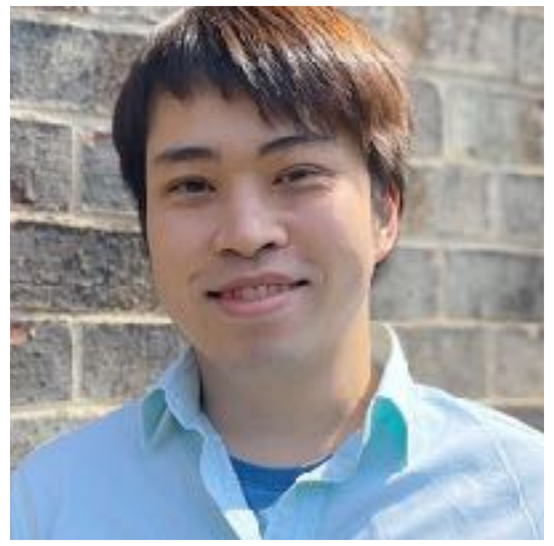
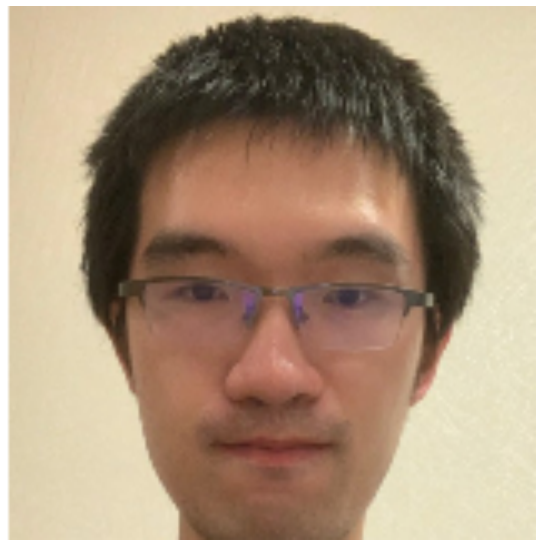
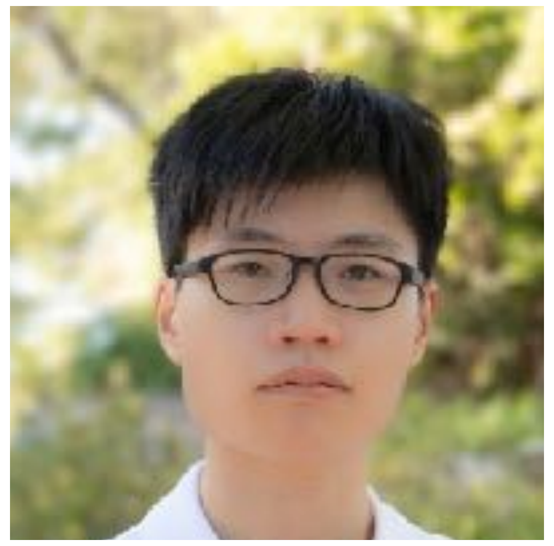
Quantum Meets the Minimum Circuit Size Problem



Nai-Hui Chia — IUB

Chi-Ning Chou — Harvard

Jiayu Zhang — Caltech

Ruizhe Zhang — UT Austin

ITCS 2022

arXiv:2108.03171

Motivation

Motivation

Study quantum computation and complexity

through the lens of meta complexity!

Motivation

Study quantum computation and complexity

through the lens of meta complexity!

The complexity of complexity!

Meta Complexity

Meta Complexity

In the classical setting

Meta Complexity

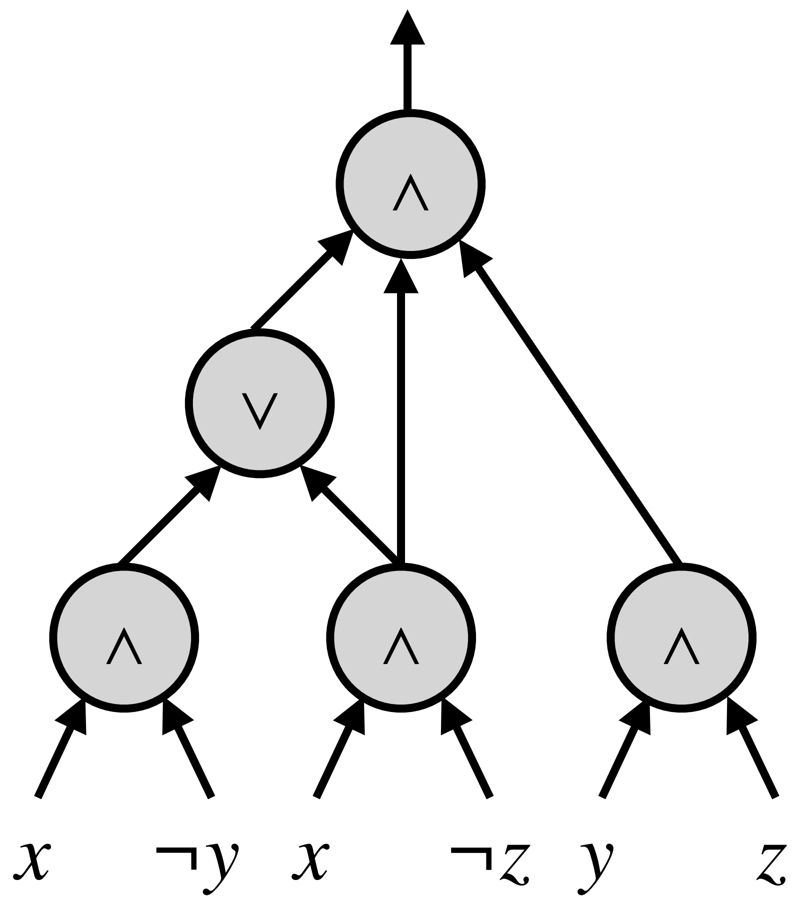
Meta Complexity

Study the complexity of computational problems about complexity.

Meta Complexity

Study the complexity of computational problems about complexity.

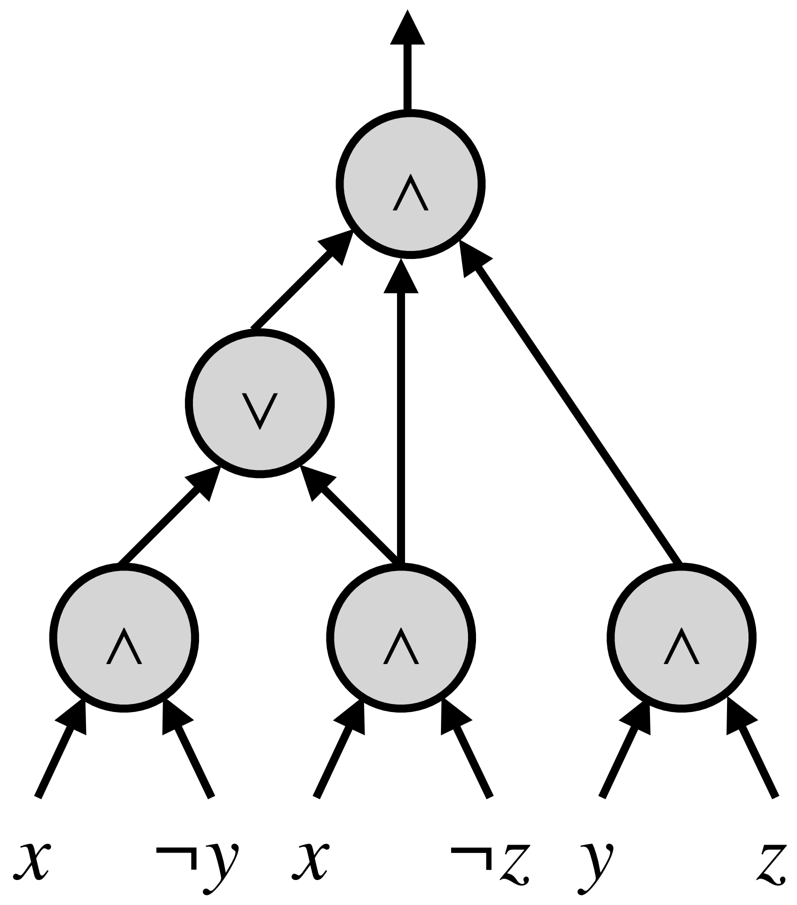
Complexity	Meta Complexity Problem
Circuit Complexity	Minimum Circuit Size Problem (MCSP)

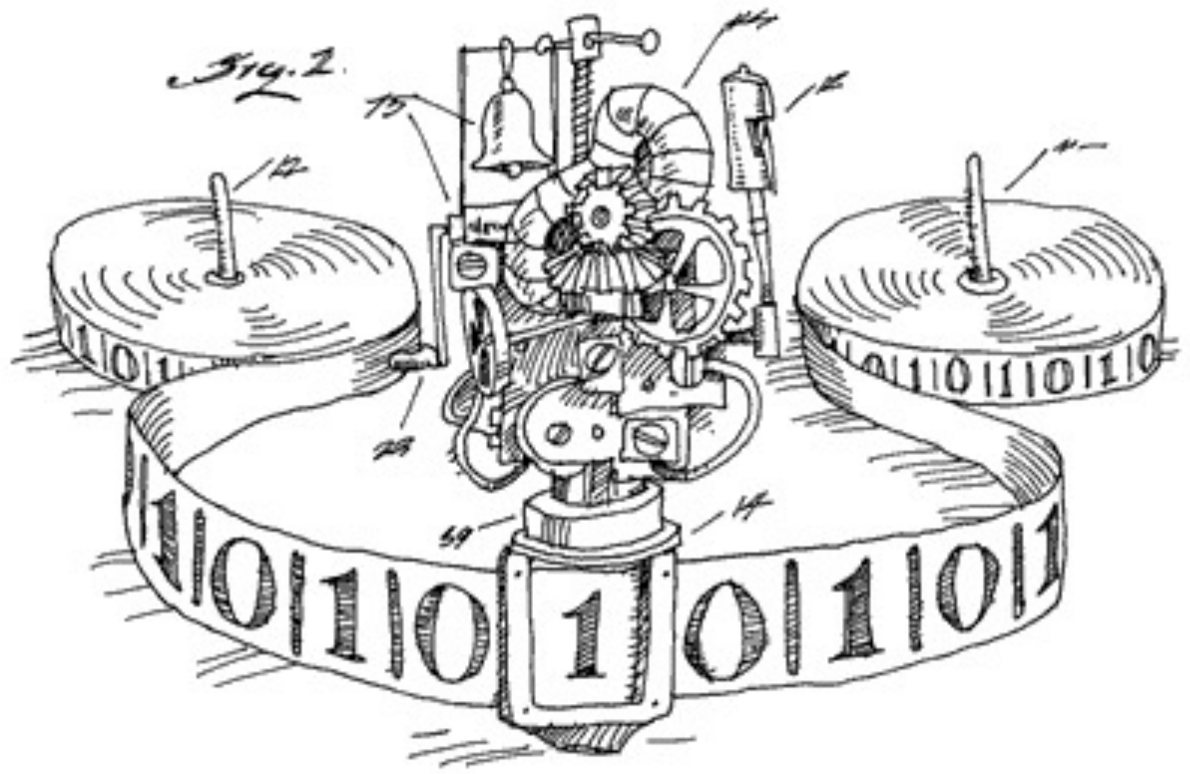


Meta Complexity

Study the complexity of computational problems about complexity.

