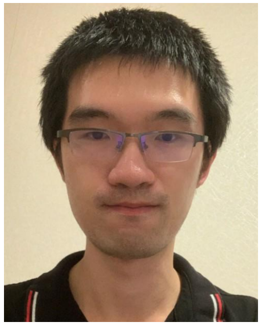
Quantum meets MCSP

Nai-Hui Chia Rice University

Joint work with



Chi-Ning Chou (Harvard), Ruizhe Zheng (UT Austin), and Jiayu Zhang (Caltech)

Minimum Circuit Size Problem

The Minimum Circuit Size Problem (MCSP) :

- Input: Truth table T of function f and s
- Output: Decide whether there exist circuits of size ≤s that compute f

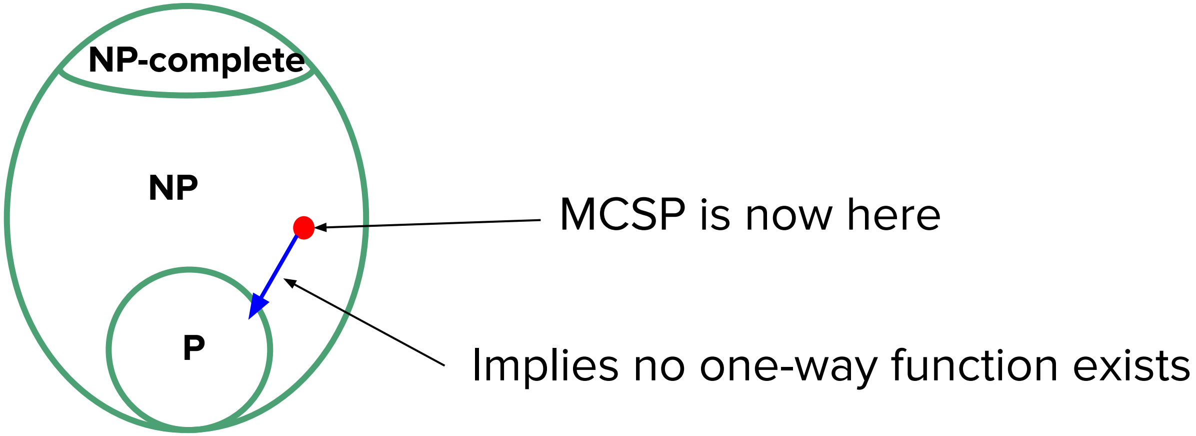
Minimum Circuit Size Problem

The Minimum Circuit Size Problem (MCSP) :

- Input: Truth table *T* of function f and *s*
- Output: Decide whether there exist circuits of size ≤s that compute f

- The input size is 2^n
- An efficient algorithm for MCSP runs in time **poly(2^n) = $2^{O(n)}$**.
- When s < logn, MCSP∈P by brute force search.
- When s > $2^n/n(1+\varepsilon)$, MCSP(f , s) = 1

The complexity of MCSP



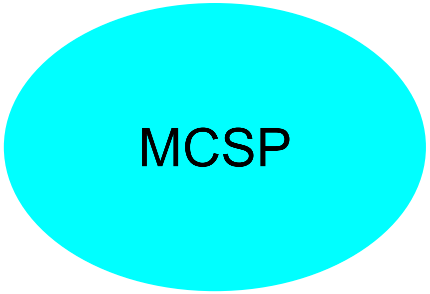
NP-intermediate problem

- MCSP ∈ NP (witness is the circuit, verifier just checks all 2^n inputs.)
- MCSP is unknown to be in any subclass of NP
- SZK ⊆ BPP^{MCSP} [Allender-Das'14]
- Perebor conjecture: brute force search is the best [Trakhtenbrot'84]
- Solving MCSP efficiently implies breaking OWF [Kabanets-Cai'00]
- Several variants are NP-hard

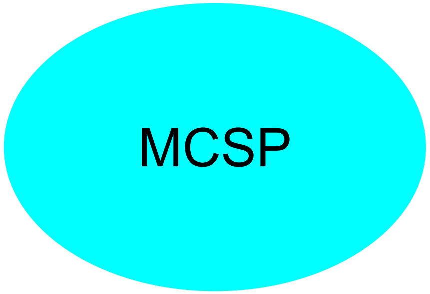
NP-hardness results for variants of MCSP

- [Masek'97]: DNF-MCSP is NP-hard
- [Hirahara-Oliveira-Santhanam'19]: DNF$\circ$XOR-MCSP is NP-hard
- [Ilango'19]: MOCSP (an oracle version) is NP-hard
- [Ilango-Loff-Oliveira'20]: Multi-MCSP is NP-hard
- [Ilango'20]: Depth-d-formula-MCSP and MCSP* are NP-hard
- [Hirahara'22]: Partial-MCSP is NP-hard

MCSP connects many problems in TCS



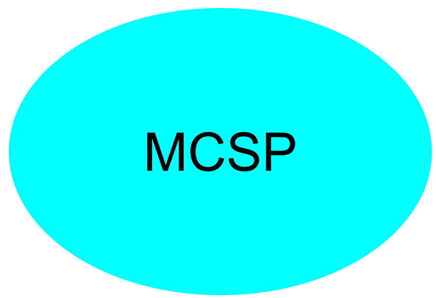
MCSP connects many problems in TCS



Circuit Lowr Bound

- [Razborov-Rudich'97]: MCSP∈ P⇒ natural property against P/poly
- [Kabanets-Cai'00]: MCSP∈ P⇒ circuit lower bound for P^{NP}
- [Murray-Williams 15]: MCSP∈ P⇒EXP ≠ ZPP
- [Arunachalam et al.'19]: MCSP∈ BQP⇒ new circuit lower bound for BQE

MCSP connects many problems in TCS



Circuit Lowr Bound

- [Razborov-Rudich'97]: MCSP$\in$ P$\Rightarrow$ natural property against P/poly
- [Kabanets-Cai'00]: MCSP$\in$ P$\Rightarrow$ circuit lower bound for P^{NP}
- [Murray-Williams 15]: MCSP$\in$ P$\Rightarrow$EXP $\neq$ ZPP
- [Arunachalam et al.'19]: MCSP$\in$ BQP$\Rightarrow$ new circuit lower bound for BQE

Learning theory

- [Carmosino et al.'16]: MCSP$\in$BPP$\Rightarrow$f $\in$ **size**(poly) can be PAC-learned in BPP

MCSP connects many problems in TCS

MCSP

Cryptography

- [Kabanets-Cai'00]: MCSP ∈ BPP ⇒ ∄ PRG ⇒ ∄ OWF
- [Allender-Da'14]: SZK ⊆ BPP^{MCSP}
- [Impagliazzo et al.'18]: Indistinguishable obfuscator(iO) ⇒ SAT $\leq_R$ MCSP

Circuit Lowr Bound

- [Razborov-Rudich'97]: MCSP∈ P⇒ natural property against P/poly
- [Kabanets-Cai'00]: MCSP∈ P⇒ circuit lower bound for P^{NP}
- [Murray-Williams 15]: MCSP∈ P⇒EXP ≠ ZPP
- [Arunachalam et al.'19]: MCSP∈ BQP⇒ new circuit lower bound for BQE

Learning theory

- [Carmosino et al.'16]: MCSP∈BPP⇒f ∈ **size**(poly) can be PAC-learned in BPP

MCSP connects many problems in TCS

Average-case complexity

- [Hirahara'18]: an approximate version of MCSP is NP-hard$\Rightarrow$equivalence of worst- and average-case hardness of NP

Cryptography

- [Kabanets-Cai'00]: MCSP $\in$ BPP$\Rightarrow\nexists$ PRG$\Rightarrow\nexists$ OWF
- [Allender-Da'14]: SZK $\subseteq$ BPP^{MCSP}
- [Impagliazzo et al.'18]: Indistinguishable obfuscator(iO) $\Rightarrow$ SAT $\leq_R$ MCSP

MCSP

Circuit Lowr Bound

- [Razborov-Rudich'97]: MCSP$\in$ P$\Rightarrow$ natural property against P/poly
- [Kabanets-Cai'00]: MCSP$\in$ P$\Rightarrow$ circuit lower bound for P^{NP}
- [Murray-Williams 15]: MCSP$\in$ P$\Rightarrow$EXP $\neq$ ZPP
- [Arunachalam et al.'19]: MCSP$\in$ BQP$\Rightarrow$ new circuit lower bound for BQE

Learning theory

- [Carmosino et al.'16]: MCSP$\in$BPP$\Rightarrow$f $\in$ **size**(poly) can be PAC-learned in BPP

Why do we study **quantum** MCSP

- We attended the MCSP workshop in STOC 2020
  - Hardness is mysterious
  - Connect many problems in TCS

Why do we study **quantum** MCSP

- We attended the MCSP workshop in STOC 2020
  - Hardness is mysterious
  - Connect many problems in TCS
- MCSP is asking complexity of **classical** circuit complexity for **classical** objects (i.e., boolean functions).
- How about complexity of **quantum** circuit complexity for **classical/quantum** objects (such as quantum states, unitary matrices, and Boolean functions)

Why do we study **quantum** MCSP

- We attended the MCSP workshop in STOC 2020
  - Hardness is mysterious
  - Connect many problems in TCS
- MCSP is asking complexity of **classical** circuit complexity for **classical** objects (i.e., boolean functions).
- How about complexity of **quantum** circuit complexity for **classical/quantum** objects (such as quantum states, unitary matrices, and Boolean functions)

Goal:

- Study the complexity of problems asking for quantum circuit complexity of quantum objects
- Connects quantum problems through quantum MCSP

"Understand quantum computing through the lens of meta-complexity"

Quantum MCSP: boolean function/quantum circuit

Boolean Minimum Quantum Circuit Size Problem (MQCSP):

- **Input:** Truth table T of f: $\{0, 1\}^n \to \{0, 1\}$ and an integer t
- **Output:** quantum circuit that can compute f by using at most t gates?

