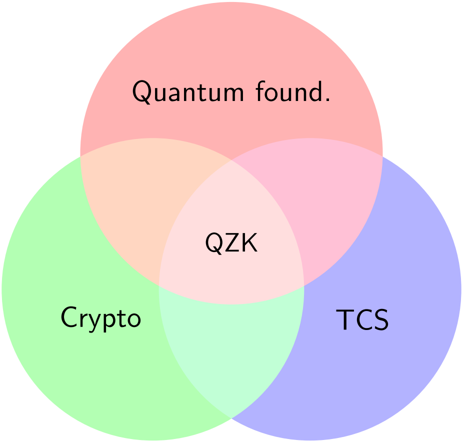
Quantum zero-knowledge from Locally Simulatable Proofs

Alex Bredariol Grilo

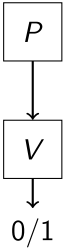
joint work with Anne Broadbent (U. of Ottawa)
arxiv:1911.07782


Quantum found.
QZK
Crypto
TCS

Interactive proofs

Interactive proofs

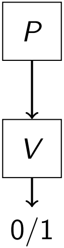
$L \in \mathrm{NP}$



for $x \in L$, $\exists P$
V accepts
for $x \notin L$, $\forall P$
V rejects

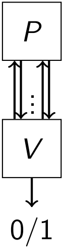
Interactive proofs

$L \in \mathrm{NP}$



for $x \in L$, $\exists P$
V accepts
for $x \notin L$, $\forall P$
V rejects

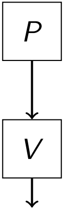
$L \in \mathrm{IP}$



for $x \in L$, $\exists P$
V accepts
for $x \notin L$, $\forall P$
V rejects whp

Interactive proofs

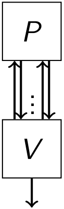
$L \in \mathrm{NP}$



$0/1$

for $x \in L$, $\exists P$
V accepts
for $x \notin L$, $\forall P$
V rejects

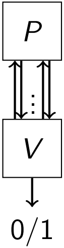
$L \in \mathrm{IP} = \mathrm{PSPACE}$



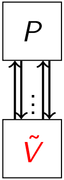
$0/1$

for $x \in L$, $\exists P$
V accepts
for $x \notin L$, $\forall P$
V rejects whp

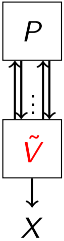
Zero-knowledge



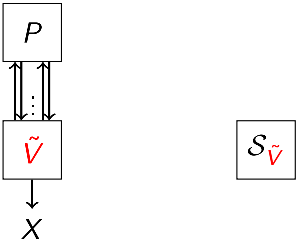
Zero-knowledge



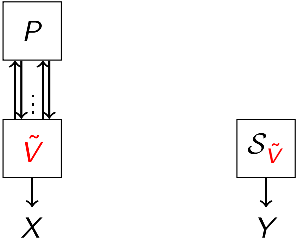
Zero-knowledge



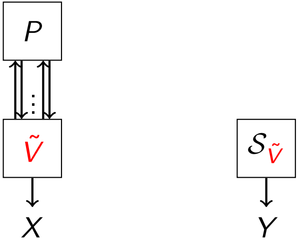
Zero-knowledge



Zero-knowledge



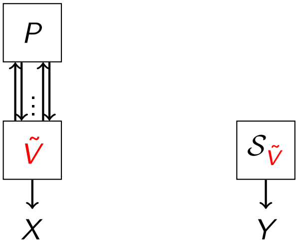
Zero-knowledge



Computational zero-knowledge

X and Y cannot be **efficiently** distinguished:

Zero-knowledge

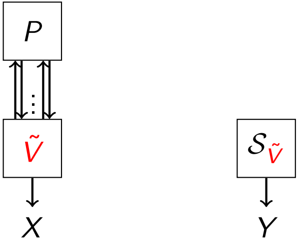


Computational zero-knowledge

X and Y cannot be **efficiently** distinguished:

$$\forall \text{ poly-time } \mathcal{A} : |Pr_{x \sim D_X}[\mathcal{A}(x) = 1] - Pr_{y \sim D_Y}[\mathcal{A}(y) = 1]| \leq negl(n)$$

Zero-knowledge



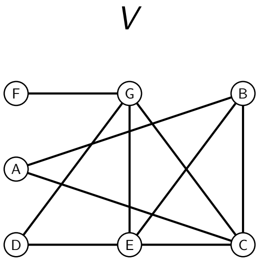
Computational zero-knowledge

X and Y cannot be **efficiently** distinguished:

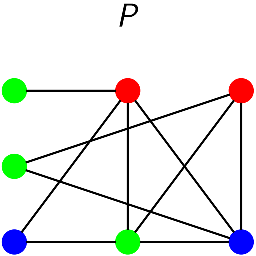
$$\forall \text{ poly-time } \mathcal{A} : |Pr_{x \sim D_X}[\mathcal{A}(x) = 1] - Pr_{y \sim D_Y}[\mathcal{A}(y) = 1]| \leq negl(n)$$

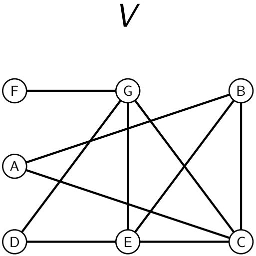
Fundamental notion in modern cryptography!