Complexity	Meta Complexity Problem
Circuit Complexity	Minimum Circuit Size Problem (MCSP)
Kolmogorov Complexity	Minimum Kolmogorov Time-Bounded Complexity Problem (MKTP)

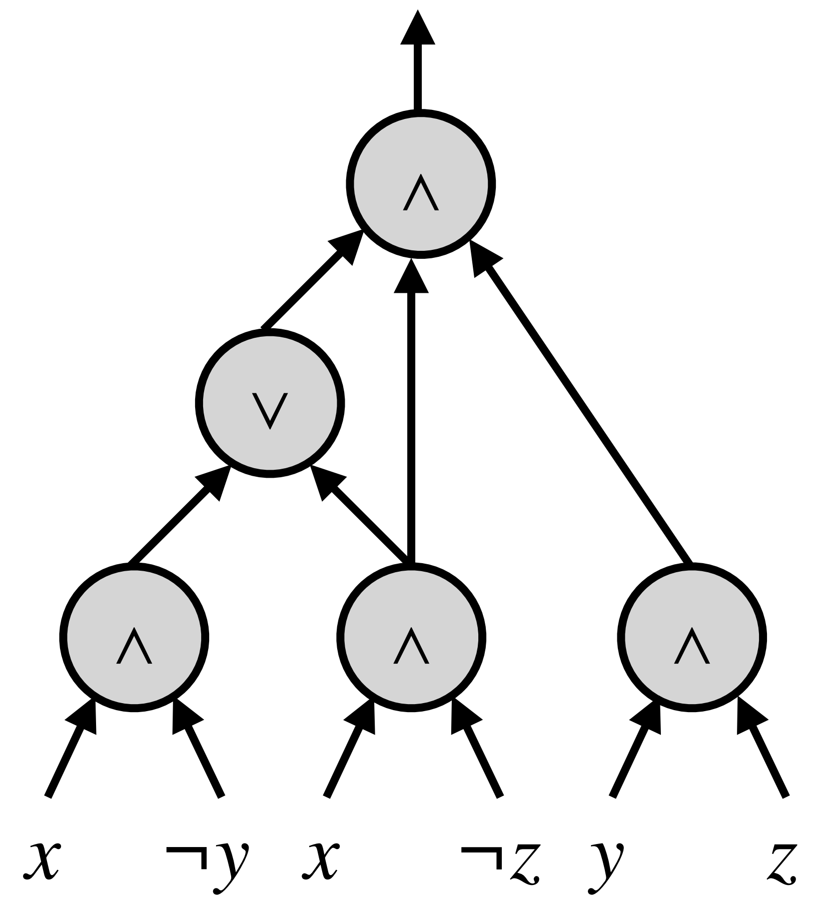


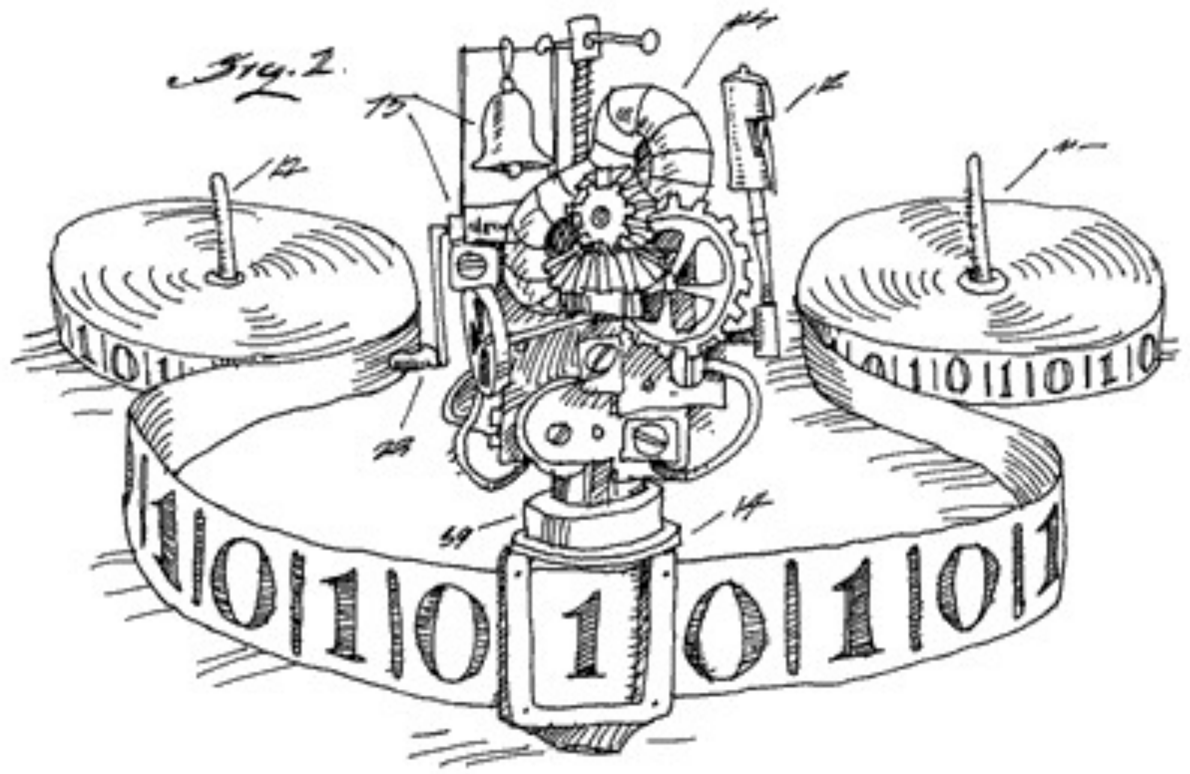


Meta Complexity

Study the complexity of computational problems about complexity.

Complexity	Meta Complexity Problem
Circuit Complexity	Minimum Circuit Size Problem (MCSP)
Kolmogorov Complexity	Minimum Kolmogorov Time-Bounded Complexity Problem (MKTP)





Minimum Circuit Size Problem (MCSP)

Minimum Circuit Size Problem (MCSP)

- **Input:** the truth table of an n-bit function f and a size parameter s.

Minimum Circuit Size Problem (MCSP)

- **Input:** the truth table of an n-bit function f and a size parameter s.
- **Output:** "Yes" if there's a circuit of size at most s for f; otherwise "No".

Minimum Circuit Size Problem (MCSP)

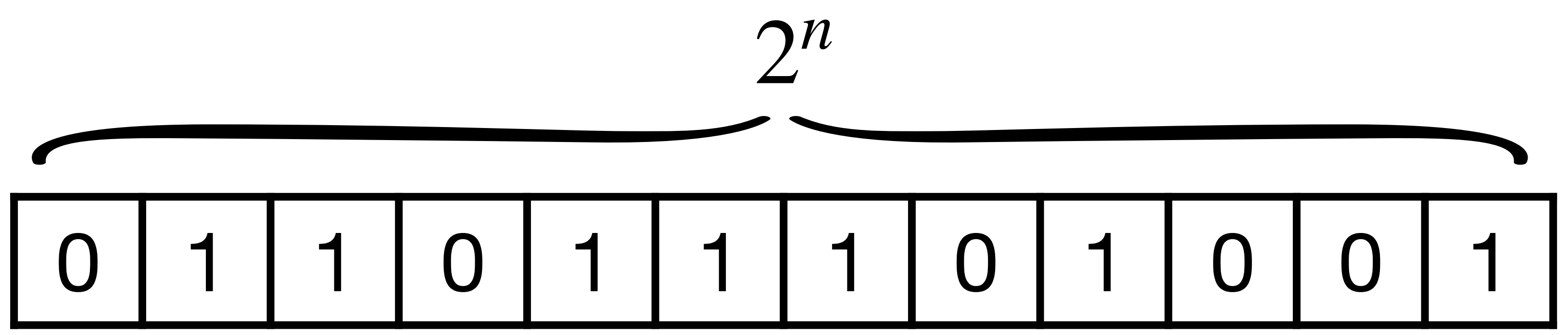
- **Input:** the truth table of an n-bit function f and a size parameter s.
- **Output:** "Yes" if there's a circuit of size at most s for f; otherwise "No".
- Note that the input length is $O(2^n)$.

Minimum Circuit Size Problem (MCSP)

- **Input:** the truth table of an n-bit function f and a size parameter s.
- **Output:** "Yes" if there's a circuit of size at most s for f; otherwise "No".
- Note that the input length is $O(2^n)$.
- MCSP $\in$ NP.

Minimum Circuit Size Problem (MCSP)

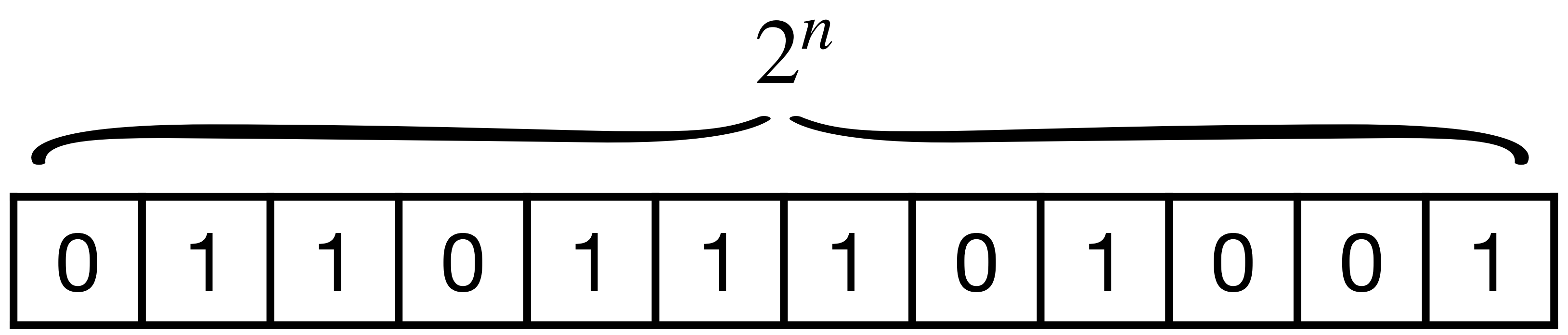
- **Input:** the truth table of an n-bit function f and a size parameter s.
- **Output:** "Yes" if there's a circuit of size at most s for f; otherwise "No".
- Note that the input length is $O(2^n)$.
- MCSP ∈ NP.