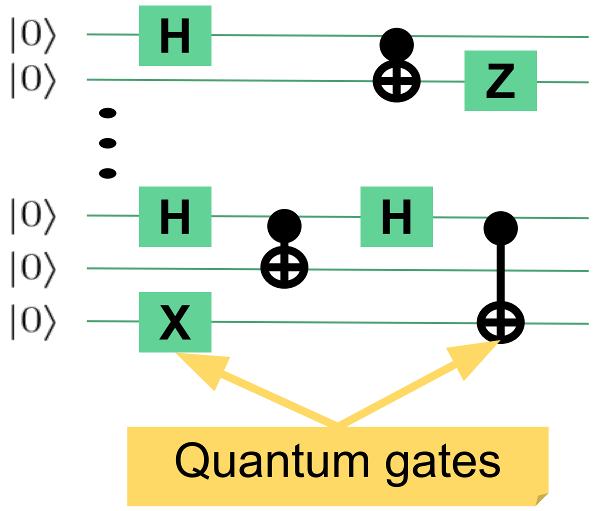
Unitary Minimum Quantum Circuit Size Problem (UMCSP):

- **Input:** Matrix M of a unitary $U \in C^{N \times N}$ and 1^t
- **Output:** quantum circuit that can compute U by using at most t gates?

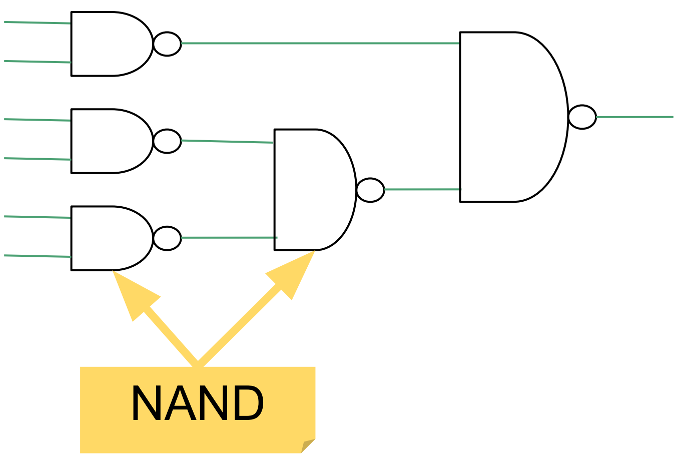
State Minimum Quantum Circuit Size Problem (SMCSP):

- **Input 1:** Vector V of an n-qubit state $|s\rangle \in C^N$ and an integer 1^t
- **Input 2:** Access to arbitrarily many copies of $|s\rangle$, 1^n, and 1^t
- **Output:** quantum circuit that can compute $|s\rangle$ by using at most t gates?

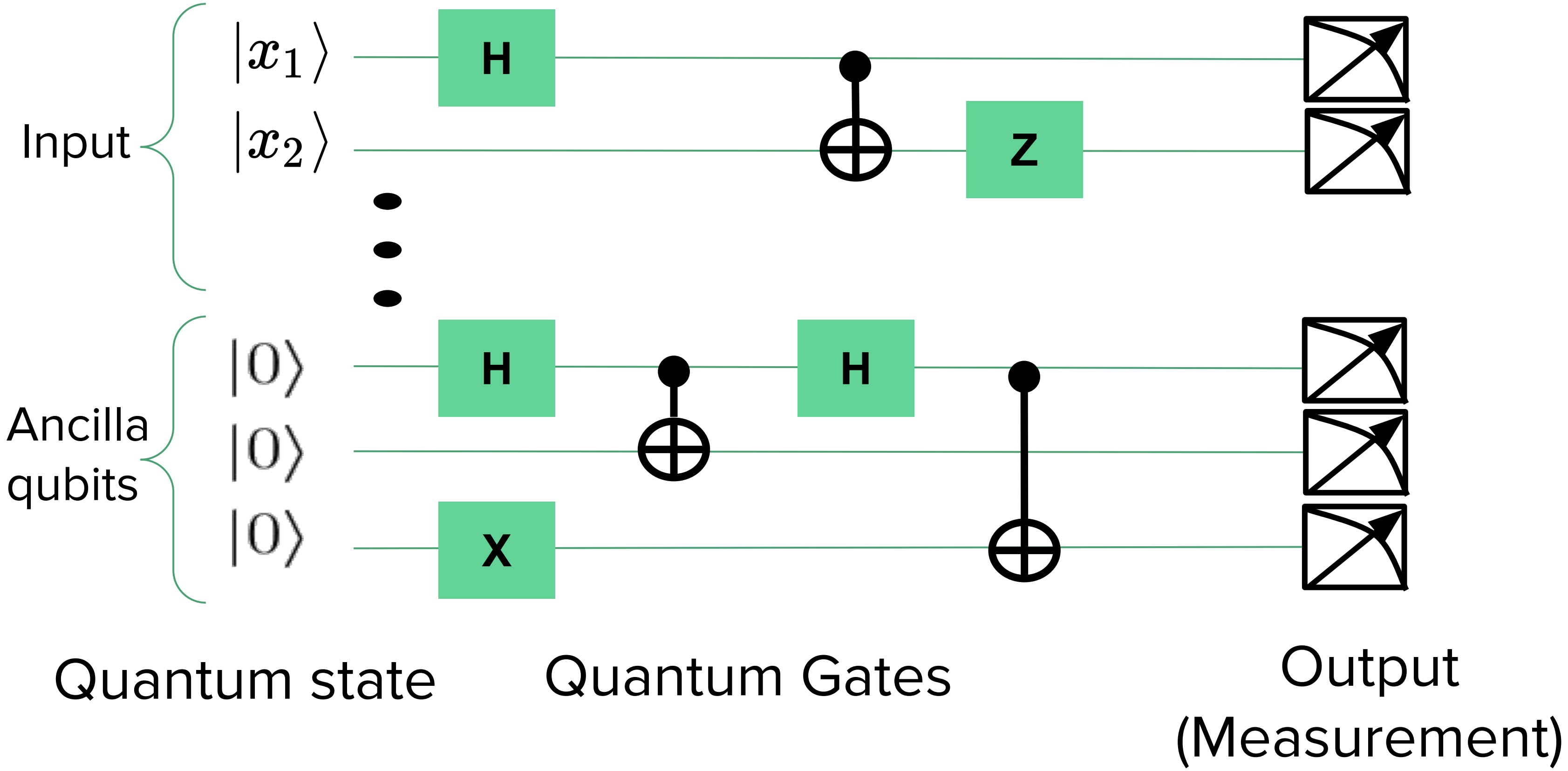
Quantum circuit model



Classical circuit model

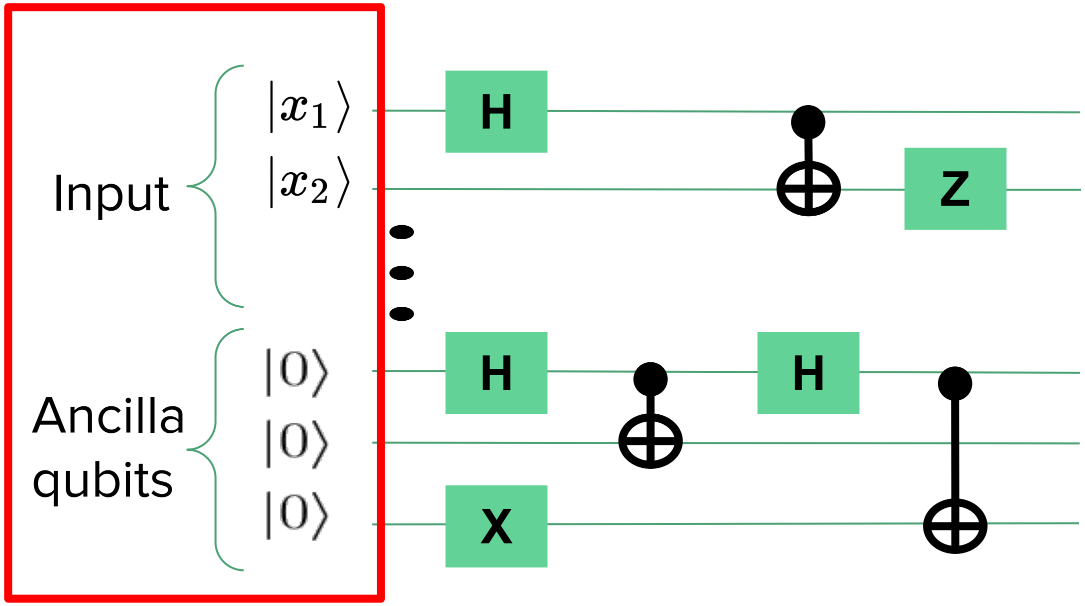


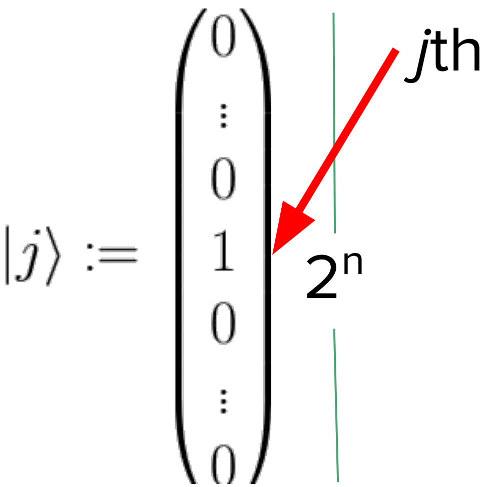
Quantum circuit model



Quantum states

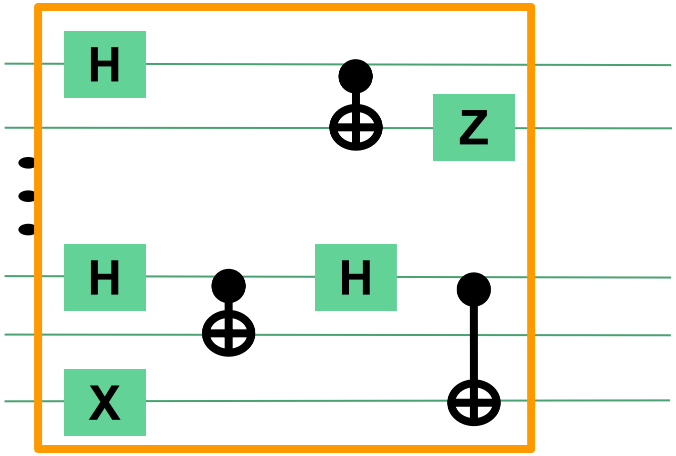
n-qubit quantum state: $\sum_{j\in\{0,1\}^n} c_j|j\rangle$, where $c_j \in \mathbb{C}$ and $\sum_j |c_j|^2 = 1$





