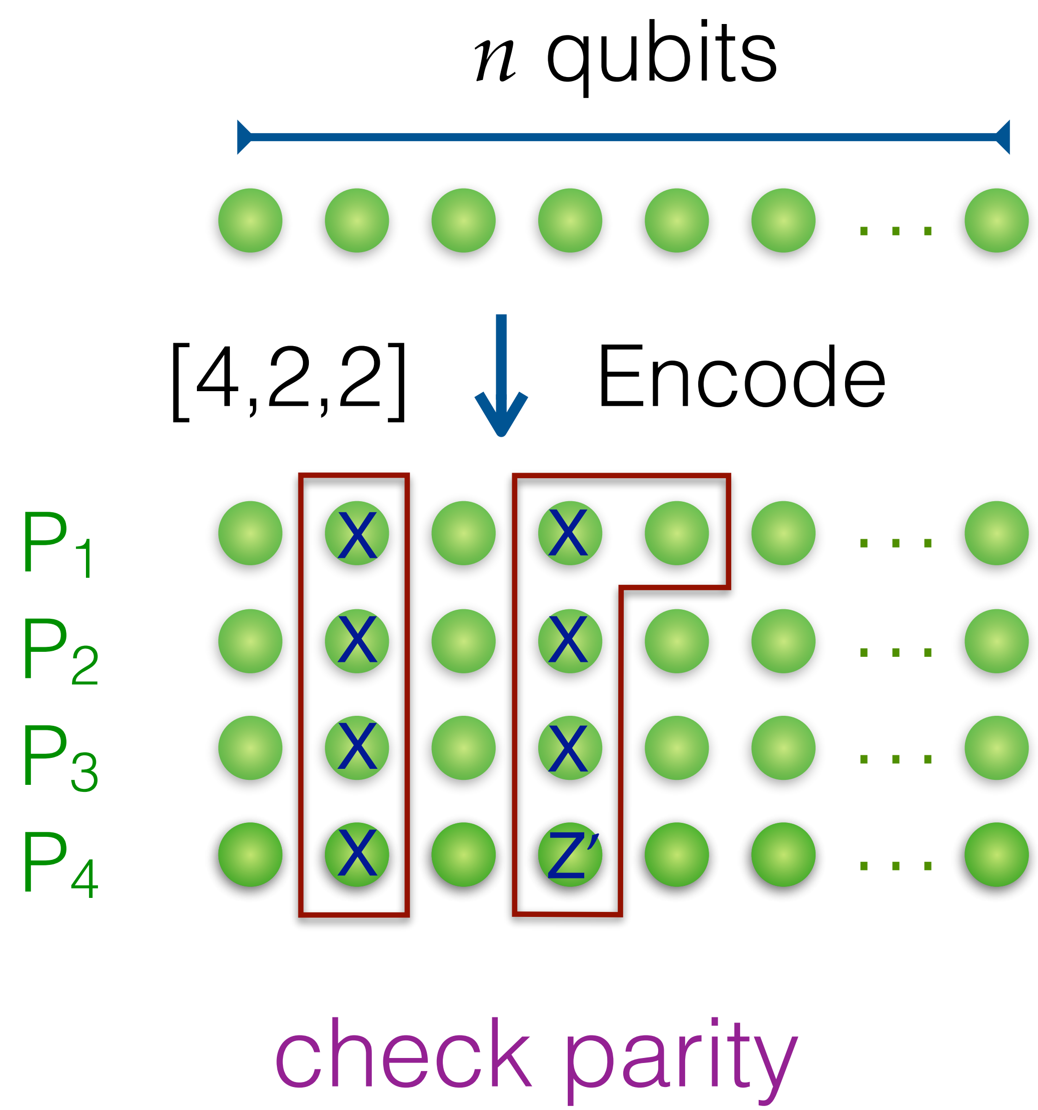
Multi-qubit stabilizer game

- For both types of the encoding checks, the verifier plays the corresponding stabilizer game