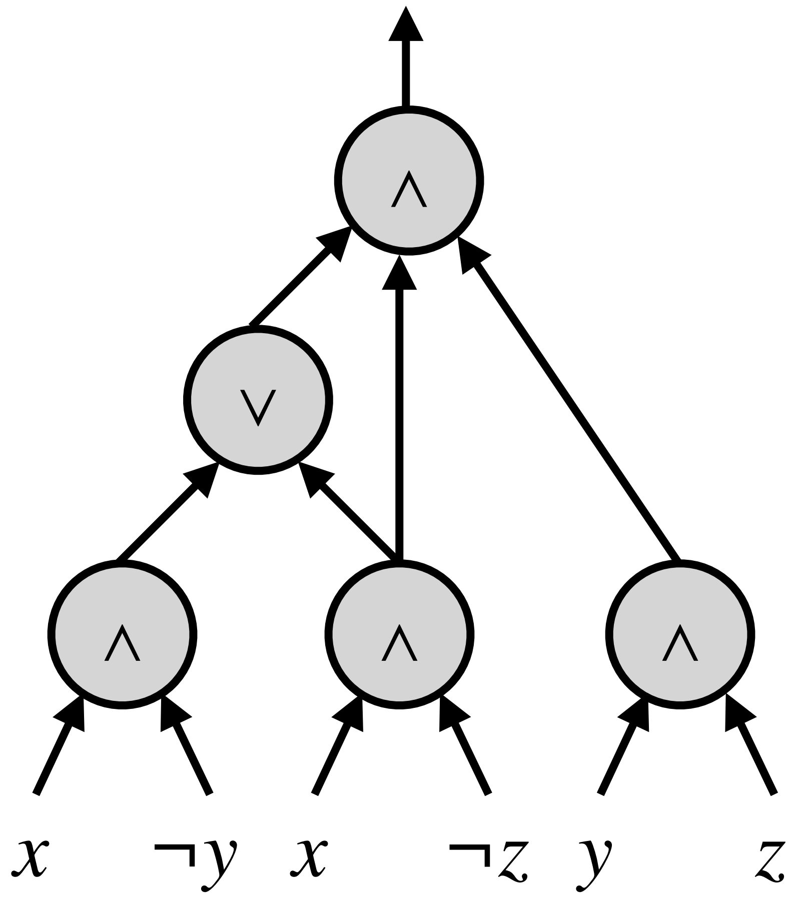
Input: the truth table of f

Minimum Circuit Size Problem (MCSP)

- **Input:** the truth table of an n-bit function f and a size parameter s.
- **Output:** "Yes" if there's a circuit of size at most s for f; otherwise "No".
- Note that the input length is $O(2^n)$.
- MCSP $\in$ NP.



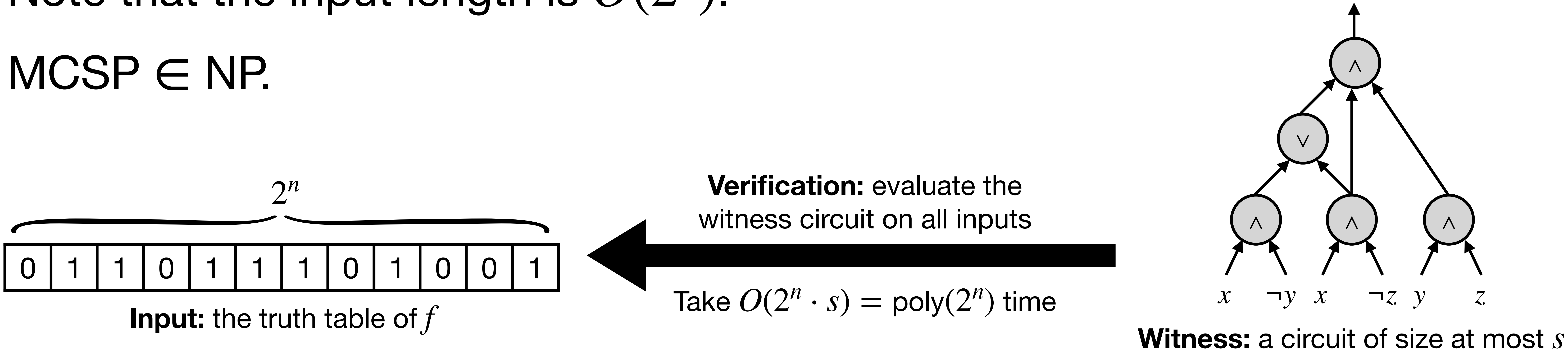
Input: the truth table of f



Witness: a circuit of size at most s

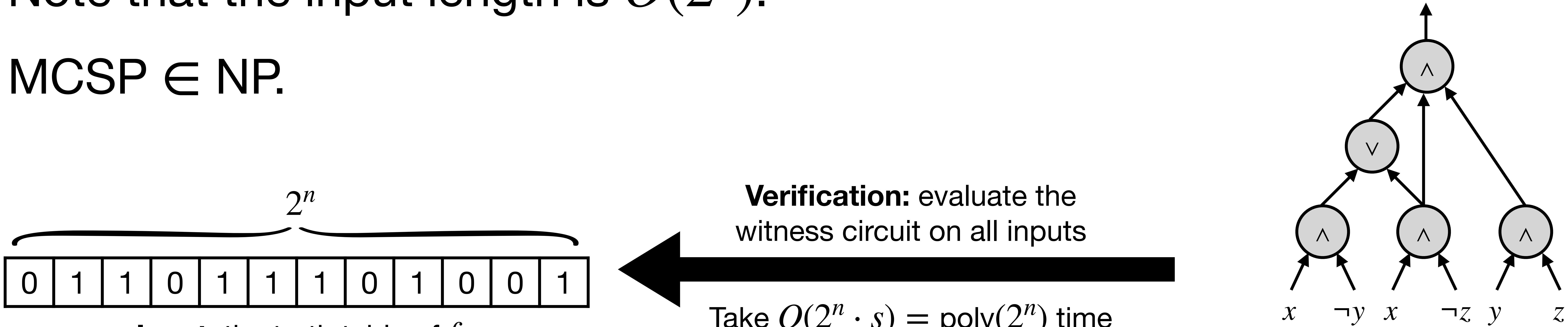
Minimum Circuit Size Problem (MCSP)

- **Input:** the truth table of an n-bit function f and a size parameter s.
- **Output:** “Yes” if there’s a circuit of size at most s for f; otherwise “No”.
- Note that the input length is $O(2^n)$.
- MCSP $\in$ NP.



Minimum Circuit Size Problem (MCSP)

- **Input:** the truth table of an n-bit function f and a size parameter s.
- **Output:** “Yes” if there’s a circuit of size at most s for f; otherwise “No”.
- Note that the input length is $O(2^n)$.
- MCSP ∈ NP.



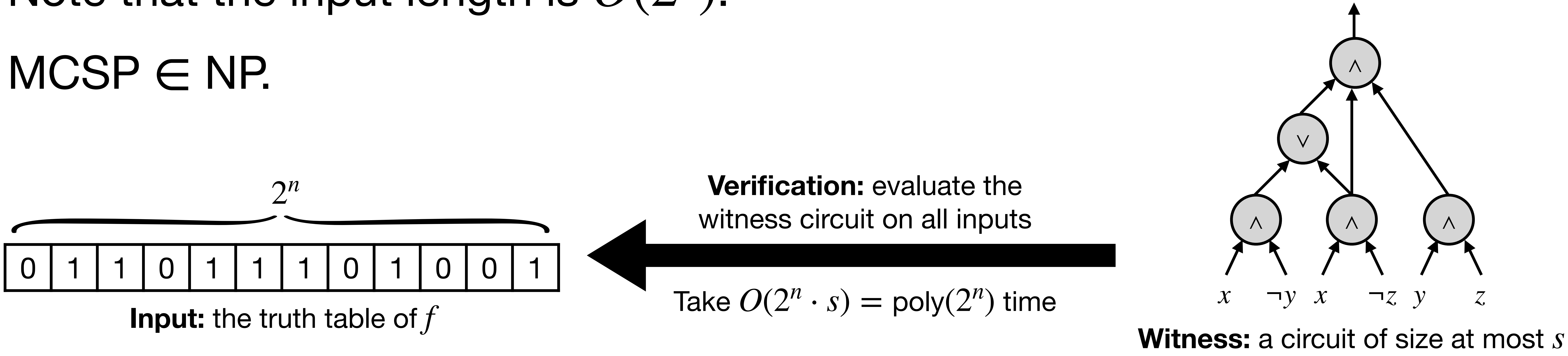
Input: the truth table of f

Witness: a circuit of size at most s

- But proving MCSP ∈ P or MCSP being NP-hard require new techniques!

Minimum Circuit Size Problem (MCSP)

- **Input:** the truth table of an n-bit function f and a size parameter s.
- **Output:** "Yes" if there's a circuit of size at most s for f; otherwise "No".
- Note that the input length is $O(2^n)$.
- MCSP $\in$ NP.



- But proving MCSP $\in$ P or MCSP being NP-hard require new techniques!
- Perebor conjecture: brute-force search is the best algorithm!?

Why MCSP?

Why MCSP?

Circuit Complexity

- [Razborov-Rudich'00]: MCSP $\in$ P $\Rightarrow$ natural property against P/poly$\Rightarrow$ no PRG.
- [Kabanets-Cai'00]: MCSP $\in$ P $\Rightarrow$ new circuit lower bound.
- [Arunachalam et al.'20]: MCSP $\in$ BQP $\Rightarrow$ new circuit lower bound.

Why MCSP?

Circuit Complexity

- [Razborov-Rudich'00]: MCSP $\in$ P $\Rightarrow$ natural property against P/poly$\Rightarrow$ no PRG.
- [Kabanets-Cai'00]: MCSP $\in$ P $\Rightarrow$ new circuit lower bound.
- [Arunachalam et al.'20]: MCSP $\in$ BQP $\Rightarrow$ new circuit lower bound.

Learning Theory

- [Carmosino et al.'16]: MCSP $\in$ P $\Rightarrow$ efficient PAC learning for P/poly.

Why MCSP?

Circuit Complexity

- [Razborov-Rudich'00]: MCSP $\in$ P $\Rightarrow$ natural property against P/poly$\Rightarrow$ no PRG.
- [Kabanets-Cai'00]: MCSP $\in$ P $\Rightarrow$ new circuit lower bound.
- [Arunachalam et al.'20]: MCSP $\in$ BQP $\Rightarrow$ new circuit lower bound.

Learning Theory

- [Carmosino et al.'16]: MCSP $\in$ P $\Rightarrow$ efficient PAC learning for P/poly.

Average-Case Complexity

- [Hirahara'18]: an approximate version of MCSP being NP-hard $\Rightarrow$ average-case and worst-case hardness in NP are the same, i.e., no Heuristica.

Why MCSP?