- Input: $|x\rangle$ and $|0^{\text{poly}(n)}\rangle$
- This represents a $2^{\text{poly(n)}}$-dimensional vector

Quantum gates

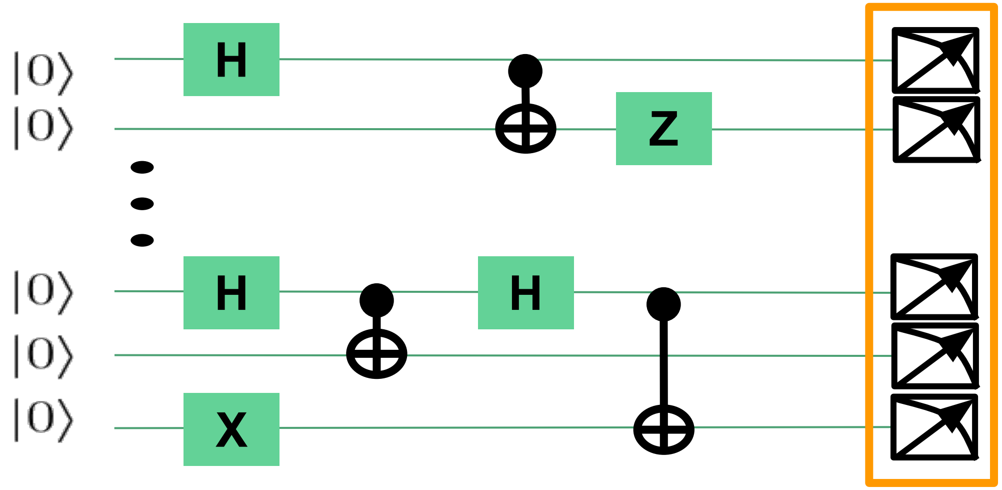


Unitary operator on *n* qubits:

$$U \in \mathbb{C}^{2^n \times 2^n} \qquad UU^\dagger = U^\dagger U = \mathcal{I} \qquad U^\dagger = (U^*)^T$$

$$CNOT := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Quantum universal gate set: CNOT + all single-qubit unitaries



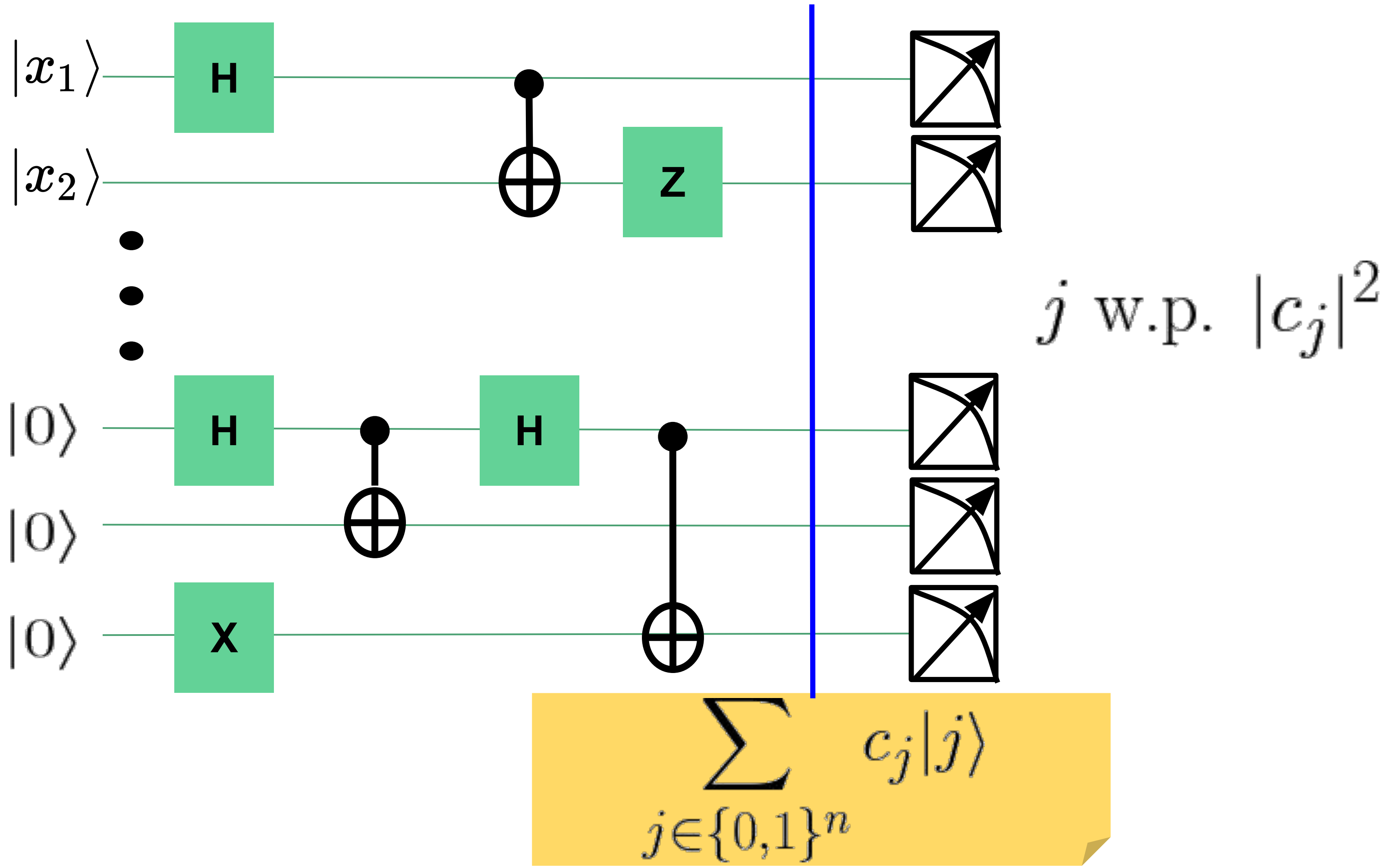
Measurement: Extract classical information from quantum information.

$$\sum_{j\in\{0,1\}^n} c_j|j\rangle \xrightarrow{\text{Measure}} j \text{ with probability } |c_j|^2$$

Schrödinger's Cat:

$$\frac{1}{\sqrt{2}}|Dead\rangle + \frac{1}{\sqrt{2}}|Live\rangle \xrightarrow{Measure} \text{Dead } or \text{ Live } w.p. \, 1/2$$

Quantum circuit



Properties of QC that affects quantum MCSP

- Quantum computing is generally **random and erroneous**
  - Decision problem ➜ Promise problems
- Quantum circuit is **reversible**
  - Search-to-decision reduction and self-reduction for UMCSP and SMCSP
- **Ancilla qubits**
  - Make the problems "harder" (NP ➜ QCMA)
- Various **universal quantum gate sets**
  - Certain results only hold for particular gate sets.
- ∃Small **classical** circuit ⇒ ∃Small **quantum** circuit

MQCSP

- Hardness of MQCSP
- MQCSP and cryptography
- MQCSP and learning theory
- MQCSP and circuit lower bounds

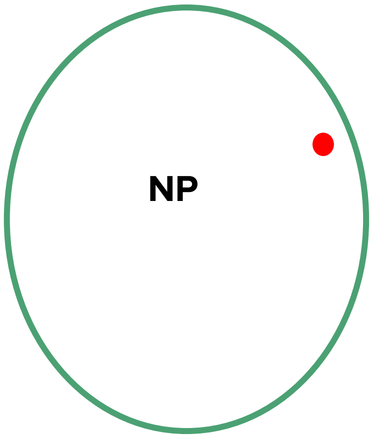
Unconditional hardness of MQCSP

Boolean Minimum Quantum Circuit Size Problem (MQCSP):

- **Input:** Truth table T of f: $\{0, 1\}^n \rightarrow \{0, 1\}$ and an integer t ($0 < t < 2^n$)
- **Output:** quantum circuit that can compute f by using at most t gates?