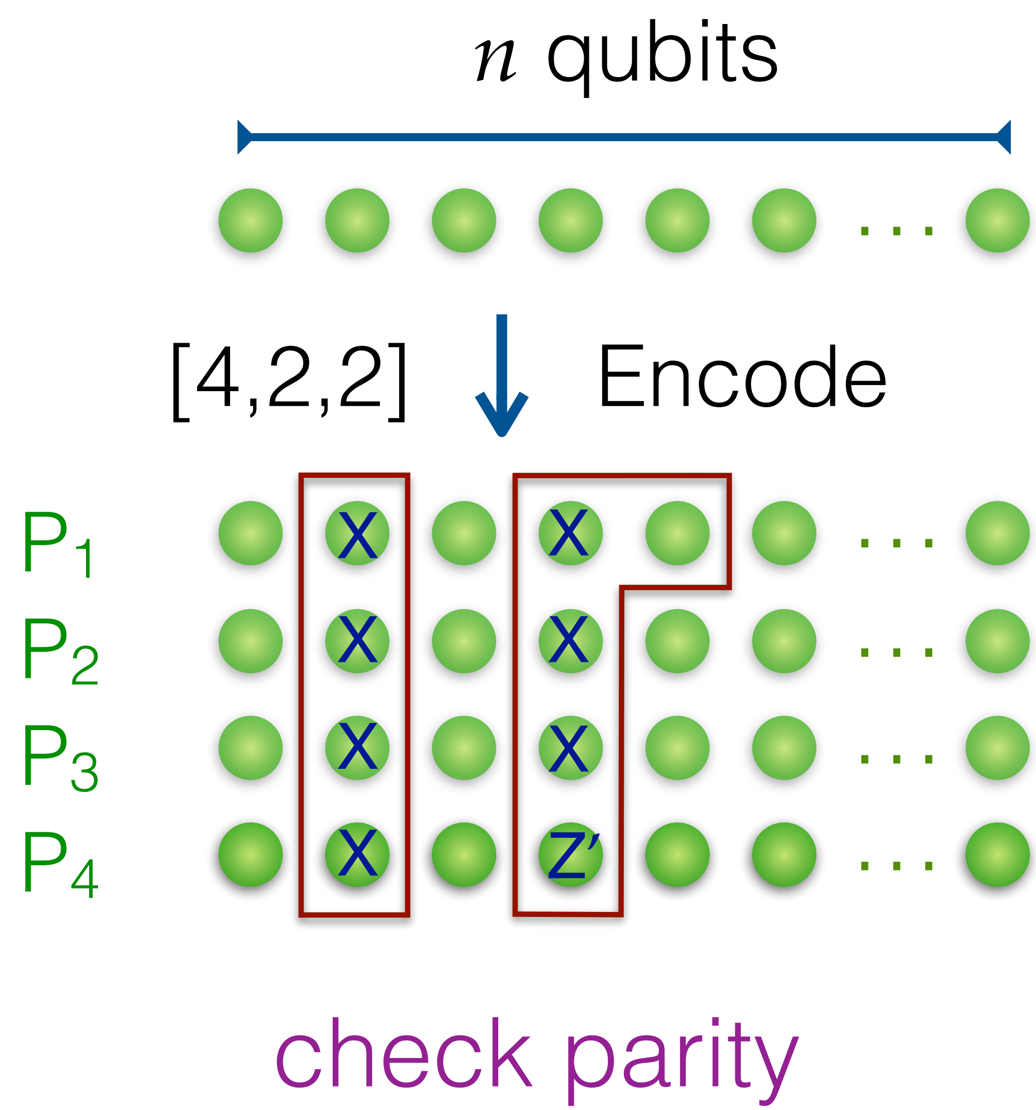
Multi-qubit stabilizer game

- For both types of the encoding checks, the verifier plays the corresponding stabilizer game