Example: ZK for 3-coloring

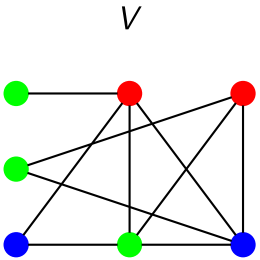


Example: ZK for 3-coloring



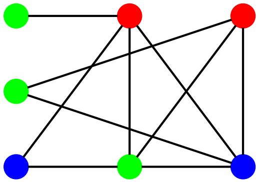


Example: ZK for 3-coloring



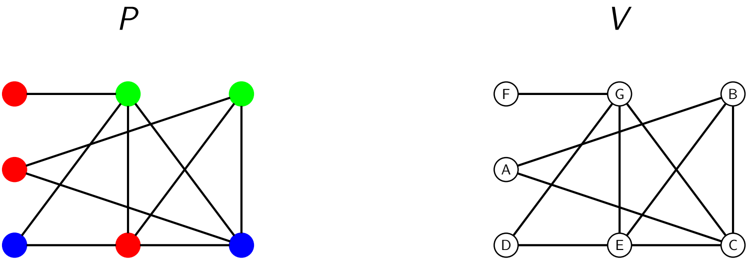
Example: ZK for 3-coloring

V

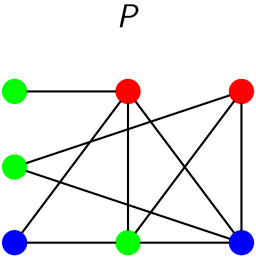


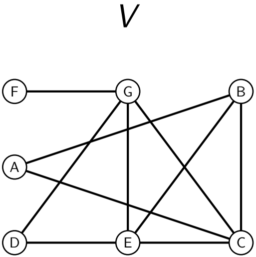
Completeness ✓ Soundness ✓ ZK ✗

Example: ZK for 3-coloring



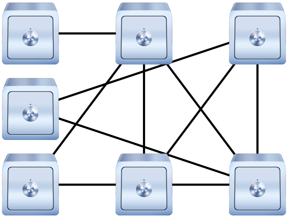
Example: ZK for 3-coloring



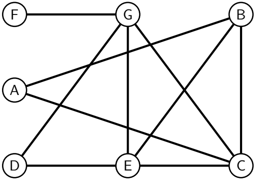


Example: ZK for 3-coloring

P



V

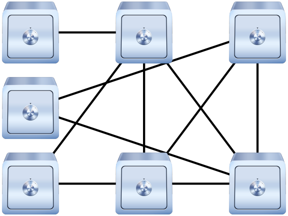


Example: ZK for 3-coloring

P

$A \rightarrow 564651$
$B \rightarrow 867132$
$C \rightarrow 984565$
$D \rightarrow 894102$
$E \rightarrow 069732$
$F \rightarrow 873210$
$G \rightarrow 897966$

V

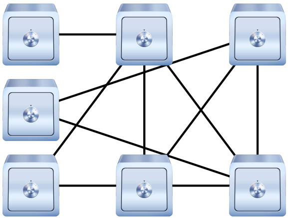


Example: ZK for 3-coloring

P

$A \to 564651$
$B \to 867132$
$C \to 984565$
$D \to 894102$
$E \to 069732$
$F \to 873210$
$G \to 897966$

V



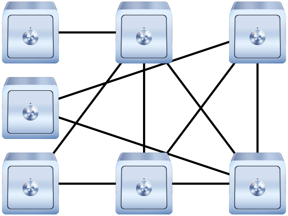
Example: ZK for 3-coloring

P

$A \to 564651$
$B \to 867132$
$C \to 984565$
$D \to 894102$
$E \to 069732$
$F \to 873210$
$G \to 897966$