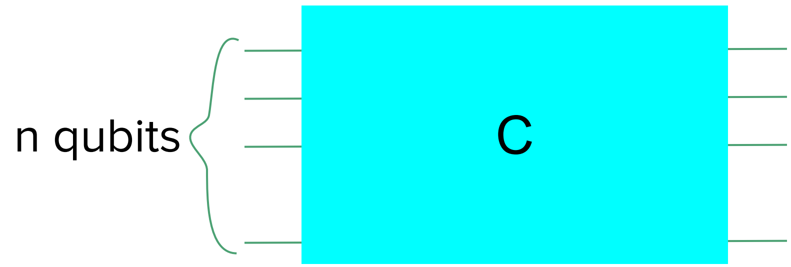
1. MQCSP ∈ **QCMA**
   - QCMA: Like MA, but allowing efficient quantum verifier and classical witness
   - Why not in NP? Ancilla qubits!
2. **Multi-output** MQCSP is NP-hard
   - "Quantize" the classical Np-hardness result of multi-output MCSP [Ilango-Loff-Oliveira'20]
   - Depends on the universal quantum gate set
   - Under randomized reduction
3. MQCSP is **SZK-hard**
   - MQCSP oracle can break PRG

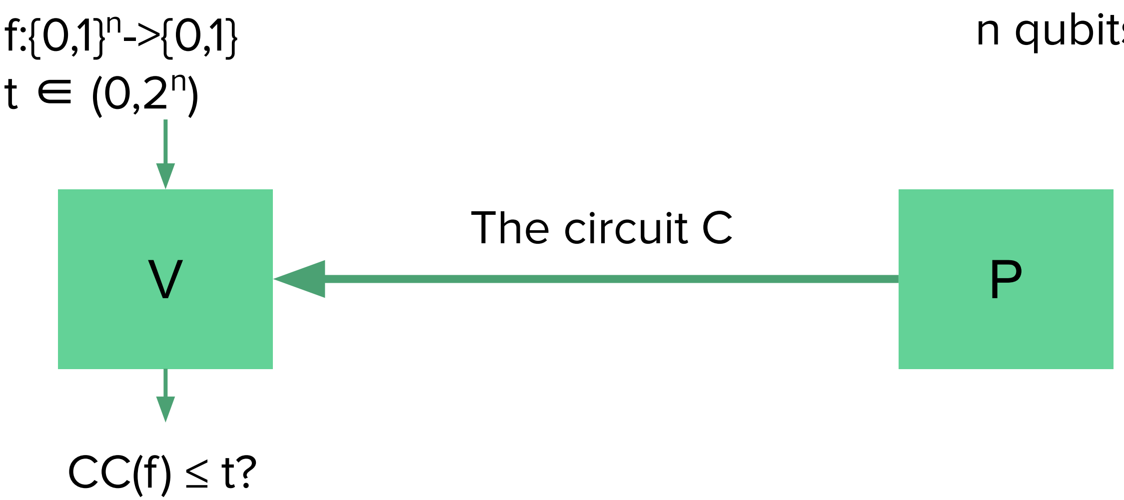
MQCSP ∈ NP?



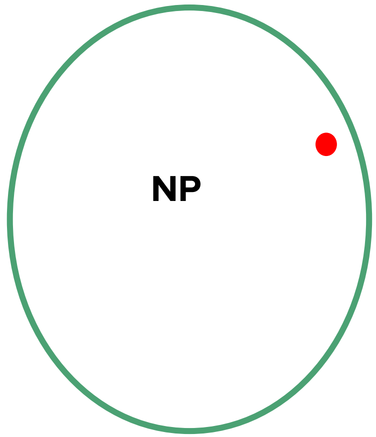
Suppose f has quantum circuit size ≤ t,

- Let C be the quantum circuit that computes f without using any ancilla qubits.



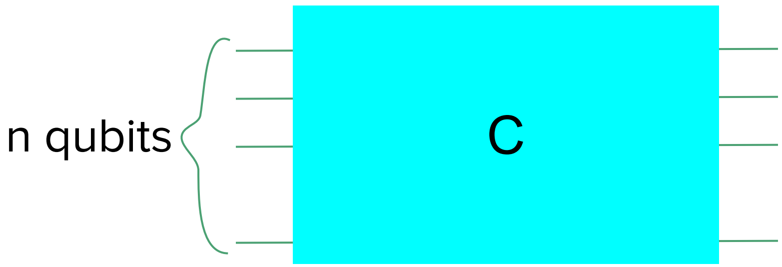


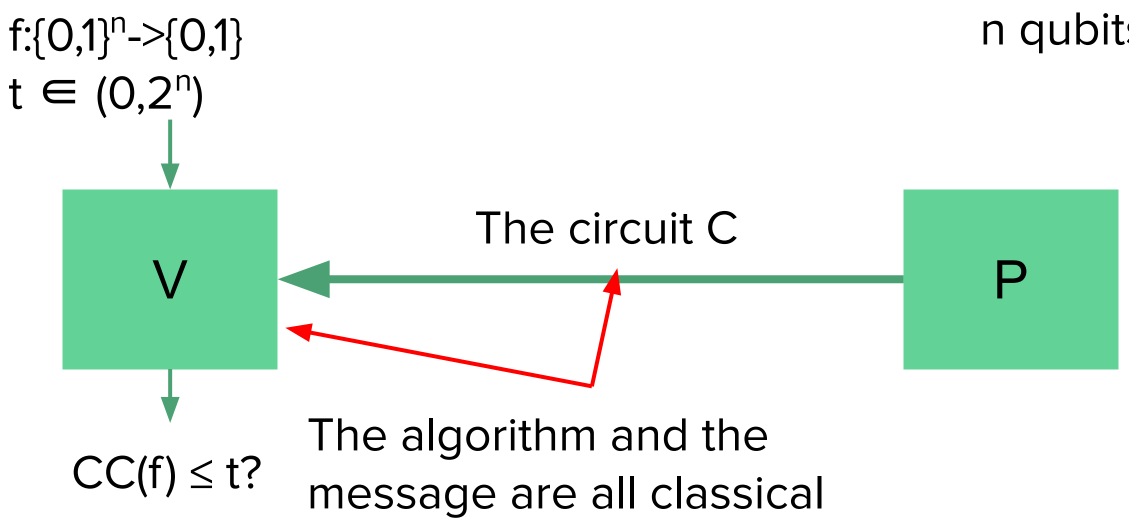
MQCSP ∈ NP?



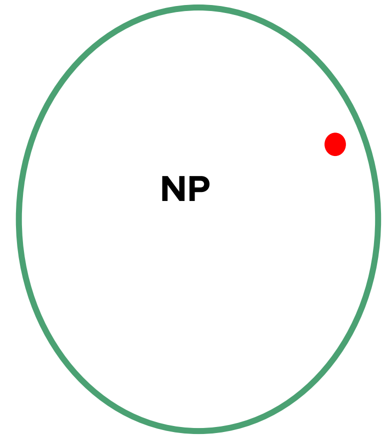
Suppose f has quantum circuit size $\leq t$,

- Let C be the quantum circuit that computes f without using any ancilla qubits.
- V cannot run C on $x \in \{0,1\}^n$ since it only has classical power.



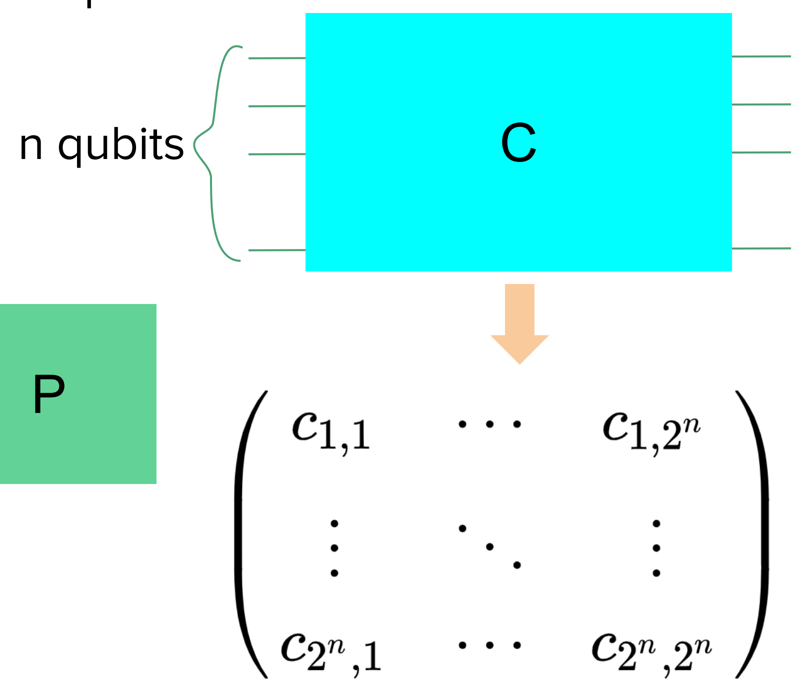


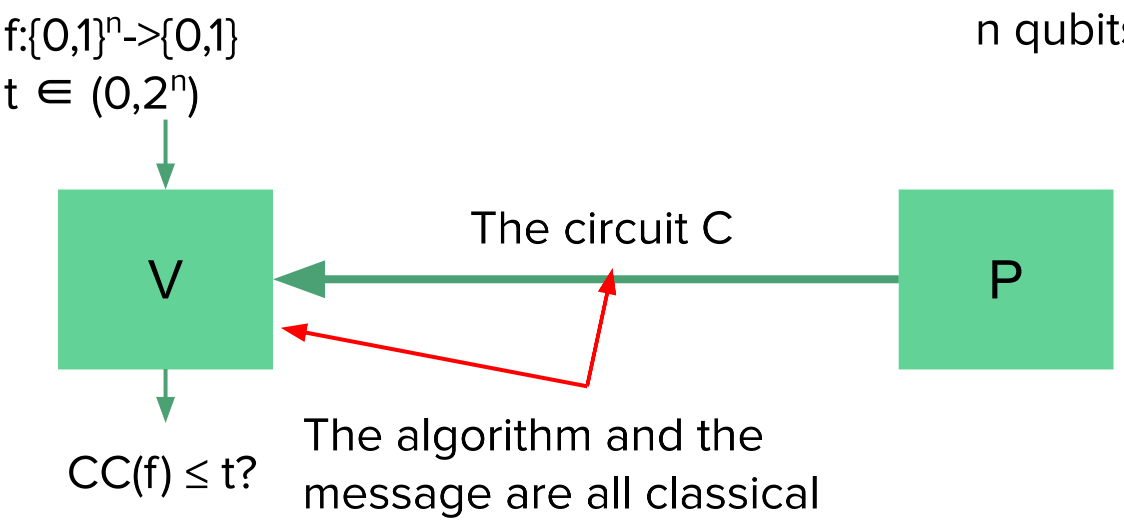
MQCSP $\in$ NP?