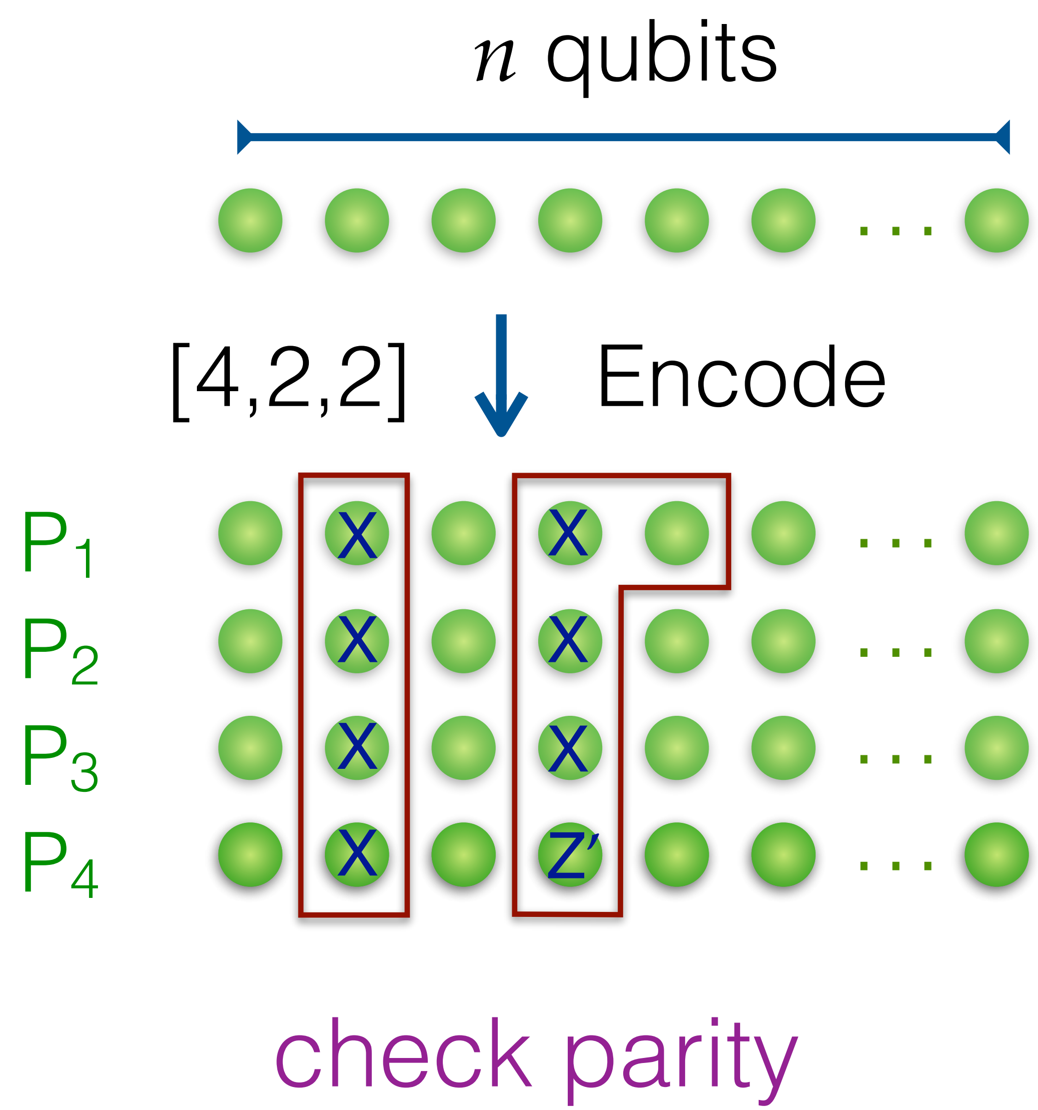
Multi-qubit stabilizer game

- For both types of the encoding checks, the verifier plays the corresponding stabilizer game
- Full rigidity