Circuit Complexity

- [Razborov-Rudich'00]: MCSP $\in$ P $\Rightarrow$ natural property against P/poly$\Rightarrow$ no PRG.
- [Kabanets-Cai'00]: MCSP $\in$ P $\Rightarrow$ new circuit lower bound.
- [Arunachalam et al.'20]: MCSP $\in$ BQP $\Rightarrow$ new circuit lower bound.

Learning Theory

- [Carmosino et al.'16]: MCSP $\in$ P $\Rightarrow$ efficient PAC learning for P/poly.

Average-Case Complexity

- [Hirahara'18]: an approximate version of MCSP being NP-hard $\Rightarrow$ average-case and worst-case hardness in NP are the same, i.e., no Heuristica.

Cryptography

- [Kabanets-Cai'00]: MCSP $\in$ BPP $\Rightarrow$ no one-way function.
- [Allender-Das'14]: SZK $\leq$ MCSP.
- [Impagliazzo et al.'18]: iO $\Rightarrow$ SAT $\leq_R$ MCSP.

Why MCSP?

Circuit Complexity

- [Razborov-Rudich'00]: MCSP $\in$ P $\Rightarrow$ natural property against P/poly$\Rightarrow$ no PRG.
- [Kabanets-Cai'00]: MCSP $\in$ P $\Rightarrow$ new circuit lower bound.
- [Arunachalam et al.'20]: MCSP $\in$ BQP $\Rightarrow$ new circuit lower bound.

Learning Theory

- [Carmosino et al.'16]: MCSP $\in$ P $\Rightarrow$ efficient PAC learning for P/poly.

Average-Case Complexity

- [Hirahara'18]: an approximate version of MCSP being NP-hard $\Rightarrow$ average-case and worst-case hardness in NP are the same, i.e., no Heuristica.

Cryptography

- [Kabanets-Cai'00]: MCSP $\in$ BPP $\Rightarrow$ no one-way function.
- [Allender-Das'14]: SZK $\leq$ MCSP.
- [Impagliazzo et al.'18]: iO $\Rightarrow$ SAT $\leq_R$ MCSP.

MCSP has connections to many sub-fields in TCS!

Quantum Meets MCSP

Roadmap

Roadmap

finition & Basic
Complexity
Results

Roadmap

A Bird-Eye View on Our Results

finition & Basic Complexity Results

Roadmap

A Bird-Eye View
on Our Results

Special
perties in the
antum Setting

finition & Basic
Complexity
Results

Roadmap

Summary &
Future Directi

Special
perties in the
antum Setting

A Bird-Eye View
on Our Results

finition & Basic
Complexity
Results

Definitions & Basic Complexity Results

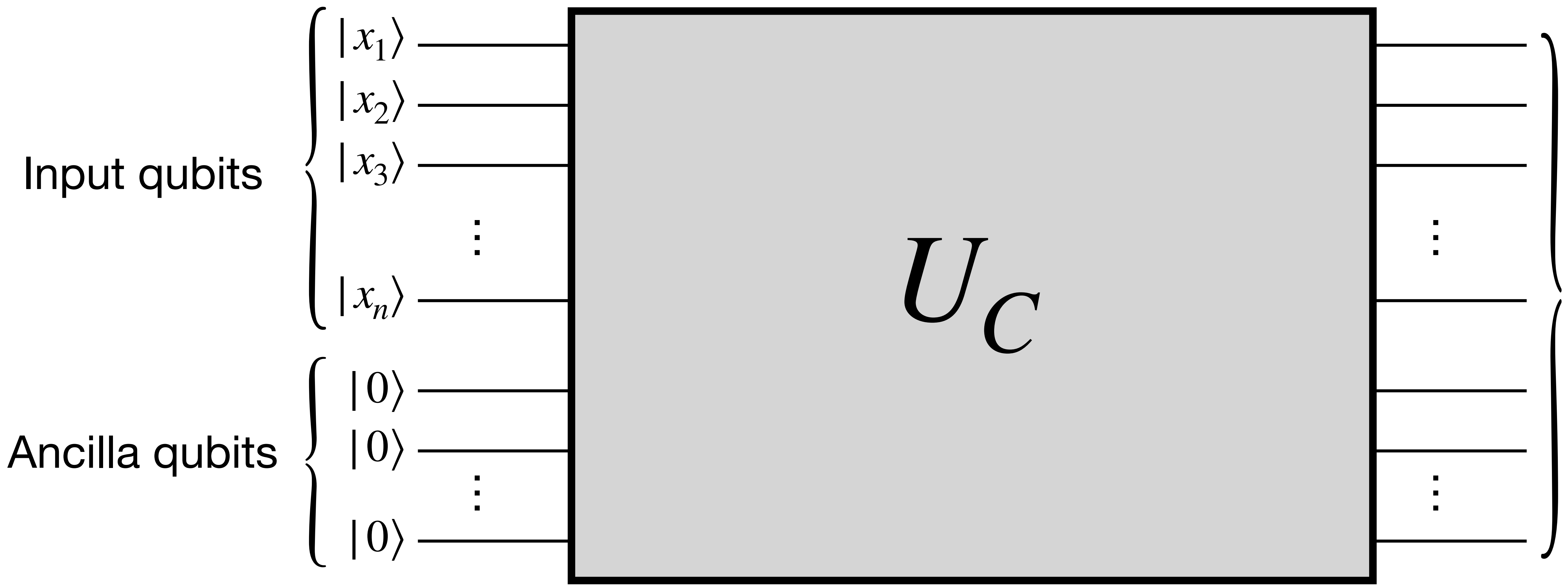
Computational Problems in the Quantum World are Different!

Computational Problems in the Quantum World are Different!

- A quantum circuit corresponds to a unitary transformation!

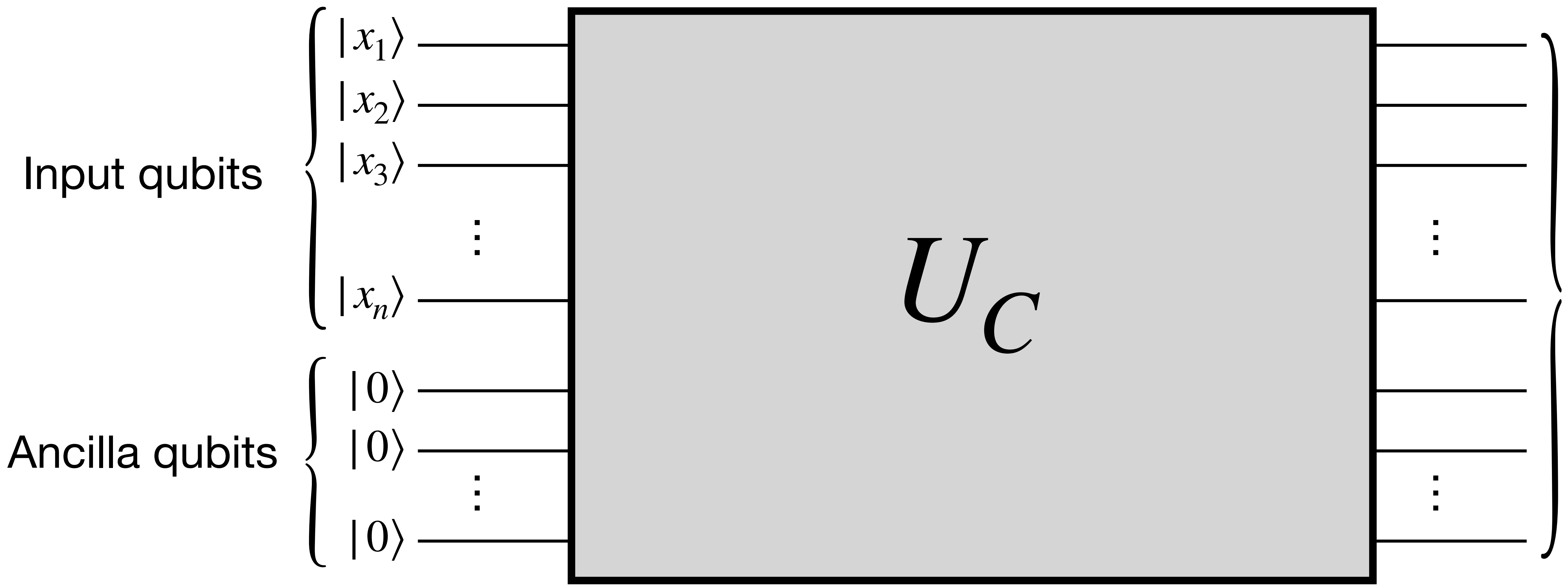
Computational Problems in the Quantum World are Different!

- A quantum circuit corresponds to a unitary transformation!



Computational Problems in the Quantum World are Different!

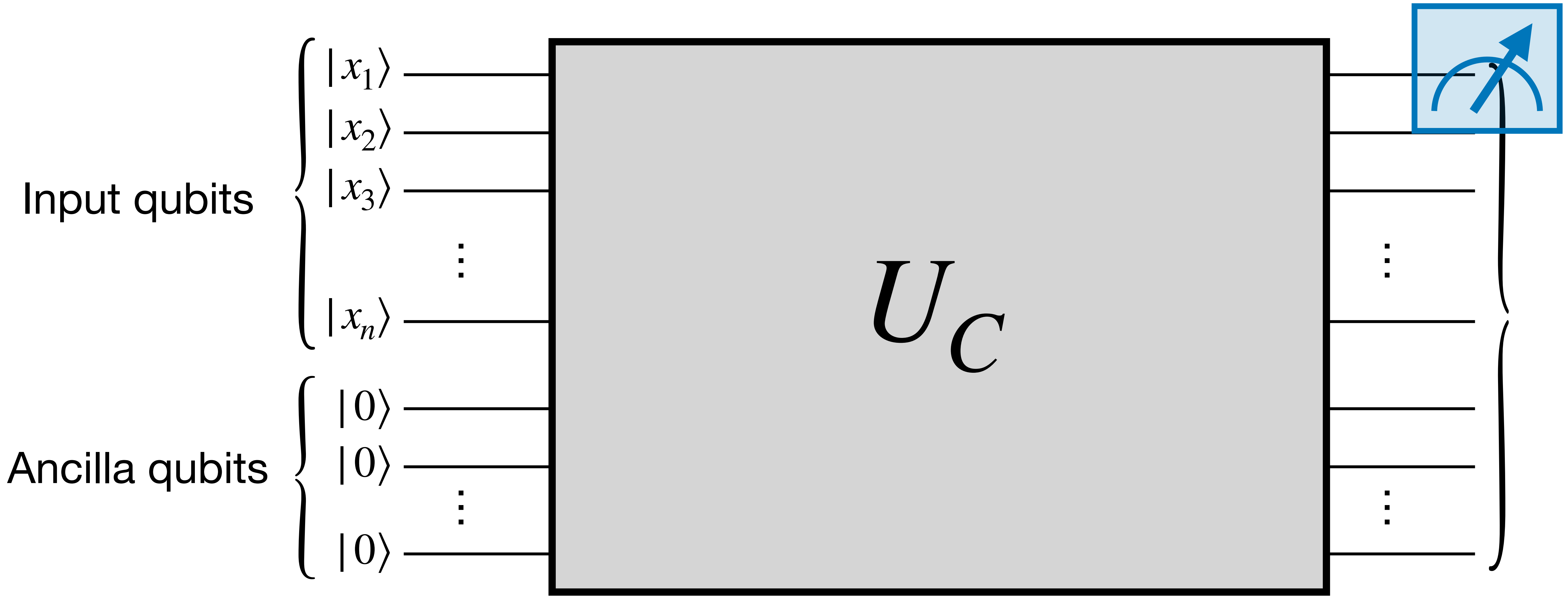
- A quantum circuit corresponds to a unitary transformation!