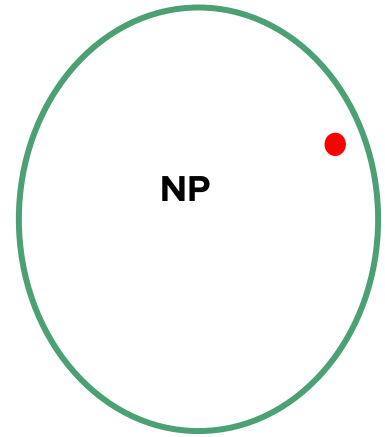
Suppose f has quantum circuit size $\leq$ t,

- Let C be the quantum circuit that computes f without using any ancilla qubits.
- V cannot run C on $x \in \{0,1\}^n$ since it only has classical power.
- Since we allow V to run in $\mathbf{2^{O(n)}}$, we can compute the unitary of C that takes $O(2^{2n})$ time.



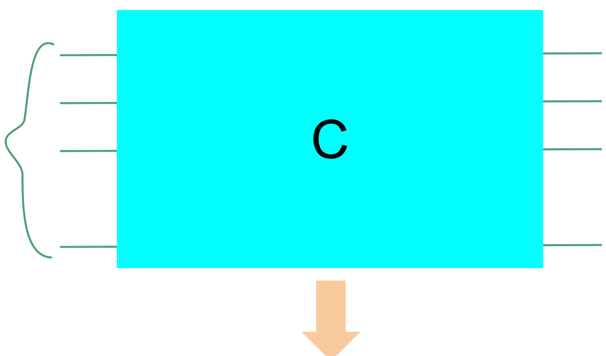


MQCSP ∈ NP?



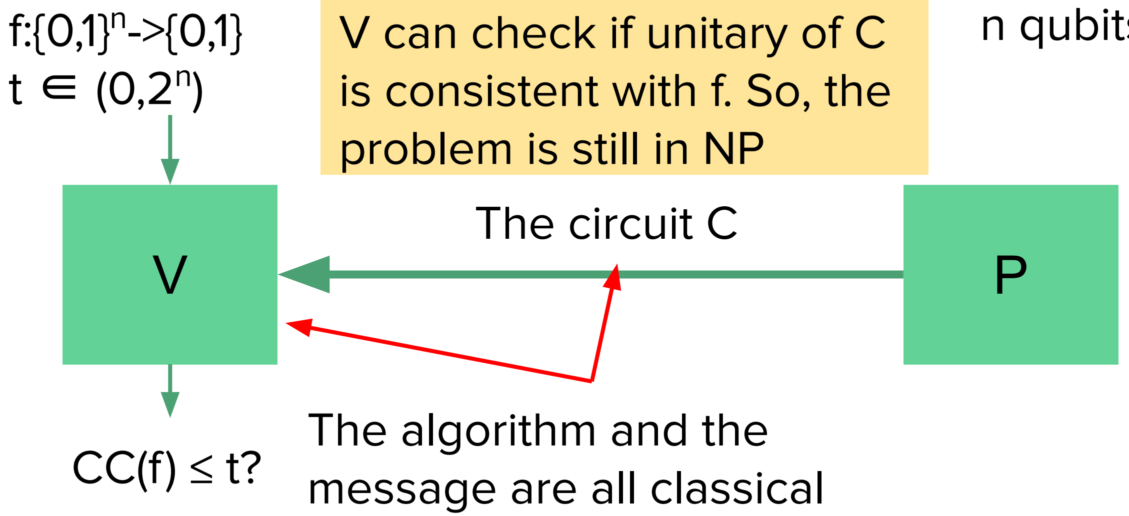
Suppose f has quantum circuit size $\leq t$,

- Let C be the quantum circuit that computes f without using any ancilla qubits.
- V cannot run C on $x \in \{0,1\}^n$ since it only has classical power.
- Since we allow V to run in $\mathbf{2^{O(n)}}$, we can compute the unitary of C that takes $O(2^{2n})$ time.



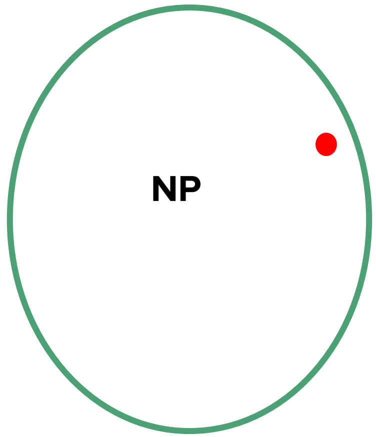
$$\begin{pmatrix} c_{1,1} & \cdots & c_{1,2^n} \\ \vdots & \ddots & \vdots \\ c_{2^n,1} & \cdots & c_{2^n,2^n} \end{pmatrix}$$

V can check if unitary of C is consistent with f. So, the problem is still in NP



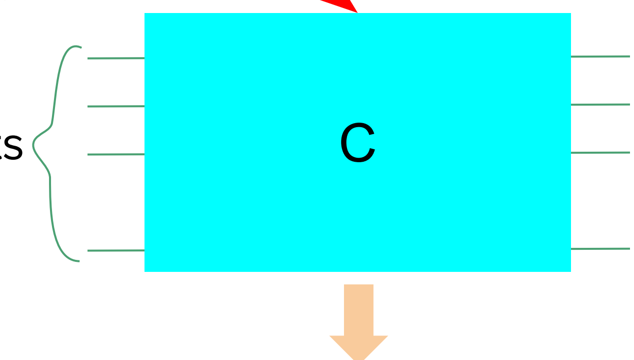
MQCSP ∈ NP?

What if we allow poly(n) ancilla qubits?



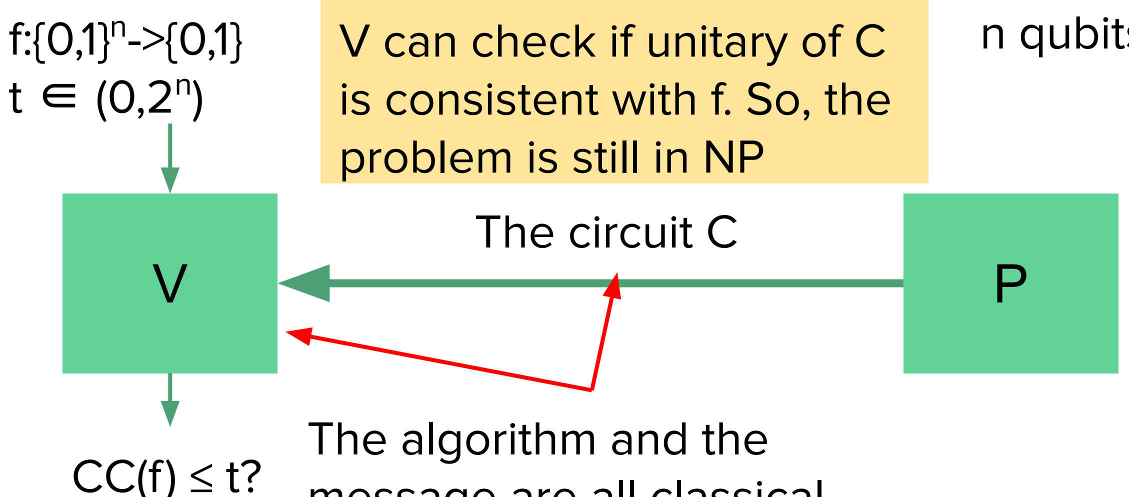
Suppose f has quantum circuit size ≤ t,

- Let C be the quantum circuit that computes f without using any ancilla qubits.
- V cannot run C on x∈$\{0,1\}^n$ since it only has classical power.
- Since we allow V to run in $\mathbf{2^{O(n)}}$, we can compute the unitary of C that takes $O(2^{2n})$ time.



$$\begin{pmatrix} c_{1,1} & \cdots & c_{1,2^n} \\ \vdots & \ddots & \vdots \\ c_{2^n,1} & \cdots & c_{2^n,2^n} \end{pmatrix}$$

V can check if unitary of C is consistent with f. So, the problem is still in NP



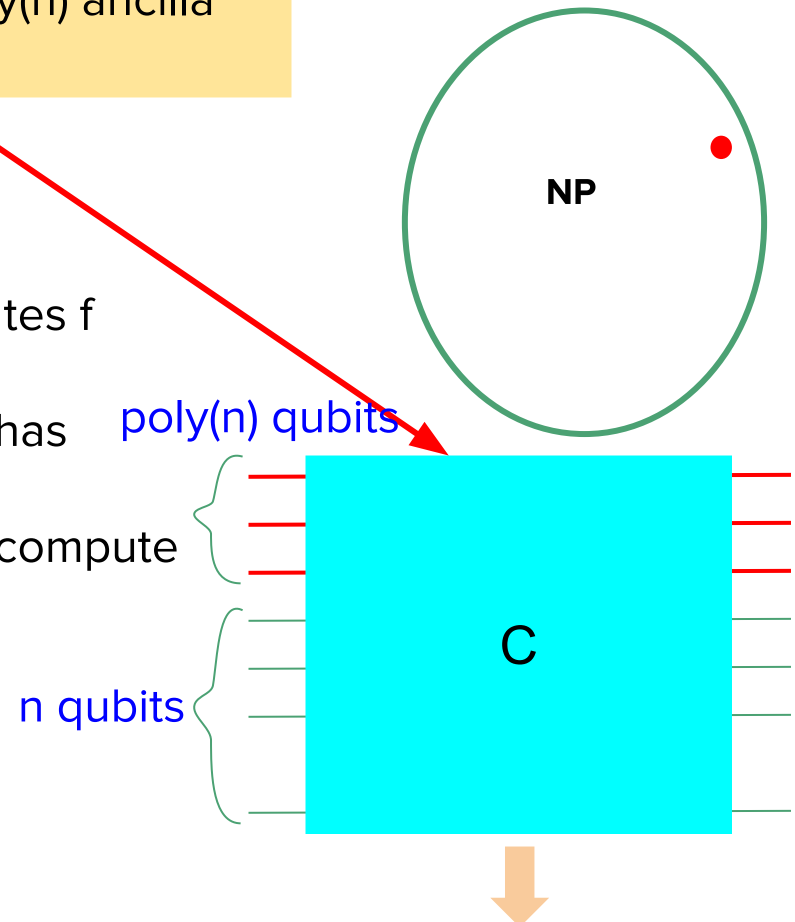
The algorithm and the message are all classical

MQCSP ∈ NP?