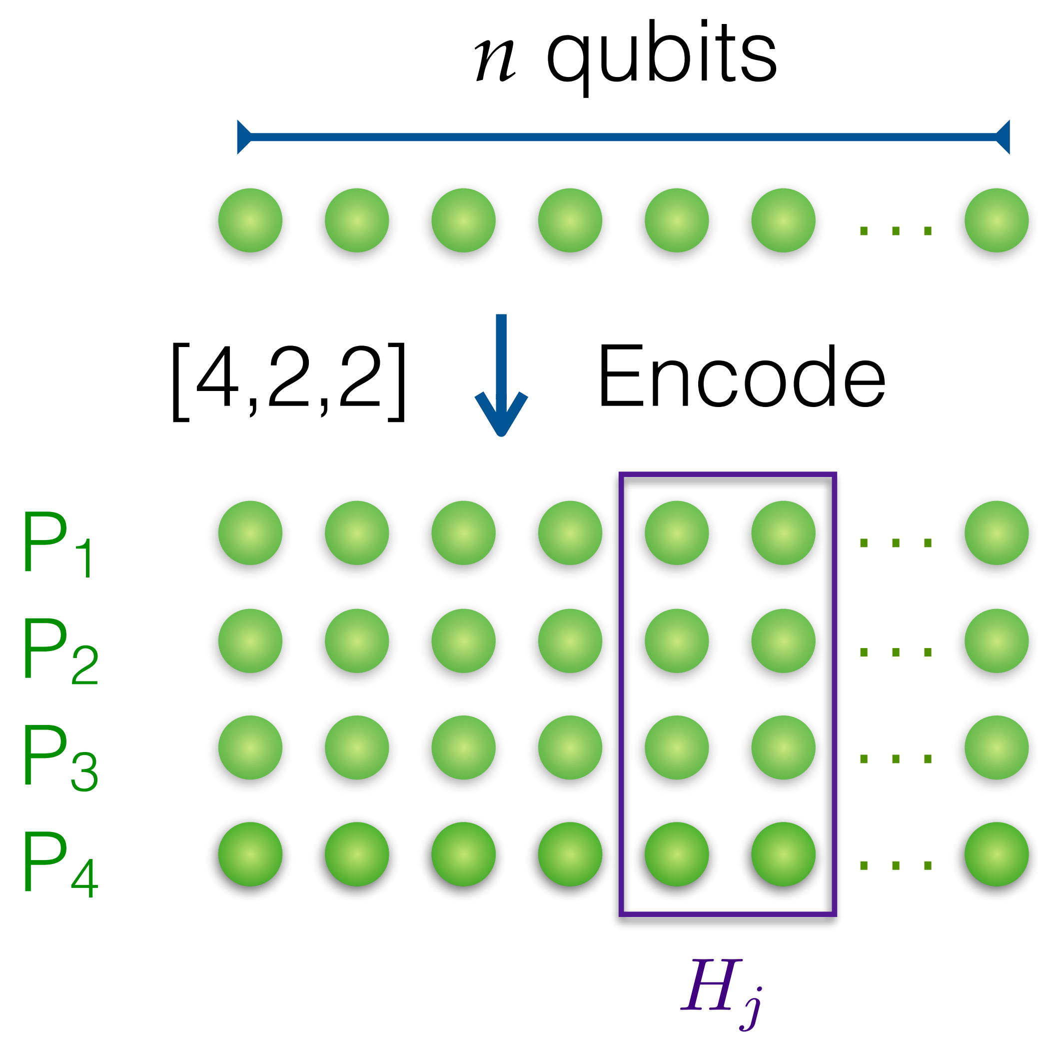


Multi-qubit stabilizer game

- For both types of the encoding checks, the verifier plays the corresponding stabilizer game
- Full rigidity
- “Locates” the n qubits in a sequential way