- Three natural types of computation:

Computational Problems in the Quantum World are Different!

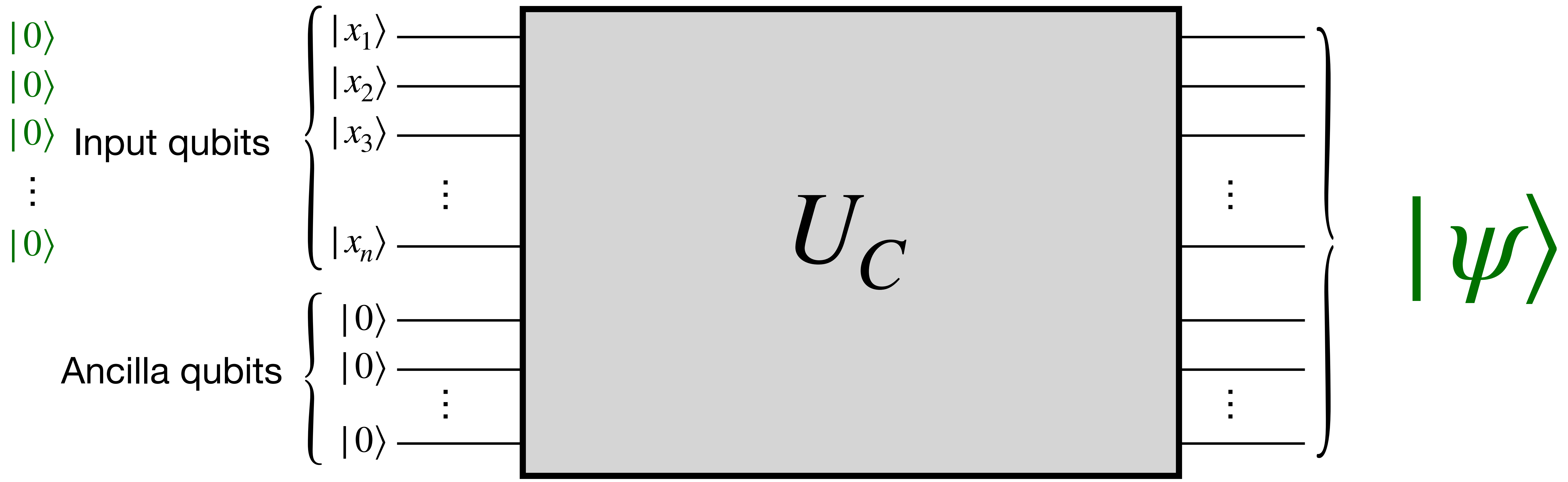
- A quantum circuit corresponds to a unitary transformation!



- Three natural types of computation:
  - Boolean function.

Computational Problems in the Quantum World are Different!

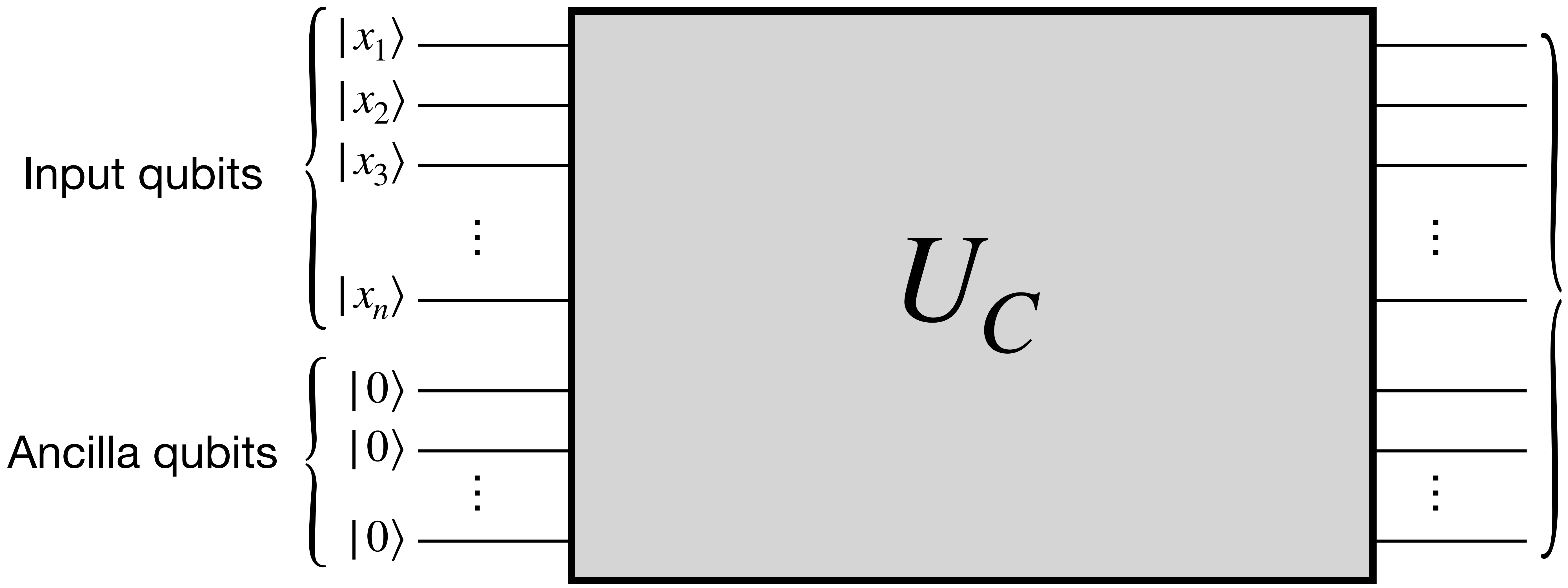
- A quantum circuit corresponds to a unitary transformation!



- Three natural types of computation:
  - ✦ Boolean function.
  - ✦ Quantum state.

Computational Problems in the Quantum World are Different!

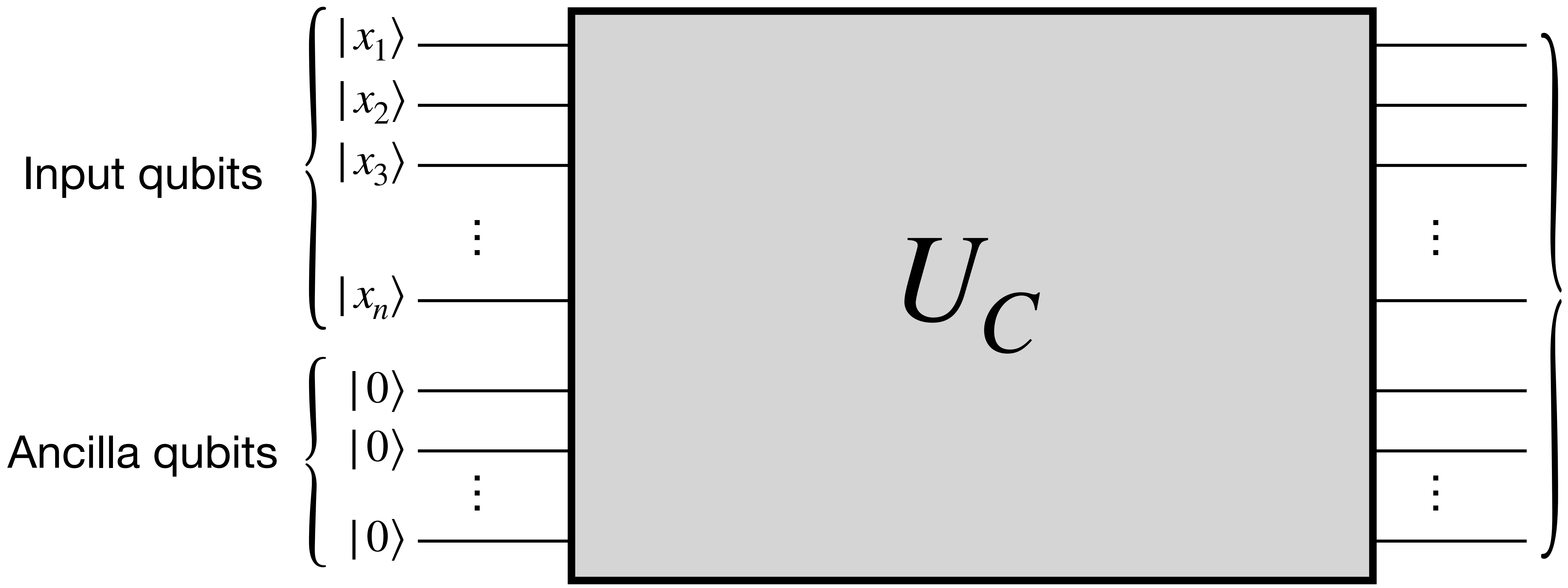
- A quantum circuit corresponds to a unitary transformation!



- Three natural types of computation:
  - Boolean function.
  - Quantum state.
  - Unitary transformation.

Computational Problems in the Quantum World are Different!