What if we allow poly(n) ancilla qubits?

Suppose f has quantum circuit size $\leq t$,

- Let C be the quantum circuit that computes f without using any ancilla qubits.
- V cannot run C on $x \in \{0,1\}^n$ since it only has classical power.
- Since we allow V to run in $\mathbf{2^{O(n)}}$, we can compute the unitary of C that takes $O(2^{2n})$ time.



$$\begin{pmatrix} c_{1,1} & \cdots & c_{1,2^{poly(n)}} \\ \vdots & \ddots & \vdots \\ c_{2^{poly(n)},1} & \cdots & c_{2^{poly(n)},2^{poly(n)}} \end{pmatrix}$$

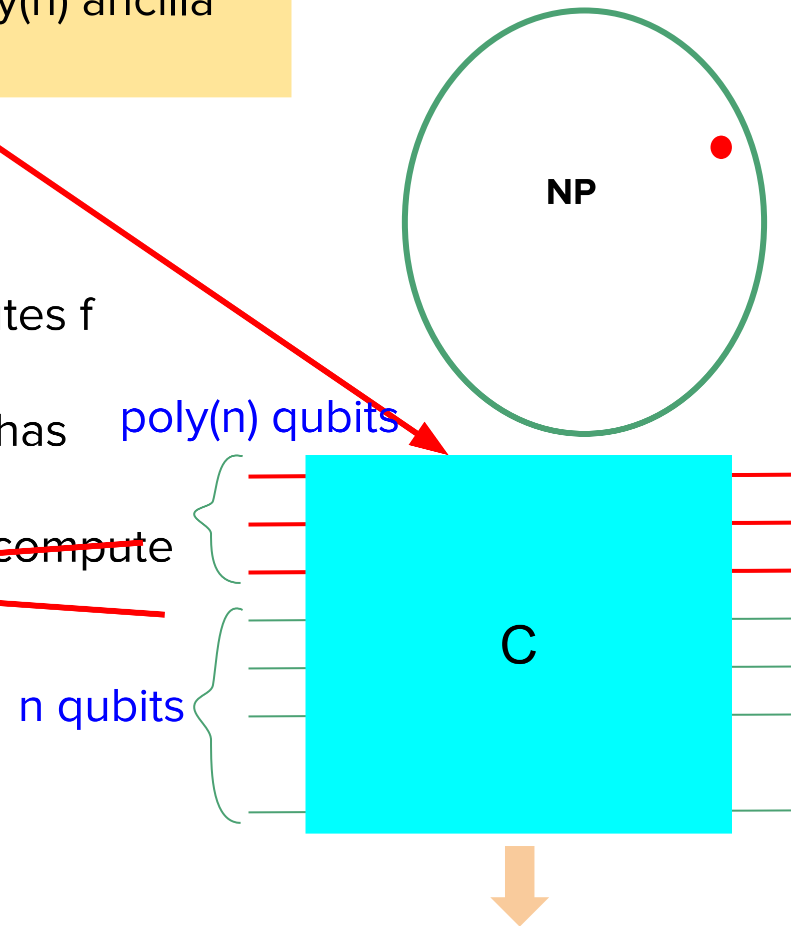
MQCSP ∈ NP?

What if we allow poly(n) ancilla qubits?

Suppose f has quantum circuit size ≤ t,

- Let C be the quantum circuit that computes f without using any ancilla qubits.
- V cannot run C on $x \in \{0,1\}^n$ since it only has classical power.
- ~~Since we allow V to run in $2^{O(n)}$, we can compute the unitary of C that takes $O(2^{2n})$ time.~~

Now, this approach takes time $2^{poly(n)}$ to compute the unitary matrix of C, which is not efficient.



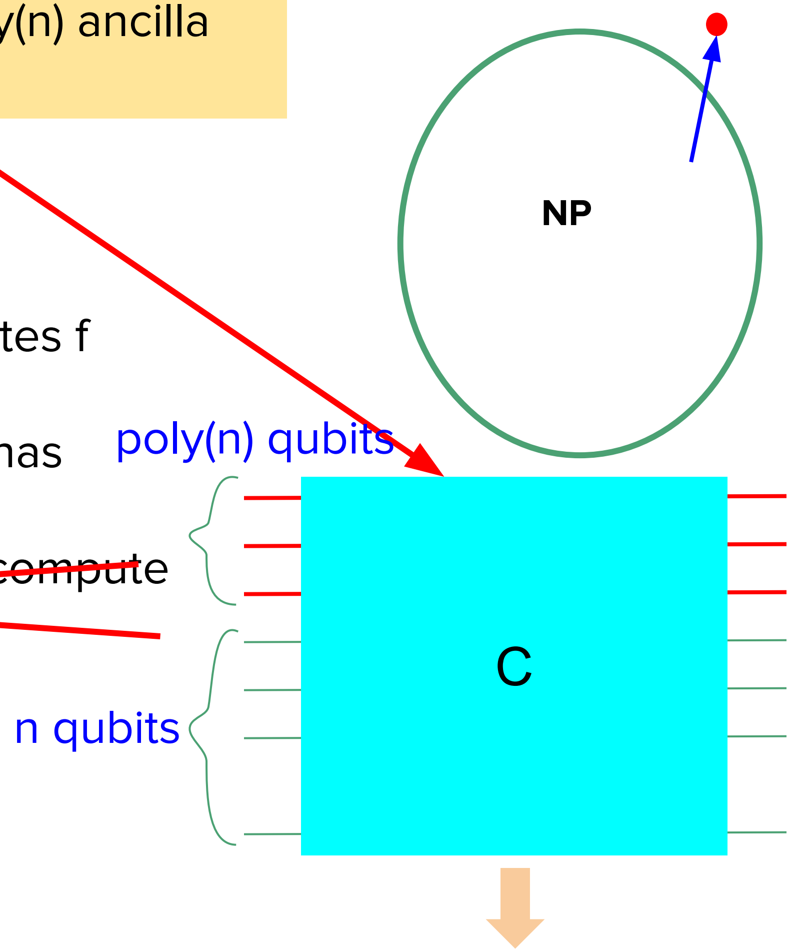
$$\begin{pmatrix} c_{1,1} & \cdots & c_{1,2^{poly(n)}} \\ \vdots & \ddots & \vdots \\ c_{2^{poly(n)},1} & \cdots & c_{2^{poly(n)},2^{poly(n)}} \end{pmatrix}$$

MQCSP ∈ NP?

What if we allow poly(n) ancilla qubits?

Suppose f has quantum circuit size ≤ t,

- Let C be the quantum circuit that computes f without using any ancilla qubits.
- V cannot run C on $x \in \{0,1\}^n$ since it only has classical power.
- ~~Since we allow V to run in $2^{O(n)}$, we can compute the unitary of C that takes $O(2^{2n})$ time.~~



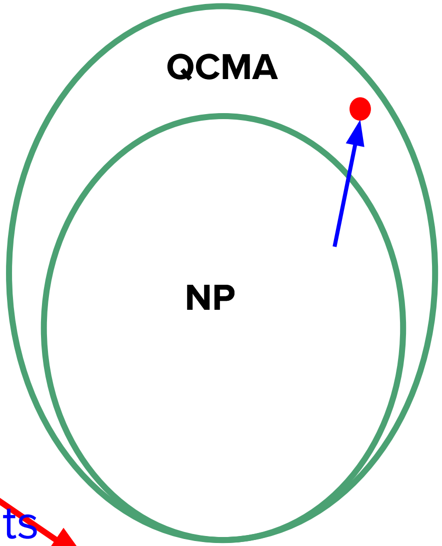
$$\begin{pmatrix} c_{1,1} & \cdots & c_{1,2^{poly(n)}} \\ \vdots & \ddots & \vdots \\ c_{2^{poly(n)},1} & \cdots & c_{2^{poly(n)},2^{poly(n)}} \end{pmatrix}$$

Now, this approach takes time $2^{poly(n)}$ to compute the unitary matrix of C, which is not efficient.

Okay, we don't know how to put it into NP yet....