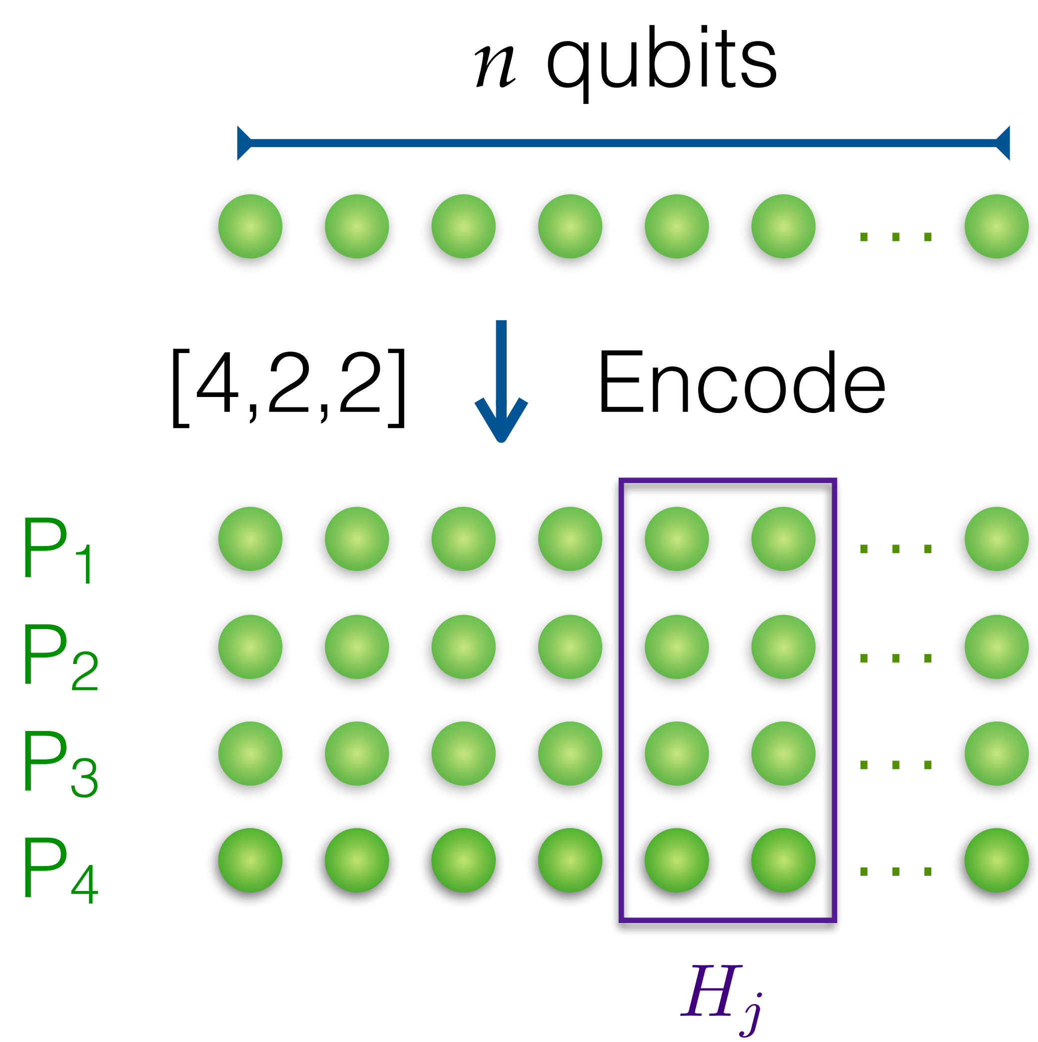
Energy measurement



Energy measurement

- Hamiltonians with XZ interactions remain **QMA**-complete

  [Cubitt, Montanaro 14]