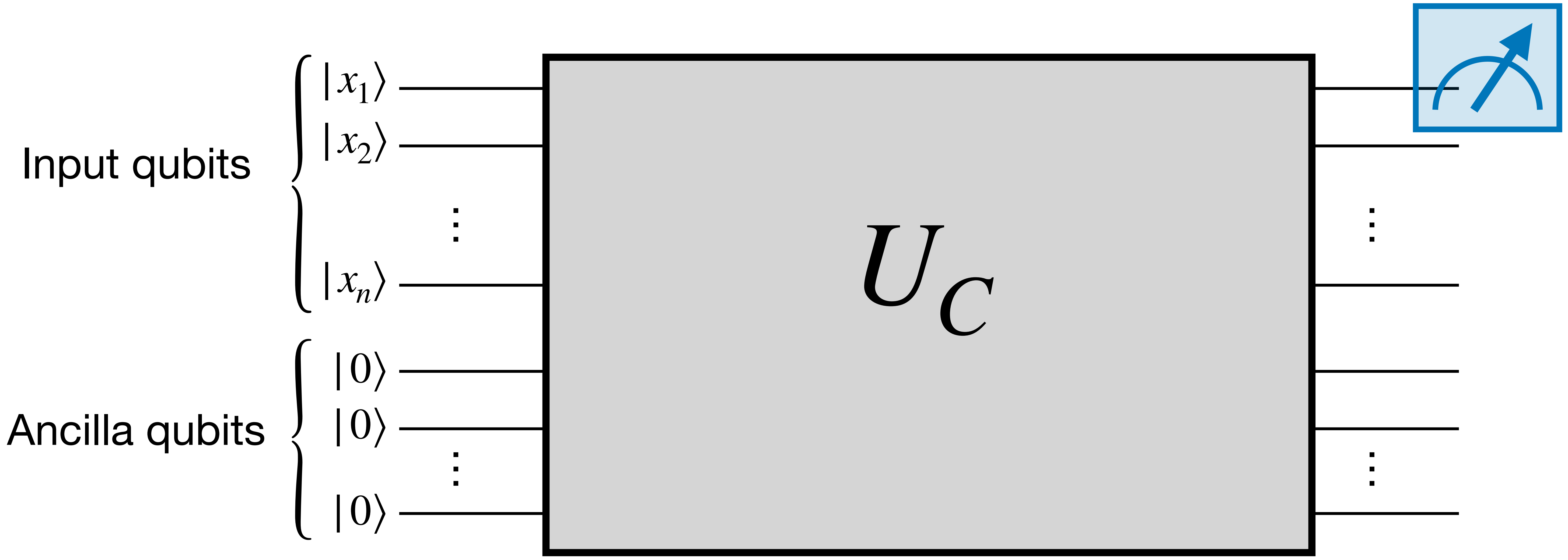
- A quantum circuit corresponds to a unitary transformation!



- Three natural types of computation:
  - Boolean function.
  - Quantum state.
  - Unitary transformation.

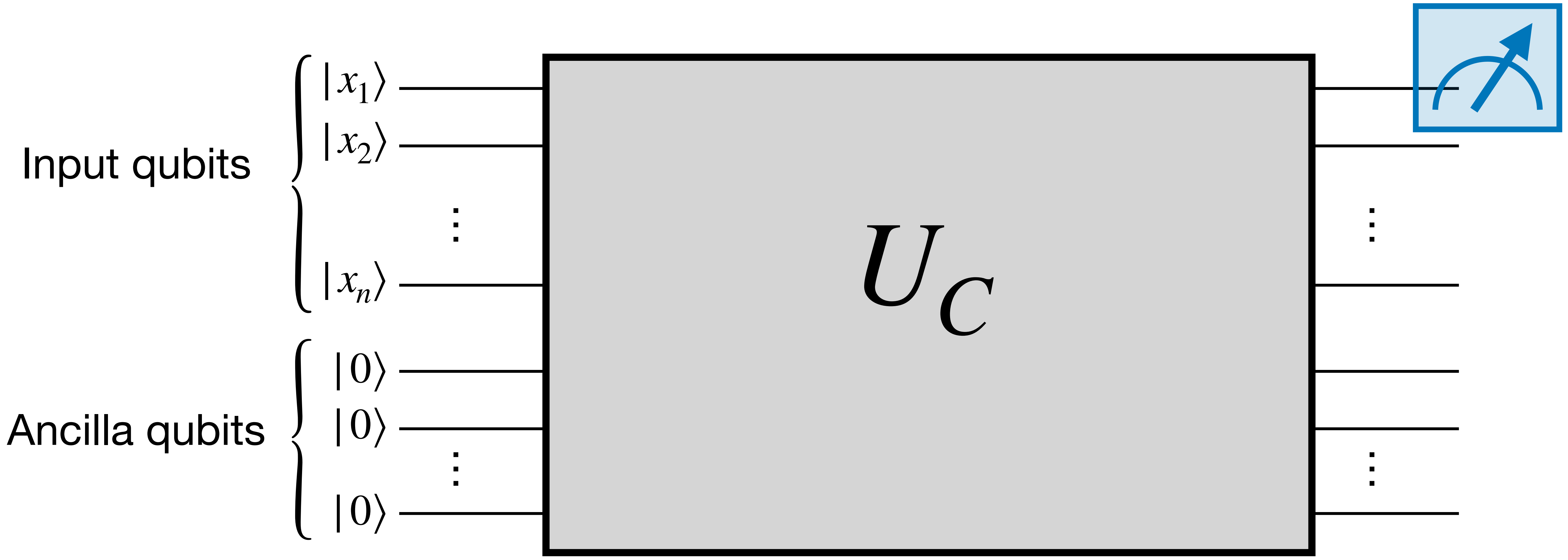
To properly define the corresponding MCSP, one needs to handle "error probability" and "distance" between quantum objects.

Minimum Quantum Circuit Size Problem (MQCSP)



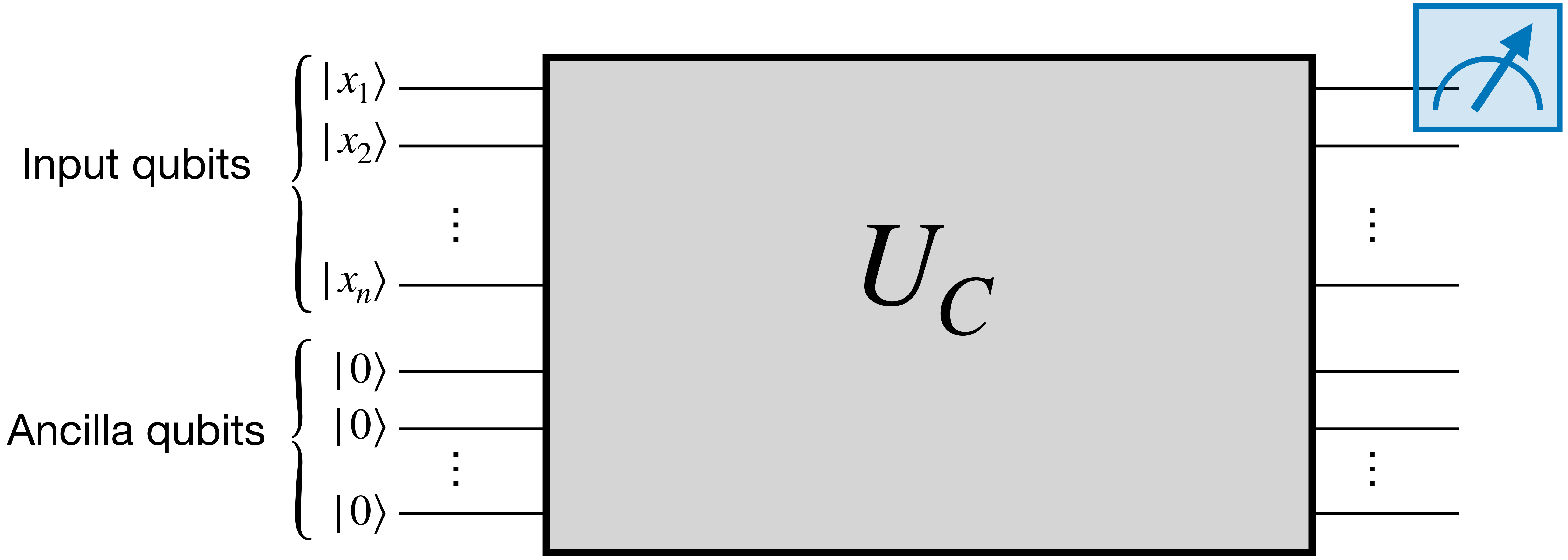
Minimum Quantum Circuit Size Problem (MQCSP)

- **Parameters:**



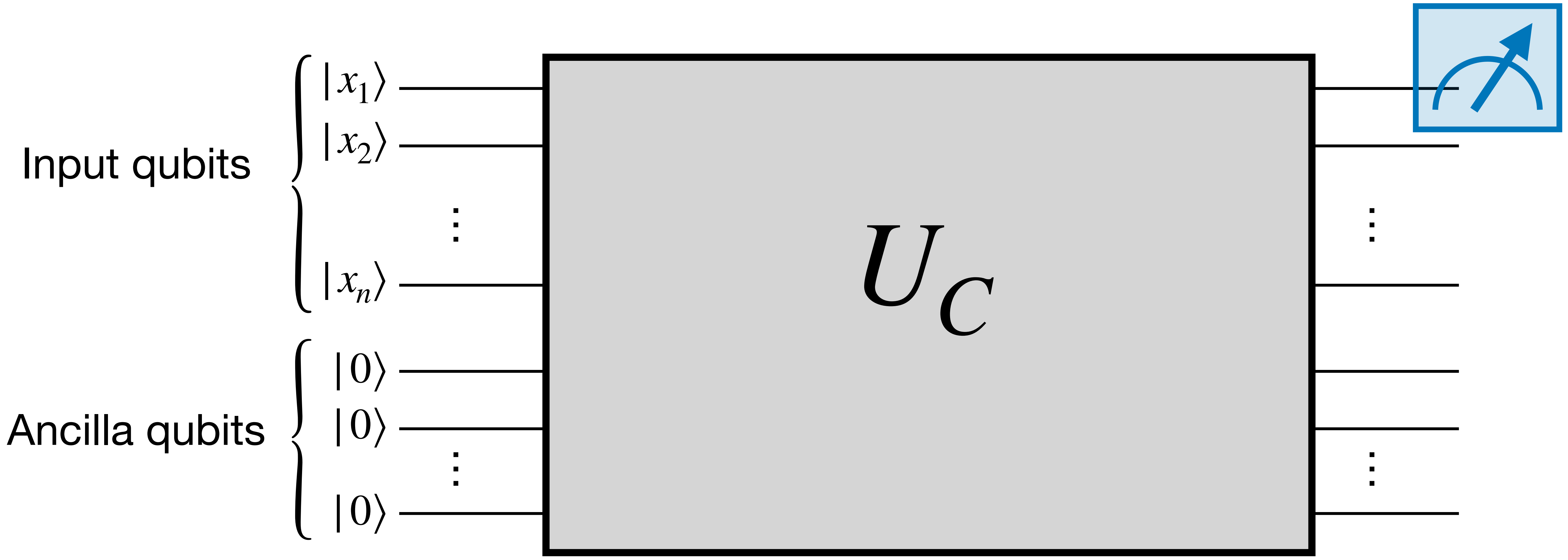
Minimum Quantum Circuit Size Problem (MQCSP)