$\xleftarrow{\{A, C\}}$

V



Example: ZK for 3-coloring

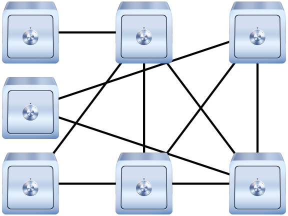
P

V

$A \to 564651$
$B \to 867132$
$C \to 984565$
$D \to 894102$
$E \to 069732$
$F \to 873210$
$G \to 897966$

$$\xleftarrow{\quad\{A, C\}\quad}$$

$$\xrightarrow[\quad 564651, 984565\quad]{}$$



Example: ZK for 3-coloring

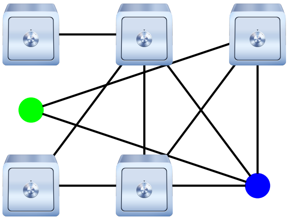
P

$A \to 564651$
$B \to 867132$
$C \to 984565$
$D \to 894102$
$E \to 069732$
$F \to 873210$
$G \to 897966$

$\xleftarrow{\{A, C\}}$

$\xrightarrow[564651,\ 984565]{}$

V



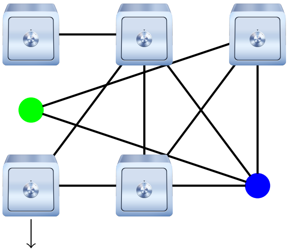
Example: ZK for 3-coloring

P $\qquad\qquad\qquad\qquad$ V

$A \to 564651$
$B \to 867132$
$C \to 984565$
$D \to 894102$
$E \to 069732$
$F \to 873210$
$G \to 897966$

$\xleftarrow{\{A, C\}}$

$\xrightarrow[564651,\, 984565]{}$



bit-commitment

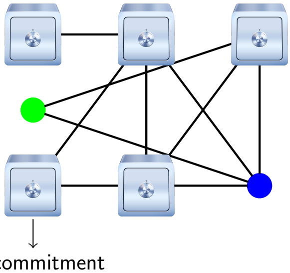
Example: ZK for 3-coloring

P $\qquad\qquad\qquad\qquad$ V

$A \to 564651$
$B \to 867132$
$C \to 984565$
$D \to 894102$
$E \to 069732$
$F \to 873210$
$G \to 897966$

$\xleftarrow{\{A, C\}}$

$\xrightarrow[564651,\ 984565]{}$

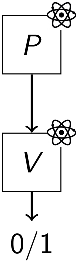


Completeness ✓ $\qquad$ Soundness ✓ $\qquad$ CZK ✓

Quantum proofs

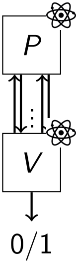
Quantum proofs

$L \in \mathrm{QMA}$



for $x \in L$, $\exists P$
V accepts whp
for $x \notin L$, $\forall P$
V rejects whp

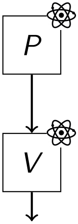
$L \in \mathrm{QIP}$



for $x \in L$, $\exists P$
V accepts
for $x \notin L$, $\forall P$
V rejects whp

Quantum proofs

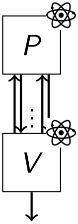
$L \in \mathrm{QMA}$



$0/1$

for $x \in L$, $\exists P$
V accepts whp
for $x \notin L$, $\forall P$
V rejects whp

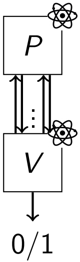
$L \in \mathrm{QIP} = \mathrm{PSPACE}$



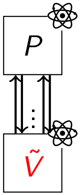
$0/1$

for $x \in L$, $\exists P$
V accepts
for $x \notin L$, $\forall P$
V rejects whp

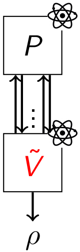
Quantum Zero-knowledge



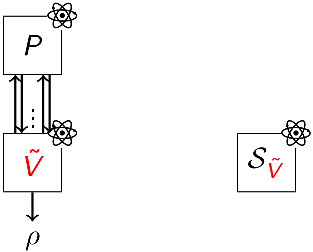
Quantum Zero-knowledge



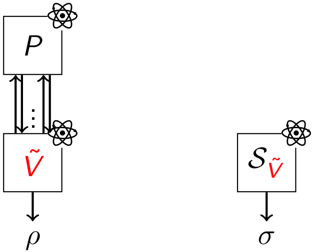
Quantum Zero-knowledge



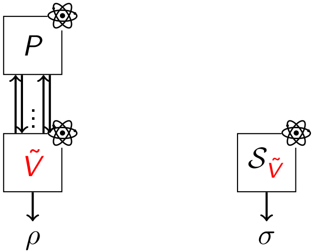
Quantum Zero-knowledge



Quantum Zero-knowledge



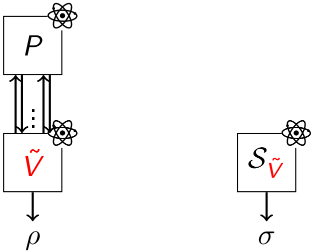
Quantum Zero-knowledge



Quantum computational zero-knowledge

ρ and σ cannot be **efficiently** distinguished:

Quantum Zero-knowledge



Quantum computational zero-knowledge

ρ and σ cannot be **efficiently** distinguished:

$\forall$ quantum poly-time $\mathcal{A}$: $|Pr[\mathcal{A}(\rho) = 1] - Pr[\mathcal{A}(\sigma) = 1]| \leq negl(n)$

Zero-knowledge for quantum proofs

Zero-knowledge for quantum proofs

- Assuming qOWF: QMA $\subseteq$ QZK since PSPACE $=$ CZK $\subseteq$ QZK

    Need to go through QMA $\subseteq$ PP

    Desired: Efficient prover with QMA witness

Zero-knowledge for quantum proofs

- Assuming qOWF: QMA $\subseteq$ QZK since PSPACE $=$ CZK $\subseteq$ QZK

  Need to go through QMA $\subseteq$ PP

  Desired: Efficient prover with QMA witness
- BJSW'16: QMA $\subseteq$ QZK with efficient prover

  Multiple rounds of communication

  Somewhat complicated

Zero-knowledge for quantum proofs

- Assuming qOWF: QMA $\subseteq$ QZK since PSPACE $=$ CZK $\subseteq$ QZK

  Need to go through QMA $\subseteq$ PP

  Desired: Efficient prover with QMA witness
- BJSW'16: QMA $\subseteq$ QZK with efficient prover

  Multiple rounds of communication

  Somewhat complicated
- B**G**19: explore Locally Simulatable codes from **G**SY19

Zero-knowledge for quantum proofs

- Assuming qOWF: QMA $\subseteq$ QZK since PSPACE $=$ CZK $\subseteq$ QZK
  Need to go through QMA $\subseteq$ PP
  Desired: Efficient prover with QMA witness
- BJSW'16: QMA $\subseteq$ QZK with efficient prover
  Multiple rounds of communication
  Somewhat complicated
- B**G**19: explore Locally Simulatable codes from **G**SY19
  Applications in Cryptography
  - ⋆ "commit-and-open" Proof of Knowledge QZK proof for QMA
  - ⋆ "commit-and-open" Proof of Knowledge QSZK argument for QMA
  - ⋆ QNISZK for QMA in the secret parameters setup

Zero-knowledge for quantum proofs

- Assuming qOWF: QMA $\subseteq$ QZK since PSPACE $=$ CZK $\subseteq$ QZK
  Need to go through QMA $\subseteq$ PP
  Desired: Efficient prover with QMA witness
- BJSW'16: QMA $\subseteq$ QZK with efficient prover
  Multiple rounds of communication
  Somewhat complicated
- B**G**19: explore Locally Simulatable codes from **G**SY19
  Applications in Cryptography
  - "commit-and-open" Proof of Knowledge QZK proof for QMA
  - "commit-and-open" Proof of Knowledge QSZK argument for QMA
  - QNISZK for QMA in the secret parameters setup

  Applications in Complexity theory
  - QMA-hardness of Consistency of local density matrices problem under Karp reductions (open for 15 years!)
  - Locally Simulatable proofs

Zero-knowledge for quantum proofs

- Assuming qOWF: QMA $\subseteq$ QZK since PSPACE $=$ CZK $\subseteq$ QZK
  - Need to go through QMA $\subseteq$ PP
  - Desired: Efficient prover with QMA witness
- BJSW'16: QMA $\subseteq$ QZK with efficient prover
  - Multiple rounds of communication
  - Somewhat complicated
- B**G**19: explore Locally Simulatable codes from **G**SY19
  - Applications in Cryptography
    - ⋆ "commit-and-open" Proof of Knowledge QZK proof for QMA
    - ⋆ "commit-and-open" Proof of Knowledge QSZK argument for QMA
    - ⋆ QNISZK for QMA in the secret parameters setup
  - Applications in Complexity theory
    - ⋆ QMA-hardness of Consistency of local density matrices problem under Karp reductions (open for 15 years!)
    - ⋆ Locally Simulatable proofs

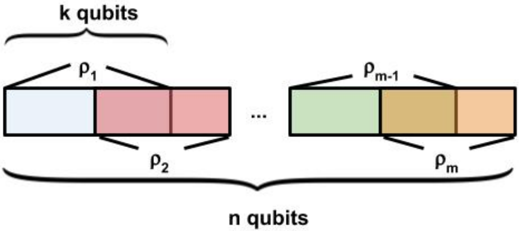
Consistency of local density matrices problem