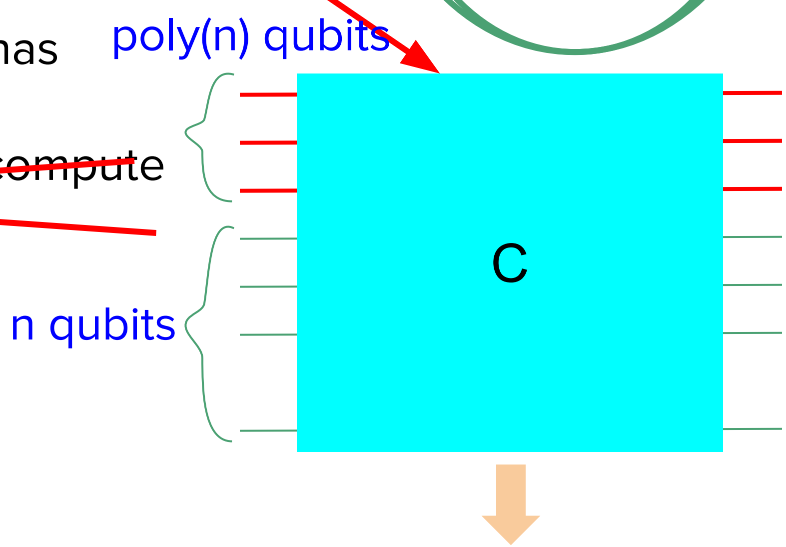
MQCSP ∈ NP?

What if we allow poly(n) ancilla qubits?



Suppose f has quantum circuit size ≤ t,

- Let C be the quantum circuit that computes f without using any ancilla qubits.
- V cannot run C on $x \in \{0,1\}^n$ since it only has classical power.
- ~~Since we allow V to run in $2^{O(n)}$, we can compute the unitary of C that takes $O(2^{2n})$ time.~~



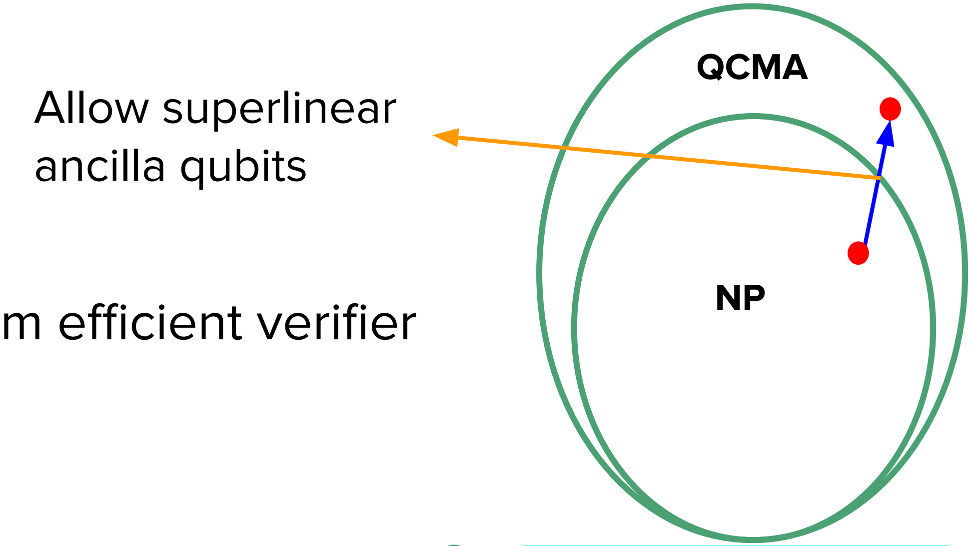
Now, this approach takes time $2^{poly(n)}$ to compute the unitary matrix of C, which is not efficient.

$$\begin{pmatrix} c_{1,1} & \cdots & c_{1,2^{poly(n)}} \\ \vdots & \ddots & \vdots \\ c_{2^{poly(n)},1} & \cdots & c_{2^{poly(n)},2^{poly(n)}} \end{pmatrix}$$

Okay, we don't know how to put it into NP yet....

But we can put it into "**QCMA**"

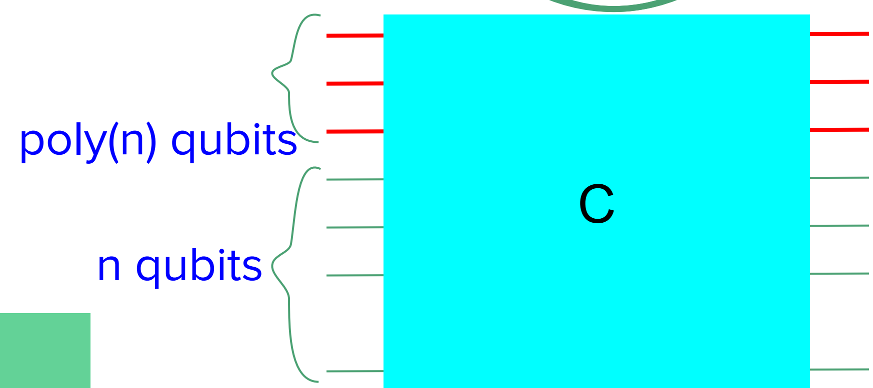
MQCSP ∈ QCMA

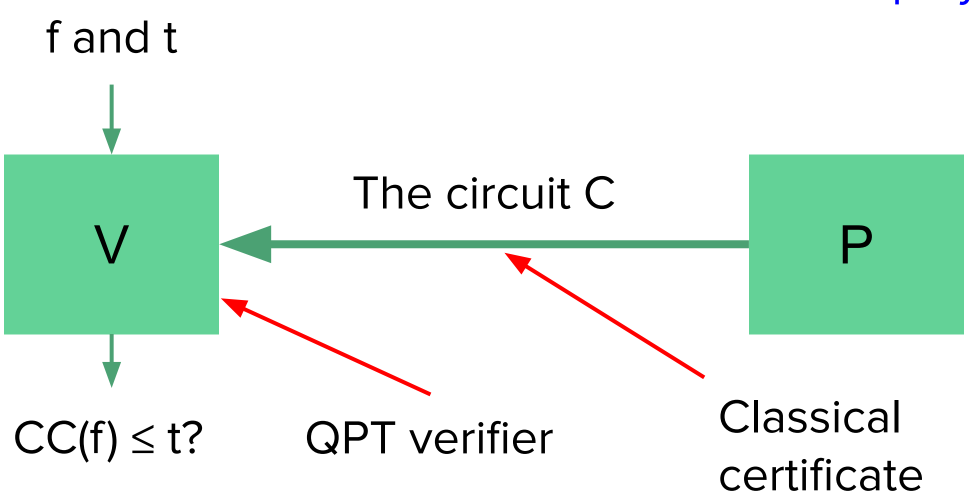


QCMA: Like MA, but with quantum efficient verifier

V:

- Implement C
- Run C on |x,0> for all x∈$\{0,1\}^n$
- Check if it is consistent with T(f).





- When O(n) ancilla qubits, MQCSP∈NP
- When ω(n) ancilla qubits, MQCSP∈QCMA

MQCSP and **cryptography**

1. $\exists$ quantum-secure OWF $\Rightarrow$ MQCSP $\notin$ BQP
    - PRG paradigm
2. Suppose $\exists$ post-quantum iO. Then NP$\not\subset$coRQP $\Rightarrow$ MQCSP $\notin$ BQP
    - coRQP: quantumly polynomial time with perfect soundness and bounded-error completeness
    - The other direction is unknown since MQCSP is unknown to be in NP

Main questions:

- Use the hardness of MQCSP to build cryptographic primitives
- Cryptographic primitives $\Rightarrow$ hardness of MQCSP

MQCSP and **learning theory**

1. **PAC learn quantum circuits**

   ∃ efficient PAC learning algorithms for BQP/poly ⇔ ∃ an efficient randomized algorithm for MQCSP

2. **Quantum learning algorithms for class C**

   ∃ efficient quantum learning algorithms for PAC learn a circuit class C ⇔ ∃ an efficient quantum algorithm for C-MQCSP

- Follow [Arunachalam et al.'19]
- Relate quantum learning theory to the hardness of MQCSP

MQCSP and **circuit lower bounds**

1. **Quantum circuit lower bounds**
   a. MQCSP$\in$BQP $\Rightarrow$ BQE and $BQP^{QCMA} \not\subset BQSIZE[n^k]$ for any k
      i. Quantum natural property against quantum circuit classes
      ii. Diagonalization lemma for quantum circuits
2. **Hardness amplification**
   a. MQCSP$\in$BQP $\Rightarrow$ $\exists$ BQP alg: f where $QCC(f)=2^{\Omega(n)}$ $\rightarrow$ $2^{\Omega(n)}$ f's where f $QCC(f)=2^{\Omega(n)}/\Omega(n)$
3. **Hardness magnification**
   a. Gap-MQCSP $\notin$ $BQSIZE[2^{n+O(\sqrt{n})}]$ $\Rightarrow$ QCMA $\not\subset$ $BQSIZE[n^k]$ for any k
4. **Fine-grained complexity**
   a. QETH $\Rightarrow$ $N^{o(\log\log N)}$-hardness of MQCSP*
      i. QETH: k-SAT cannot be solved in quantum $2^{o(n)}$-time

Quantum MCSP for **Quantum objects**

Unitary Minimum Quantum Circuit Size Problem (UMCSP):

- **Input:** Matrix M of a unitary $U \in C^{N \times N}$ and 1^t
- **Output:** quantum circuit C with size $\leq t$ that can compute U

$$\forall |\psi\rangle,\ |\langle\psi|U^\dagger C|\psi\rangle|^2 \approx 1$$

State Minimum Quantum Circuit Size Problem (SMCSP):

- **Input 1:** Vector V of an n-qubit state $|s\rangle \in C^N$ and an integer 1^t
- **Input 2:** Access to arbitrarily many copies of $|s\rangle$, 1^n, and 1^t
- **Output:** quantum circuit that can compute $|s\rangle$ by using at most t gates?