- **Parameters:**
  - Number of ancilla qubits: t



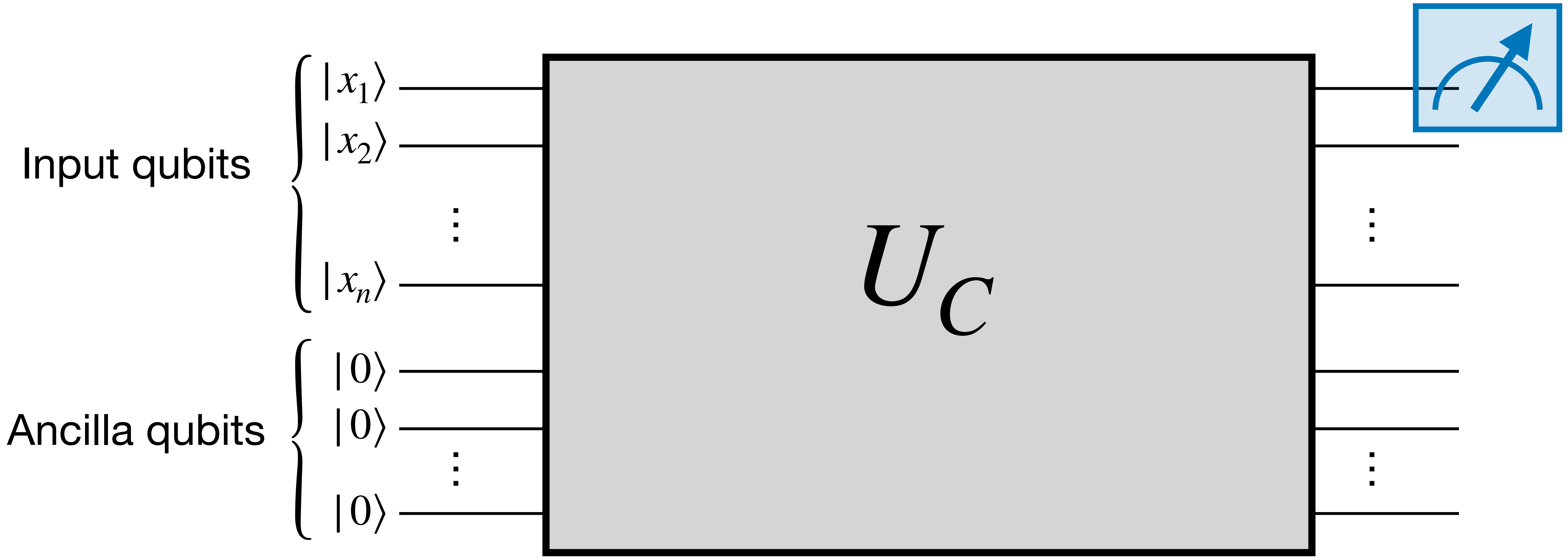
Minimum Quantum Circuit Size Problem (MQCSP)

- **Parameters:**
  - Number of ancilla qubits: t
  - Completeness: α



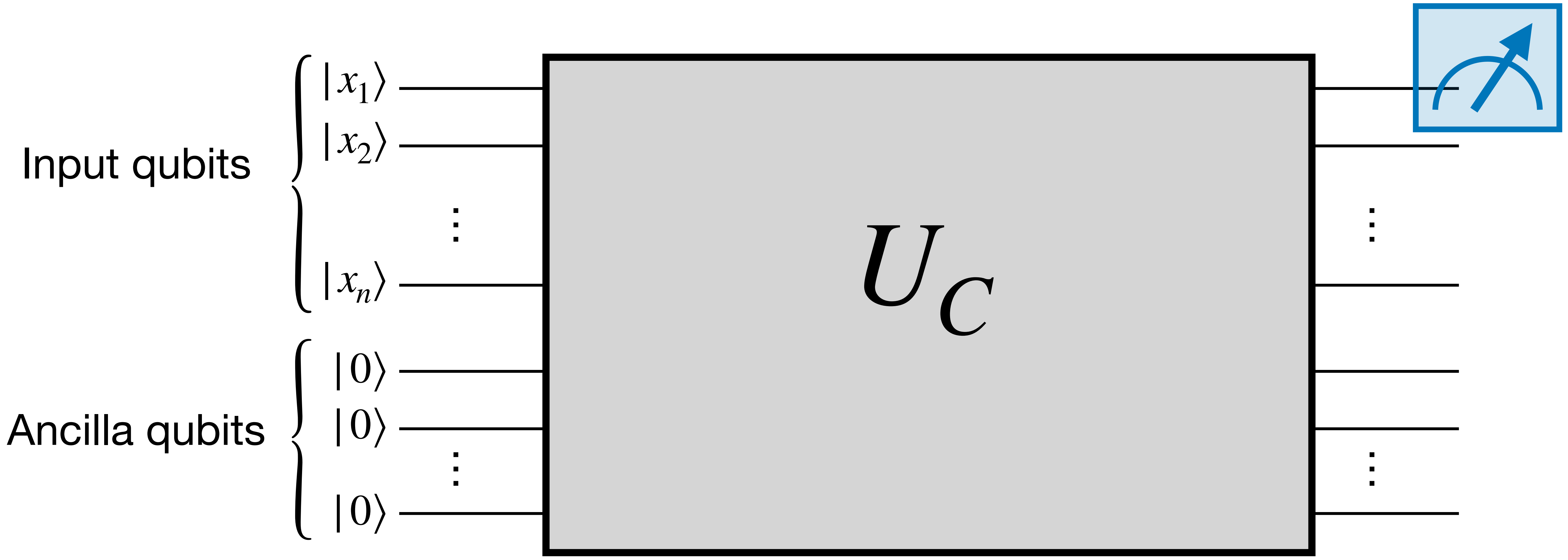
Minimum Quantum Circuit Size Problem (MQCSP)

- **Parameters:**
  - Number of ancilla qubits: t
  - Completeness: α
  - Soundness: β



Minimum Quantum Circuit Size Problem (MQCSP)

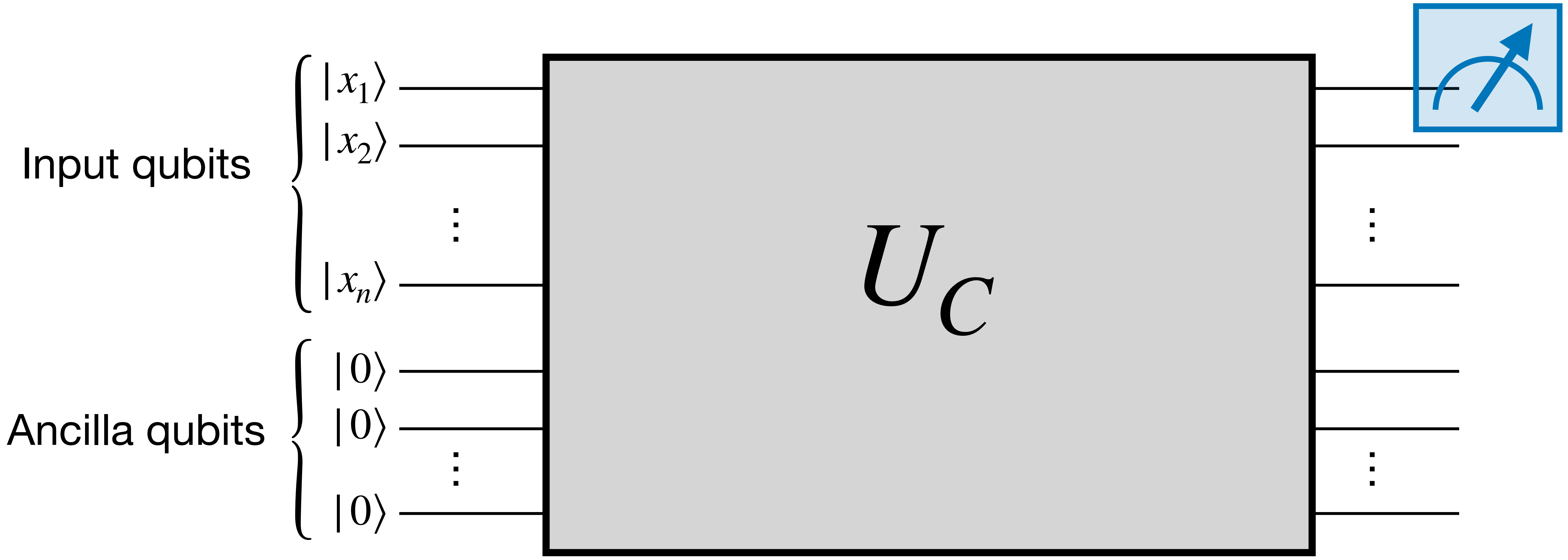
- **Parameters:**
  - ✦ Number of ancilla qubits: t
  - ✦ Completeness: α
  - ✦ Soundness: β



- **Input:** The truth table of an n-bit boolean function f and a size parameter s.

Minimum Quantum Circuit Size Problem (MQCSP)

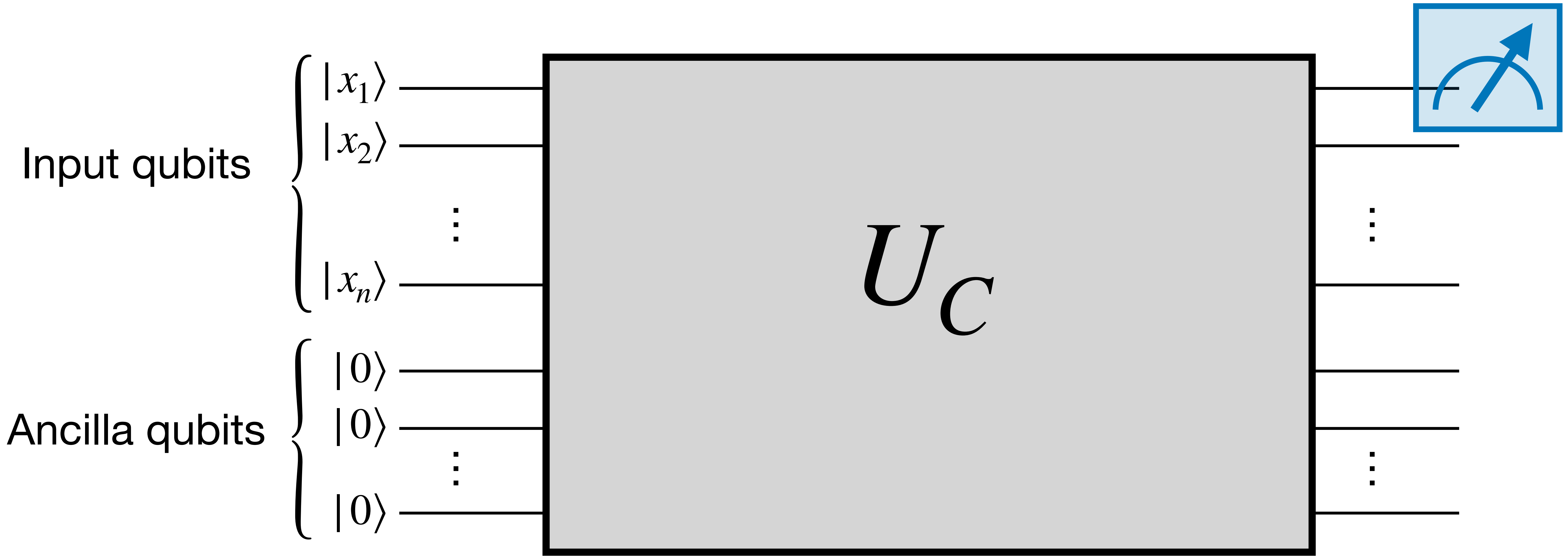
- **Parameters:**
  - Number of ancilla qubits: t
  - Completeness: α
  - Soundness: β



- **Input:** The truth table of an n-bit boolean function f and a size parameter s.
- **Goal:** Distinguish the following two cases.