Consistency of local density matrices problem

Input: Reduced density matrices $\rho_1, ..., \rho_m$ on k-qubits

Output: yes: $\exists \psi$ such that $\forall i$: $\left\| Tr_{\overline{S_i}}(\psi) - \rho_i \right\| \leq \varepsilon$

no: $\forall \psi$, $\exists i$: $\left\| Tr_{\overline{S_i}}(\psi) - \rho_i \right\| \geq \frac{1}{poly(n)}$

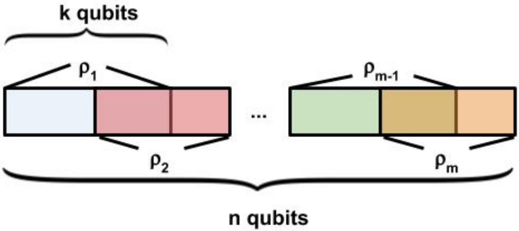


Consistency of local density matrices problem

Input: Reduced density matrices $\rho_1, ..., \rho_m$ on k-qubits

Output: yes: $\exists\psi$ such that $\forall i$: $\left\| Tr_{\overline{S_i}}(\psi) - \rho_i \right\| \leq \varepsilon$

no: $\forall\psi$, $\exists i$: $\left\| Tr_{\overline{S_i}}(\psi) - \rho_i \right\| \geq \frac{1}{poly(n)}$



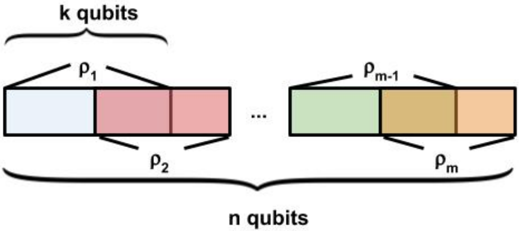
- Liu'06: containment in QMA, and partial result on QMA-hardness

Consistency of local density matrices problem

Input: Reduced density matrices $\rho_1, ..., \rho_m$ on k-qubits

Output: yes: $\exists \psi$ such that $\forall i : \left\| Tr_{\overline{S_i}}(\psi) - \rho_i \right\| \leq \varepsilon$

no: $\forall \psi$, $\exists i : \left\| Tr_{\overline{S_i}}(\psi) - \rho_i \right\| \geq \frac{1}{poly(n)}$



- Liu'06: containment in QMA, and partial result on QMA-hardness
- B**G**'19: QMA-hardness

Very simple ZK proof for QMA

P V

$\rho_1, \ldots, \rho_m$

Very simple ZK proof for QMA

P $\qquad\qquad$ V

$\psi^{\otimes \ell}$ $\qquad\qquad$ $\rho_1, \ldots, \rho_m$

Very simple ZK proof for QMA

P

V

$X^a Z^b \psi^{\otimes \ell} Z^b X^a$

$\rho_1, \ldots, \rho_m$

a_1, b_1

a_2, b_2

$\ldots$

a_{n-1}, b_{n-1}

a_n, b_n

Very simple ZK proof for QMA

P V

$X^a Z^b \psi^{\otimes \ell} Z^b X^a$ $\rho_1, \ldots, \rho_m$

Very simple ZK proof for QMA

P

$a_1, b_1 \rightarrow 564651$
$a_2, b_2 \rightarrow 984565$
$\dots$
$a_n, b_n \rightarrow 894102$

V

$\rho_1, \dots, \rho_m$

$X^a Z^b \psi^{\otimes \ell} X^a Z^b$

...

Very simple ZK proof for QMA

P

$a_1, b_1 \to 564651$

$a_2, b_2 \to 984565$

$\ldots$

$a_n, b_n \to 894102$

$\xleftarrow{\quad i \quad}$

V

$\rho_1, \ldots, \rho_m$

$X^a Z^b \psi^{\otimes \ell} X^a Z^b$

Very simple ZK proof for QMA

P $\qquad\qquad$ V

$a_1, b_1 \to 564651$
$a_2, b_2 \to 984565$
$\dots$
$a_n, b_n \to 894102$

$\rho_1, \dots, \rho_m$

$X^a Z^b \psi^{\otimes \ell} X^a Z^b$

$\xleftarrow{\quad i \quad}$

$\xrightarrow{\qquad\qquad}$
984565, 894102
keys to open otp of copies of ρ_i

...