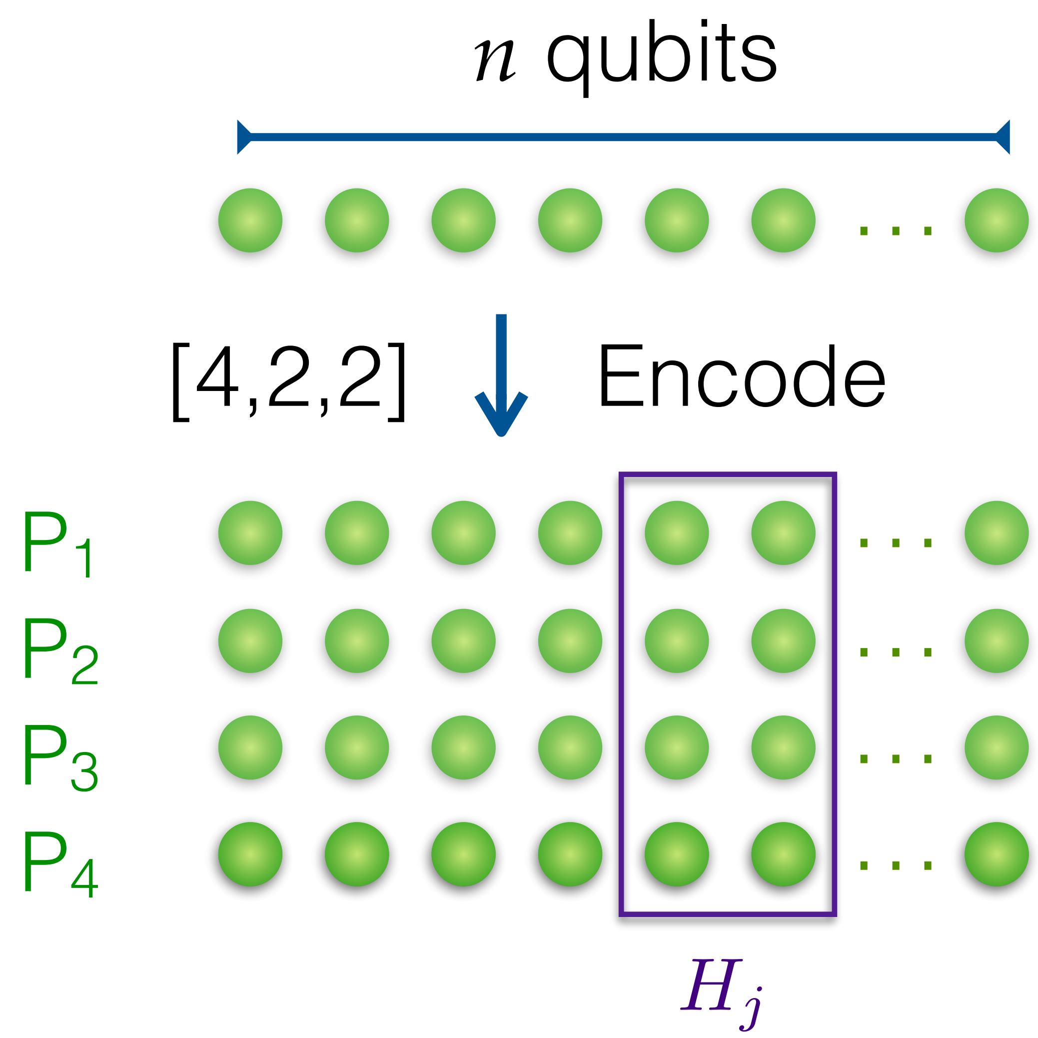


Energy measurement

- Hamiltonians with XZ interactions remain **QMA**-complete

  [Cubitt, Montanaro 14]