$$|\langle s|C|0\rangle|^2 \approx 1$$

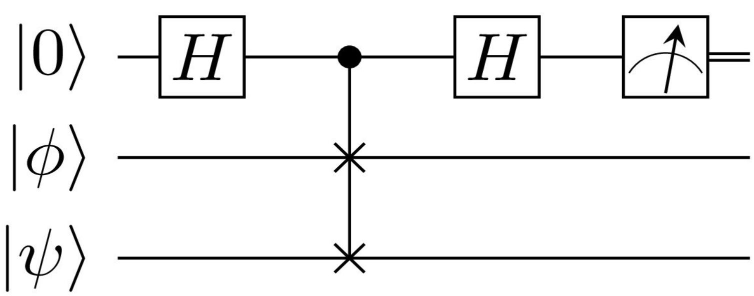
Our results for UMCSP and SMCSP

- UMCSP and SMCSP are in **QCMA**
- **Reductions** for UMCSP and SMCSP
    - Search-to-decision reductions
    - Self-reduction
- Applications of UMCSP and SMCSP

SMCSP is in **QCMA**

SMCSP is in QCMA

- **Witness:** quantum circuit C of size ≤t that computes |s>
- **Verification:**
  - **SMCSP:** Swap test on |s> and C|0>
- Prepare |s> from the inputs
  - **Input 1:** Vector V of an n-qubit state |s>∈C^N
    - Given V, one can prepare |s> using 2^n controlled rotations
  - **Input 2:** Access to arbitrarily many copies of |s>



$$\Pr[\text{Outputs } 0] = \frac{1}{2} + \frac{|\langle\phi|\psi\rangle|}{2}$$

UMCSP is in **QCMA**

- **Naive approach:** Swap test for all computational-basis states
  - **Fail!** C and U can differ on **superposition states**
    - E.g., C(|0>+|1>) = |0> - |1>. But, U(|0>+|1>) = |0>+|1>
  - Tests on all computational basis give no information about the **phase**
    - E.g., Cannot distinguish - |1> and |1>
  - **Entanglement** between output qubits and ancilla qubits
- **Coherent test:** Swap test on all states of the form $\frac{1}{\sqrt{2}}(|a\rangle + |b\rangle)$, for all $a, b \in \{0,1\}^n$

Key lemma: Suppose $\mathcal{C}$ passes the "standard basis test" + "coherent test" with high probability. Then, for any $a, b \in \{0,1\}^n$, define the ancilla states $|\chi_a\rangle$, $|\chi_b\rangle$ as follows:

$$(U^\dagger \otimes I)\mathcal{C}|a, 0\rangle \approx_\delta |a\rangle|\chi_a\rangle$$
$$(U^\dagger \otimes I)\mathcal{C}|b, 0\rangle \approx_\delta |b\rangle|\chi_b\rangle$$

We have $|\chi_a\rangle \approx_\epsilon |\chi_b\rangle$.

Search-to-decision reductions

- Unknown whether MCSP has search-to-decision reduction
  - MCSP∈BPP⇒randomized poly-time algorithms for finding an approximately optimal circuit [Carmosino et al.'16]
  - Search-to=decision reduction for Gap-MCSP [Hirahara'18]
  - Search-to-decision reduction for AveMCSP [Santhanam'19]
  - Search-to-decision reduction for MFSP [Ilango'20]
  - Relativization barrier for deterministic search-to-decision reduction for MCSP [Ren-Santhanam'21]

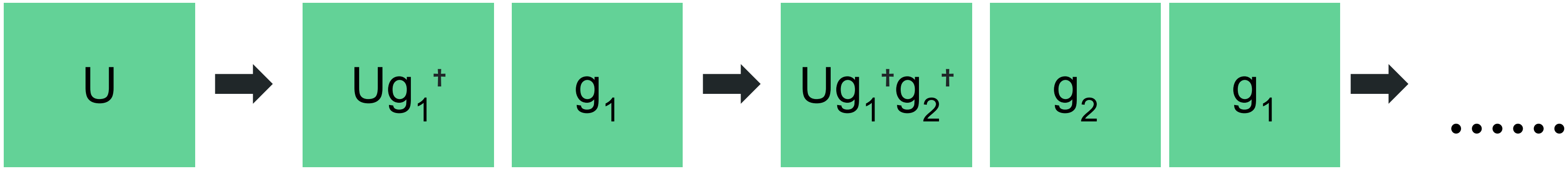
UMCSP is search-to-decision reducible

Main idea: Unitary is **reversible** => we can **uncompute** the gates from U

The reduction (from search to decision)

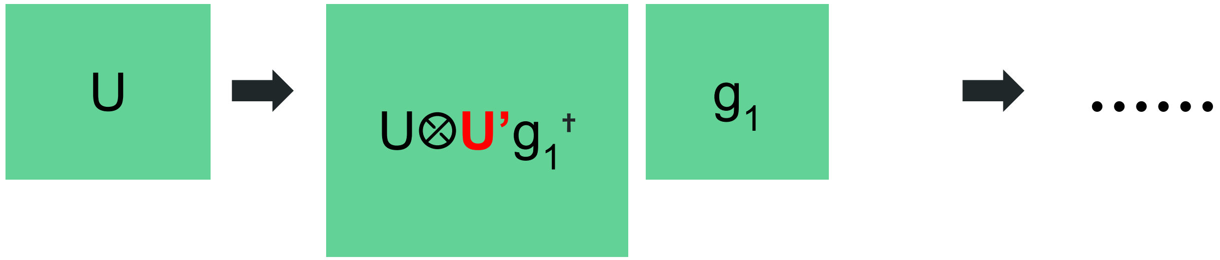
- Goal: given U and an oracle for UMCSP, find the quantum circuit C
- Use UMCSP oracle to find s = CC(U)
- Set i=1
- While i<s
  - For all g in the universal gate set
    - if UMCSP($Ug^\dagger$, **s-i**) = 1, then g is the i-th gate of C. Denote as g_i
- Return $C=g_1g_2...g_s$

SMCSP is similar



Notes on the search-to-decision reductions

- Our results hold when the quantum circuits **use no ancilla qubits**
  - We don't know the full unitary or states of the optimal circuit
  - When there are ancilla qubits, you need to guess both g_i and the **unitary/state on the ancilla qubits**
  - When #ancilla qubits is small, we can use ε-net
  - When #ancilla qubits is large, it is an open problem



Self-reduction for SMCSP

Goal: Computes the quantum circuit complexity of an **(n-1)-qubit state**

⇒ **approximate** the quantum circuit complexity of an **n-qubit state**

$$\epsilon \cdot \max_{i=0,1} CC(|\psi_i\rangle, 2\epsilon) \leq CC(|\psi\rangle, \epsilon) \leq O(1) \cdot (CC(|\psi_0\rangle, \epsilon) + CC(|\psi_1\rangle, \epsilon)) + 3$$

For any n-qubit quantum state, we can write

$$|\psi\rangle = a_0|0\rangle|\psi_0\rangle + a_1|1\rangle|\psi_1\rangle$$

- Estimate a_0 and a_1 to precision $\varepsilon/2$
- Two cases:
  a. a_0 or $a_1 \leq \varepsilon/2$
  b. Both a_0 and $a_1 > \varepsilon/2$

Case a (suppose $a_1 < \varepsilon/2$):

$$|\psi\rangle \approx |0\rangle|\psi_0\rangle \longrightarrow CC(|\psi\rangle, \epsilon) \text{ can be bounded by } CC(|0\rangle|\psi_0\rangle, \epsilon')$$

Self-reduction for SMCSP

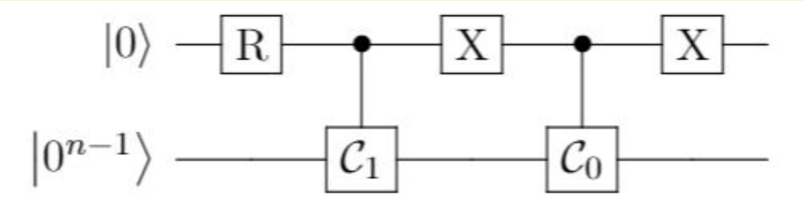
$$\epsilon \cdot \max_{i=0,1} CC(|\psi_i\rangle, 2\epsilon) \leq CC(|\psi\rangle, \epsilon) \leq O(1) \cdot (CC(|\psi_0\rangle, \epsilon) + CC(|\psi_1\rangle, \epsilon)) + 3$$

For any n-qubit quantum state, we can write

$$|\psi\rangle = a_0|0\rangle|\psi_0\rangle + a_1|1\rangle|\psi_1\rangle$$

Case b (both a_0 and $a_1 \geq \varepsilon/2$):

- **Lower bound:**
  - Measuring |ψ> O(1/ε) times gives $|\psi_i\rangle$ for desired i w.h.p.
- **Upper bound:**
  - Let C_i be the optimal circuit for $|\psi_i\rangle$
  - The following circuits approximate |ψ>



Applications of UMCSP and SMCSP

- UMCSP
  - **Gap-MQCSP ≤ UMCSP**
    - This reduction generalize many applications of MQCSP to UMCSP, e.g., hardness magnification, quantum circuit lower bound, and inverting OWF.
- SMCSP
  - Break **quantum pseudorandom states**
  - **Estimate wormhole volume** under AdS/CFT correspondence and C=V conjecture using SMCSP oracle
  - Solve succinct state tomography problem

Conclusion

We study the **hardness** and **applications** of Quantum MCSP

- Boolean / quantum circuit complexity
- Unitary / quantum circuit complexity
- State / quantum circuit complexity

Conclusion

We study the **hardness** and **applications** of Quantum MCSP

- Boolean / quantum circuit complexity
- Unitary / quantum circuit complexity
- State / quantum circuit complexity

Open questions:

- Unconditional hardness of quantum MCSPs?
- Hardness of quantum MCSP <=> quantum cryptographic primitives?
- Relationships between (quantum) MCSPs
- Worst-case to average-case (quantum) reductions? Average-case quantum MCSP?
- Fine-grained complexity and quantum MCSP
- Quantum meta-complexity

Thank you!