Very simple ZK proof for QMA

P		V
$a_1, b_1 \to 564651$	
$a_2, b_2 \to 984565$		$\rho_1, \ldots, \rho_m$
$\ldots$	$\xleftarrow{i}$	$X^a Z^b \psi^{\otimes \ell} X^a Z^b$
$a_n, b_n \to 894102$	

$\xrightarrow{\quad\quad\quad}$

984565, 894102

keys to open otp of copies of ρ_i

a_2, b_2

...

a_n, b_n

Very simple ZK proof for QMA

P

$a_1, b_1 \to 564651$

$a_2, b_2 \to 984565$

$\dots$

$a_n, b_n \to 894102$

$$\xleftarrow{\quad i \quad}$$

$$\xrightarrow[\text{keys to open otp of copies of } \rho_i]{984565, 894102}$$

V

$\rho_1, \dots, \rho_m$

$X^a Z^b \psi^{\otimes \ell} X^a Z^b$

a_2, b_2

...

a_n, b_n

Completeness ✓ Soundness ✓ ZK ✓

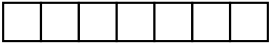
Simulatable codes - Steane code

$$
\begin{aligned}
|0\rangle \mapsto \frac{1}{2\sqrt{2}}(\,&|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\
&+ |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle) \\
|1\rangle \mapsto \frac{1}{2\sqrt{2}}(\,&|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle \\
&+ |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle)
\end{aligned}
$$

Simulatable codes - Steane code

$$
\begin{aligned}
|0\rangle \mapsto \frac{1}{2\sqrt{2}}(\,&|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\
&+ |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle) \\
|1\rangle \mapsto \frac{1}{2\sqrt{2}}(\,&|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle \\
&+ |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle)
\end{aligned}
$$

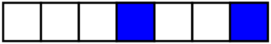
$Enc(|\psi\rangle)$



Simulatable codes - Steane code

$$
\begin{aligned}
|0\rangle \mapsto \frac{1}{2\sqrt{2}}\big(\, &|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\
&+ |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle\big) \\
|1\rangle \mapsto \frac{1}{2\sqrt{2}}\big(\, &|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle \\
&+ |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle\big)
\end{aligned}
$$

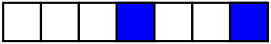
$\mathit{Enc}(|\psi\rangle)$



Simulatable codes - Steane code

$$|0\rangle \mapsto \frac{1}{2\sqrt{2}}\big(\,|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle$$
$$+ |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle\big)$$
$$|1\rangle \mapsto \frac{1}{2\sqrt{2}}\big(\,|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle$$
$$+ |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle\big)$$

$Enc(|\psi\rangle)$



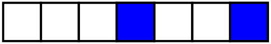
- For every $|\psi\rangle$ and $i, j \in [7]$, $Tr_{\overline{\{i,j\}}}(Enc(|\psi\rangle)) = \frac{I}{4}$

Simulatable codes - Steane code

$$|0\rangle \mapsto \frac{1}{2\sqrt{2}}\big(|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle\big)$$

$$|1\rangle \mapsto \frac{1}{2\sqrt{2}}\big(|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle + |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle\big)$$

$Enc(|\psi\rangle)$



- For every $|\psi\rangle$ and $i, j \in [7]$, $Tr_{\overline{\{i,j\}}}(Enc(|\psi\rangle)) = \frac{I}{4}$

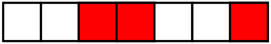
  The reduced density matrix on 2 qubits can be *efficiently computed* (independently of the logical state)

Simulatable codes - Steane code

$$|0\rangle \mapsto \frac{1}{2\sqrt{2}}\big(|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle \big)$$

$$|1\rangle \mapsto \frac{1}{2\sqrt{2}}\big(|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle + |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle \big)$$

$Enc(|\psi\rangle)$



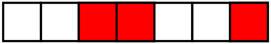
- For every $|\psi\rangle$ and $i, j \in [7]$, $Tr_{\overline{\{i,j\}}}(Enc(|\psi\rangle)) = \frac{I}{4}$

  The reduced density matrix on 2 qubits can be *efficiently computed* (independently of the logical state)

Simulatable codes - Steane code

$$|0\rangle \mapsto \frac{1}{2\sqrt{2}}(\,|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle$$
$$+ |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle)$$
$$|1\rangle \mapsto \frac{1}{2\sqrt{2}}(\,|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle$$
$$+ |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle)$$

$Enc(|\psi\rangle)$



- For every $|\psi\rangle$ and $i, j \in [7]$, $Tr_{\overline{\{i,j\}}}(Enc(|\psi\rangle)) = \frac{I}{4}$

  The reduced density matrix on 2 qubits can be *efficiently computed* (independently of the logical state)
- Not true anymore for $i, j, k \in [7]$

Simulatable codes - concatenated Steane code

Simulatable codes - concatenated Steane code

Lemma (s-locally simulatable codes)

Simulatable codes - concatenated Steane code

Lemma (s-locally simulatable codes)

Fix s and let $k = \log_3(s)$. We have the following properties of k-fold concatenation of the Steane code $\mathcal{C}_k$:

Simulatable codes - concatenated Steane code

Lemma (s-locally simulatable codes)

Fix s and let $k = \log_3(s)$. We have the following properties of k-fold concatenation of the Steane code $\mathcal{C}_k$:

1. *There is a* $\mathrm{poly}(2^k)$*-time* classical *algorithm that compute s-reduced density matrix of a* $\mathrm{Enc}_{\mathcal{C}_k}(\rho)$, *without knowing ρ*

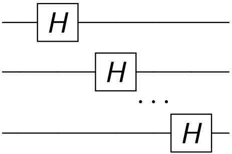
Simulatable codes - concatenated Steane code

Lemma (s-locally simulatable codes)

Fix s and let $k = \log_3(s)$. We have the following properties of k-fold concatenation of the Steane code $\mathcal{C}_k$:

1. *There is a* $\mathrm{poly}(2^k)$*-time* classical *algorithm that compute s-reduced density matrix of a* $\mathrm{Enc}_{\mathcal{C}_k}(\rho)$*, without knowing ρ*
2. *There is a* $\mathrm{poly}(2^k)$*-time* classical *algorithm that compute s-reduced density matrix of (partial) computation on* $\mathrm{Enc}_{\mathcal{C}_k}(\rho)$
   - *transversal Clifford gates*
   - T*-gadgets*

$Enc(\rho)$



CLDM is QMA-hard

Circuit-to-hamiltonian construction

Given a circuit $V = U_T ... U_1$ and initial state $|\psi_{init}\rangle$, there is a reduction to a 5-Local Hamiltonian H_V such that

CLDM is QMA-hard

Circuit-to-hamiltonian construction

Given a circuit $V = U_T ... U_1$ and initial state $|\psi_{init}\rangle$, there is a reduction to a 5-Local Hamiltonian H_V such that

- If V accepts with high probability, then the *history state*

$$\frac{1}{\sqrt{T+1}} \sum_{t \in [T+1]} |t\rangle \otimes U_t ... U_1 |\psi_{init}\rangle$$

  has low energy in respect to H_V.

CLDM is QMA-hard

Circuit-to-hamiltonian construction

Given a circuit $V = U_T ... U_1$ and initial state $|\psi_{init}\rangle$, there is a reduction to a 5-Local Hamiltonian H_V such that

- If V accepts with high probability, then the *history state*

$$\frac{1}{\sqrt{T+1}} \sum_{t \in [T+1]} |t\rangle \otimes U_t ... U_1 |\psi_{init}\rangle$$

  has low energy in respect to H_V.
- If V accepts with low probability, then all states have high energy in respect to H_V.

CLDM is QMA-hard

Circuit-to-hamiltonian construction

Given a circuit $V = U_T \dots U_1$ and initial state $|\psi_{init}\rangle$, there is a reduction to a 5-Local Hamiltonian H_V such that

- If V accepts with high probability, then the *history state*

$$\frac{1}{\sqrt{T+1}} \sum_{t \in [T+1]} |t\rangle \otimes U_t \dots U_1 |\psi_{init}\rangle$$

  has low energy in respect to H_V.
- If V accepts with low probability, then all states have high energy in respect to H_V.

Goal

Tweak the verification algorithm such that we can compute the reduced density matrices of history states.

CLDM is QMA-hard

Encoded circuit

Instead of $V = U_T \ldots U_1$ and initial state $|\psi_{init}\rangle$, consider the circuit V' that

1. Receives $\frac{1}{2^n} \sum_{a,b} Enc(|a,b\rangle \langle a,b| \otimes X^a Z^b |\psi\rangle \langle\psi| Z^b X^a)$
2. Check encoding of the witness
3. Undoes the OTP of the witness
4. Create $Enc(|0\rangle)$ and $Enc(|\mathrm{T}\rangle)$
5. Perform logical V on encoded states
6. Decode the output

CLDM is QMA-hard

Encoded circuit

Instead of $V = U_T \ldots U_1$ and initial state $|\psi_{init}\rangle$, consider the circuit V' that

1. Receives $\frac{1}{2^n}\sum_{a,b} Enc(|a,b\rangle\langle a,b| \otimes X^a Z^b |\psi\rangle\langle\psi| Z^b X^a)$
2. Check encoding of the witness
3. Undoes the OTP of the witness
4. Create $Enc(|0\rangle)$ and $Enc(|\mathrm{T}\rangle)$
5. Perform logical V on encoded states
6. Decode the output

Theorem

There is a classical simulator that computes in polynomial time the reduced density matrices of the history state of the encoded verifier.