- Send measurement specifications of the logical X and logical Z operators



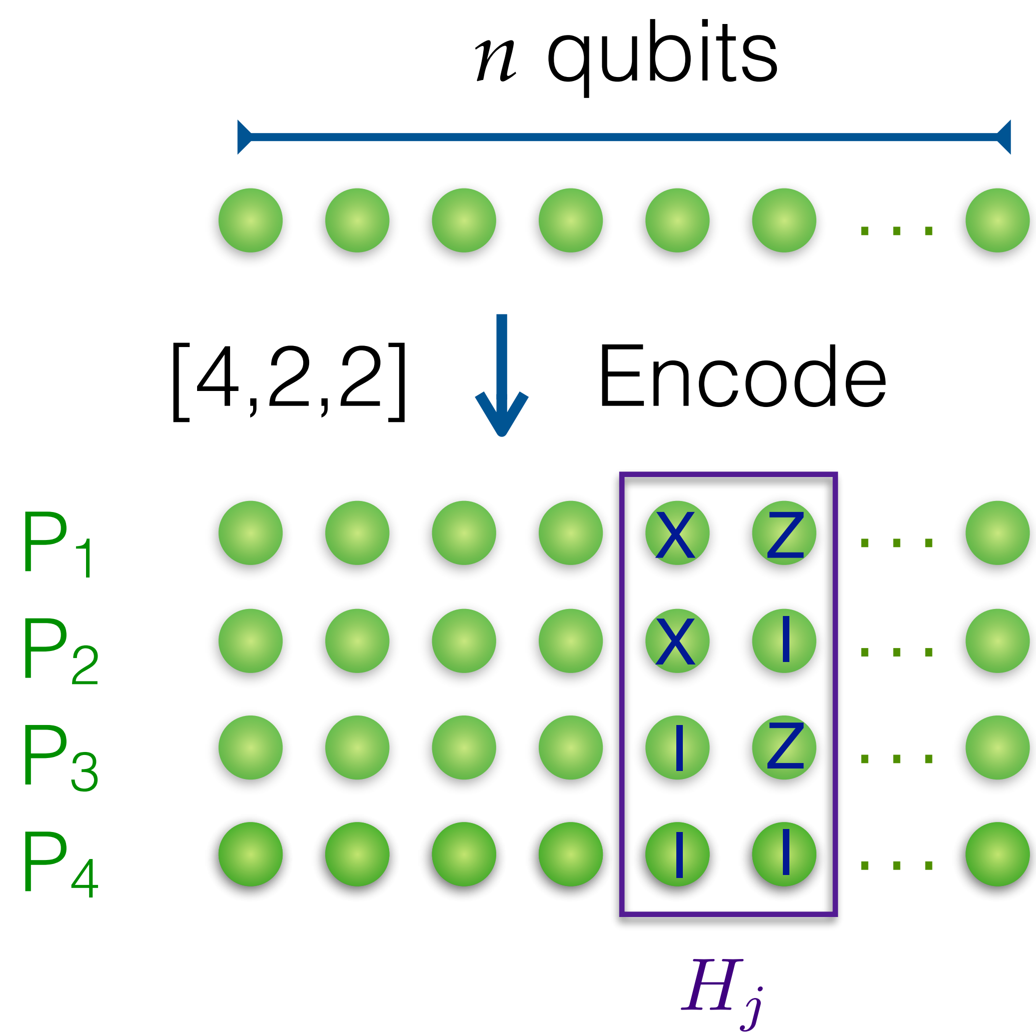
Energy measurement

- Hamiltonians with XZ interactions remain **QMA**-complete

  [Cubitt, Montanaro 14]

- Send measurement specifications of the logical X and logical Z operators

X	X	I	I
Z	I	Z	I



Conclusion and open problems

Conclusion and open problems

- Approximation of the entangled game value to inverse polynomial precision is **QMA**-hard

Conclusion and open problems

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

Conclusion and open problems

- 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?

Conclusion and open problems

- 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?

[Anand, Vidick 15]

Conclusion and open problems

- 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?