CLDM is QMA-hard

Encoded circuit

Instead of $V = U_T \dots U_1$ and initial state $|\psi_{init}\rangle$, consider the circuit V' that

1. Receives $\frac{1}{2^n}\sum_{a,b} Enc(|a,b\rangle\langle a,b| \otimes X^a Z^b |\psi\rangle\langle\psi| Z^b X^a)$
2. Check encoding of the witness
3. Undoes the OTP of the witness
4. Create $Enc(|0\rangle)$ and $Enc(|\mathrm{T}\rangle)$
5. Perform logical V on encoded states
6. Decode the output

Theorem

There is a classical simulator that computes in polynomial time the reduced density matrices of the history state of the encoded verifier. Moreover there is a global state consistent with the reduced density matrices iff it is a yes-instance.

CLDM is QMA-hard - Overview of the proof

1. There is a polynomial-time algorithm that computes the density matrices of snapshot of the computation at time t
   - At every step, every qubit is encoded and if it is decoded, we know exactly its value

CLDM is QMA-hard - Overview of the proof

1. There is a polynomial-time algorithm that computes the density matrices of snapshot of the computation at time t
   - At every step, every qubit is encoded and if it is decoded, we know exactly its value
2. There is a polynomial-time algorithm that computes the density matrices of "invervals" of the computation
   - Uses the snapshot simulation with some loss in the parameters

CLDM is QMA-hard - Overview of the proof

1. There is a polynomial-time algorithm that computes the density matrices of snapshot of the computation at time t
   - At every step, every qubit is encoded and if it is decoded, we know exactly its value
2. There is a polynomial-time algorithm that computes the density matrices of “invervals” of the computation
   - Uses the snapshot simulation with some loss in the parameters
3. There is a polynomial-time algorithm that computes the density matrices of the history state
   - Most of clock qubits are traced-out, so the remaining state is a mixture of intervals

Proof of Quantum Knowledge

Proof of Quantum Knowledge

- Properties of (ZK) interactive proof system

  Completeness: there is a good strategy for yes-instance

  Soundness: there is no good strategy for no-instance

Proof of Quantum Knowledge

- Properties of (ZK) interactive proof system

  Completeness: there is a good strategy for yes-instance

  Soundness: there is no good strategy for no-instance
- Proof of Knowledge for NP:
  - If Prover passes with high enough probability, then a NP-witness is known

Proof of Quantum Knowledge

- Properties of (ZK) interactive proof system

  Completeness: there is a good strategy for yes-instance

  Soundness: there is no good strategy for no-instance
- Proof of Knowledge for NP:
  - If Prover passes with high enough probability, then a NP-witness is known
  - There is an extractor K, such that if $\tilde{P}$ passes with probability $\geq \kappa$

    $K^{\tilde{P}}$ outputs a good witness with high probability

Proof of Quantum Knowledge

- Properties of (ZK) interactive proof system

  Completeness: there is a good strategy for yes-instance

  Soundness: there is no good strategy for no-instance
- Proof of Knowledge for NP:
  - If Prover passes with high enough probability, then a NP-witness is known
  - There is an extractor K, such that if $\tilde{P}$ passes with probability $\geq \kappa$

    $K^{\tilde{P}}$ outputs a good witness with high probability
- Proof of Quantum Knowedge for QMA
  - If Prover passes with high enough probability, then a QMA-witness is known

Proof of Quantum Knowledge

- Properties of (ZK) interactive proof system

  Completeness: there is a good strategy for yes-instance

  Soundness: there is no good strategy for no-instance
- Proof of Knowledge for NP:
  - If Prover passes with high enough probability, then a NP-witness is known
  - There is an extractor K, such that if $\tilde{P}$ passes with probability $\geq \kappa$

    $K^{\tilde{P}}$ outputs a good witness with high probability
- Proof of Quantum Knowedge for QMA
  - If Prover passes with high enough probability, then a QMA-witness is known
  - B**G**'19: Definition of PoQ and prove that our protocol is also a PoQ

Proof of Quantum Knowledge

- Properties of (ZK) interactive proof system

  Completeness: there is a good strategy for yes-instance

  Soundness: there is no good strategy for no-instance

- Proof of Knowledge for NP:
  - If Prover passes with high enough probability, then a NP-witness is known
  - There is an extractor K, such that if $\tilde{P}$ passes with probability $\geq \kappa$

    $K^{\tilde{P}}$ outputs a good witness with high probability

- Proof of Quantum Knowedge for QMA
  - If Prover passes with high enough probability, then a QMA-witness is known
  - B**G**'19: Definition of PoQ[1] and prove that our protocol is also a PoQ

[1] Independent concurrent work by Coladangelo, Vidick and Zhang.

Open questions

- Find applications for QZK
- $\mathsf{MIP}^{ns} = \mathsf{PZK}\text{-}\mathsf{MIP}^{ns}$?
- QNIZK protocol for QMA in the CRS model
- QMA-hardness of (bosonic) representability [LCV'07, WMN'10], universal functional of density function theory [SV'09]

Thank you for your attention!