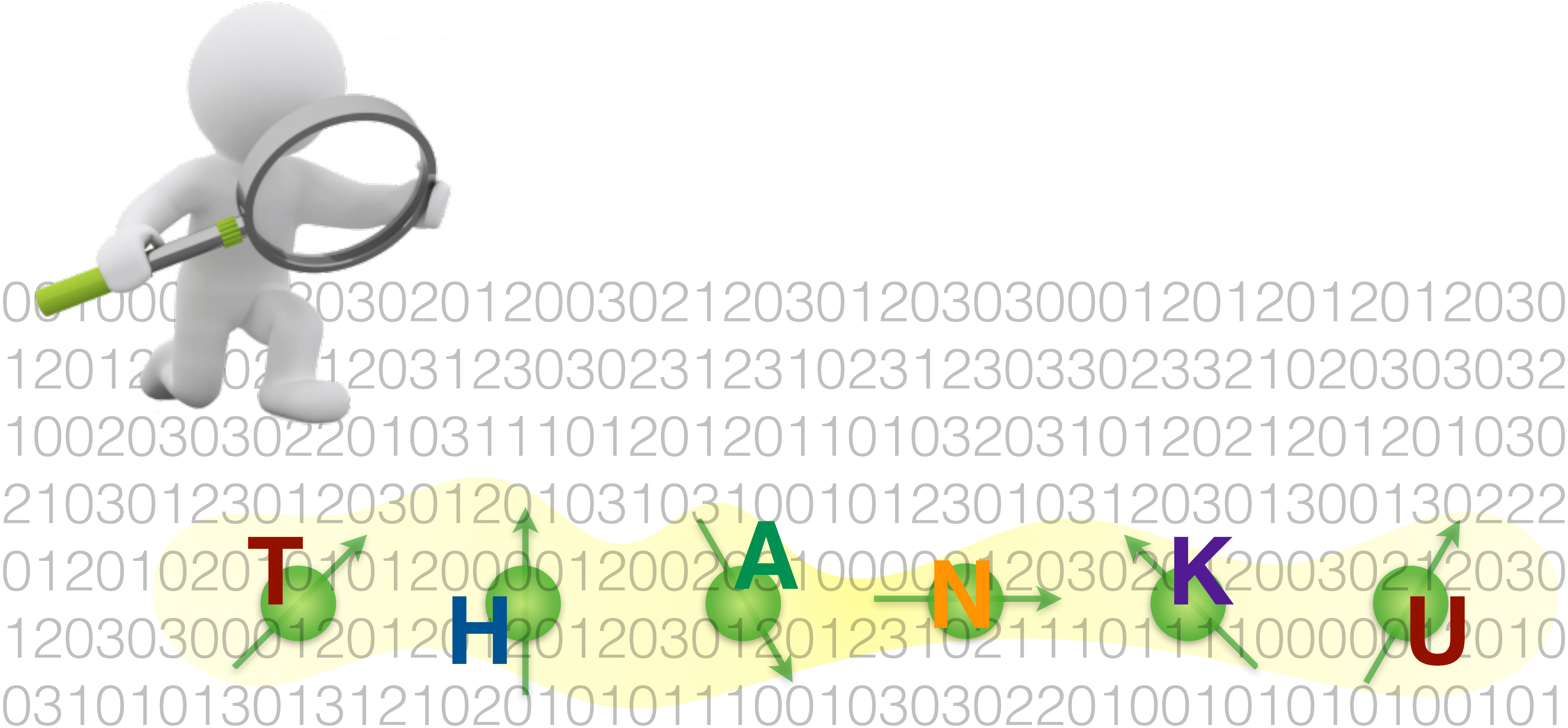
  [Anand, Vidick 15]
- Can we reduce the number of players down to 2?

Conclusion and open problems

- 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?

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

001000[illegible]2030201200302120301203030001201201201 2030
12012[illegible]02[illegible]1203123030231231023123033023321020303032
10020303022010311101201201101032031012021201201030
21030123012030120103103100101230103120301300130222
01201020101012000012002031000001203020120030212030
12030300012012012012030120123102111011110000012010
03101013013121020101011100103030220100101010100101


T H A N K U