Minimum Quantum Circuit Size Problem (MQCSP)

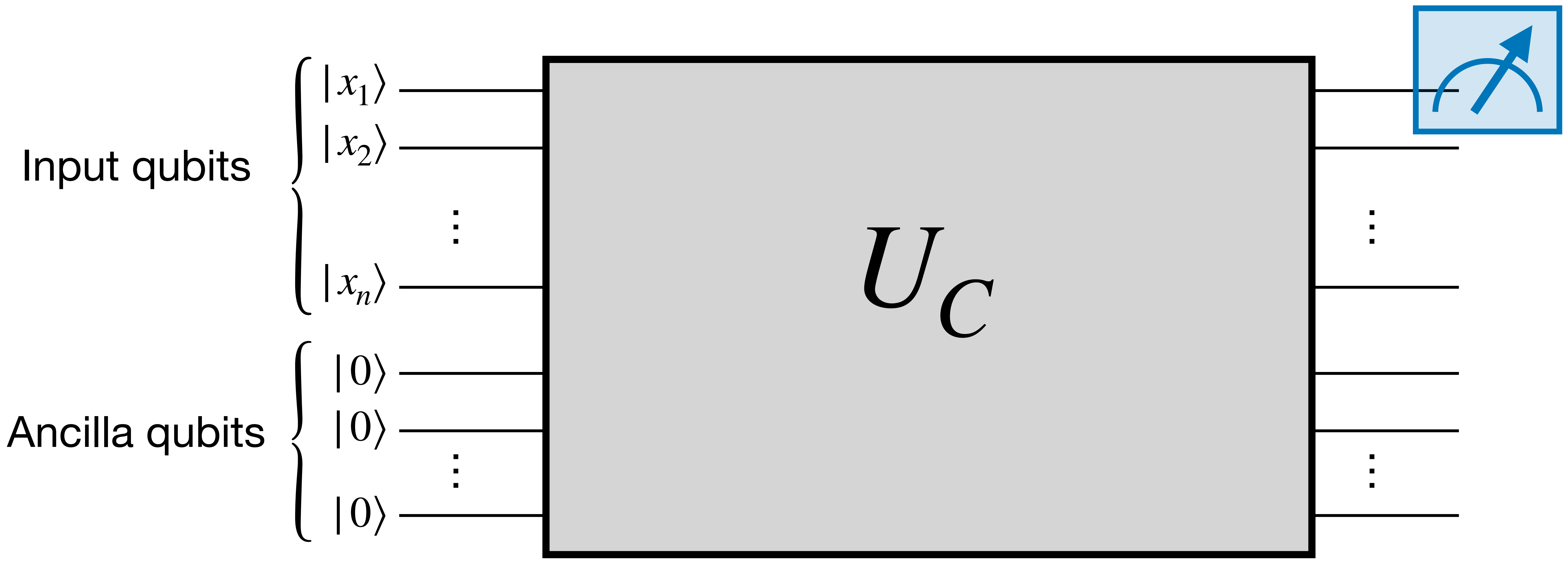
- **Parameters:**
  - Number of ancilla qubits: t
  - Completeness: α
  - Soundness: β



- **Input:** The truth table of an n-bit boolean function f and a size parameter s.
- **Goal:** Distinguish the following two cases.
  - Yes: $\exists$ circuit $\mathscr{C}$ of size $\leq s$, s.t. $\forall x \in \{0,1\}^n$, $\|\langle(f(x)| \otimes I_{n+t-1})\mathscr{C}|x,0^t\rangle\| \geq \alpha$.

Minimum Quantum Circuit Size Problem (MQCSP)

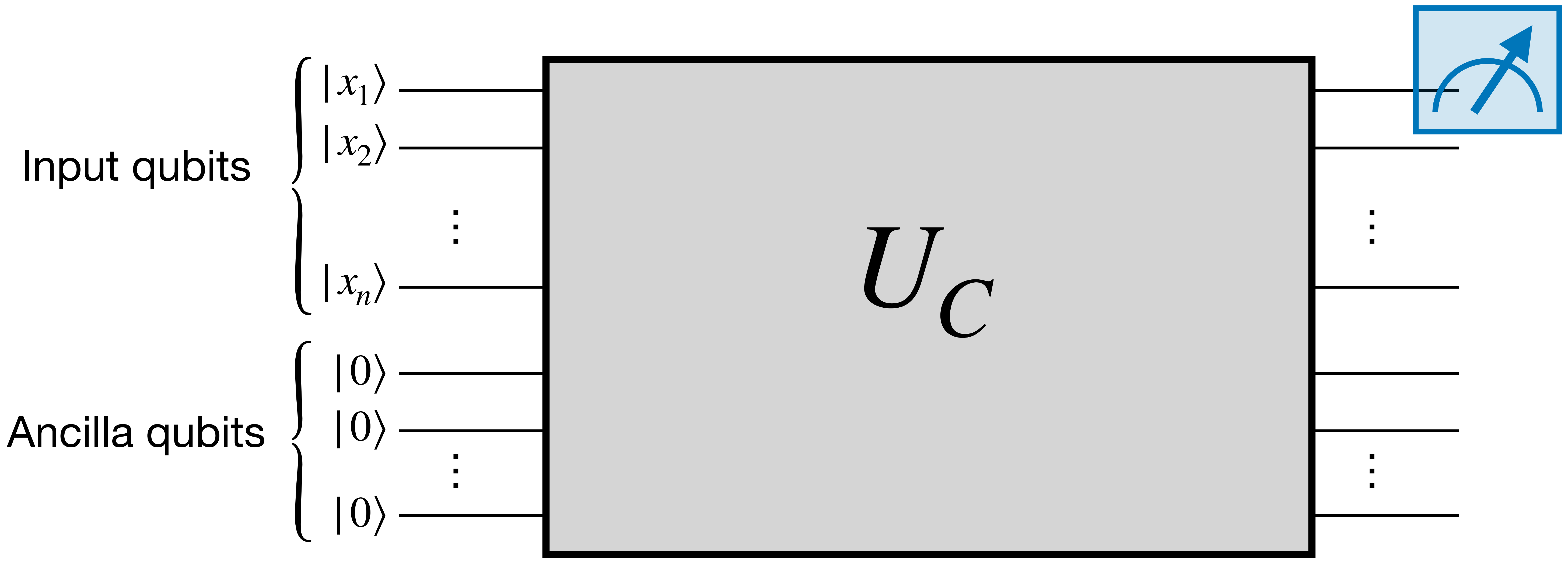
- **Parameters:**
  - Number of ancilla qubits: t
  - Completeness: α
  - Soundness: β



- **Input:** The truth table of an n-bit boolean function f and a size parameter s.
- **Goal:** Distinguish the following two cases.
  - Yes: $\exists$ circuit $\mathscr{C}$ of size $\leq s$, s.t. $\forall x \in \{0,1\}^n$, $\|\langle (f(x) | \otimes I_{n+t-1}) \mathscr{C} | x, 0^t \rangle \| \geq \alpha$.
  - No: $\forall$ circuit $\mathscr{C}$ of size $\leq s$, $\exists x \in \{0,1\}^n$ s.t. $\|\langle (f(x) | \otimes I_{n+t-1}) \mathscr{C} | x, 0^t \rangle \| \leq \beta$.

Minimum Quantum Circuit Size Problem (MQCSP)

- **Parameters:**
  - Number of ancilla qubits: t
  - Completeness: α
  - Soundness: β



- **Input:** The truth table of an n-bit boolean function f and a size parameter s.
- **Goal:** Distinguish the following two cases.
  - Yes: $\exists$ circuit $\mathscr{C}$ of size $\leq s$, s.t. $\forall x \in \{0,1\}^n$, $\| \langle (f(x) | \otimes I_{n+t-1}) \mathscr{C} | x, 0^t \rangle \| \geq \alpha$.
  - No: $\forall$ circuit $\mathscr{C}$ of size $\leq s$, $\exists x \in \{0,1\}^n$ s.t. $\| \langle (f(x) | \otimes I_{n+t-1}) \mathscr{C} | x, 0^t \rangle \| \leq \beta$.

Note that MQCSP is a promise problem!

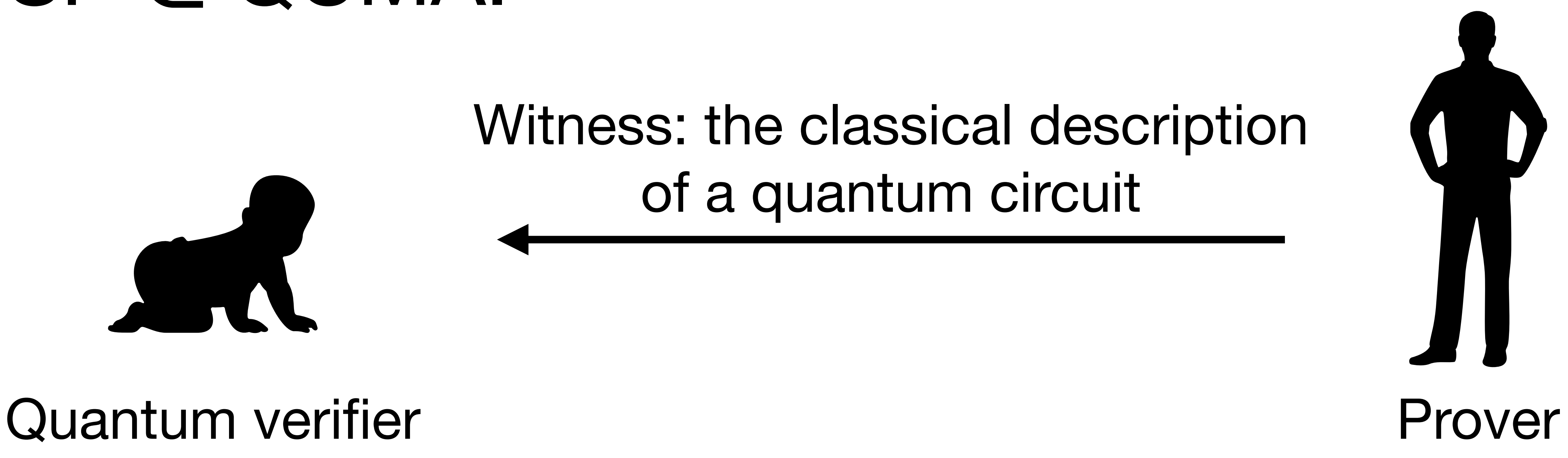
Basic Complexity Results

Basic Complexity Results

- **Upper bound:** MQCSP $\in$ QCMA.

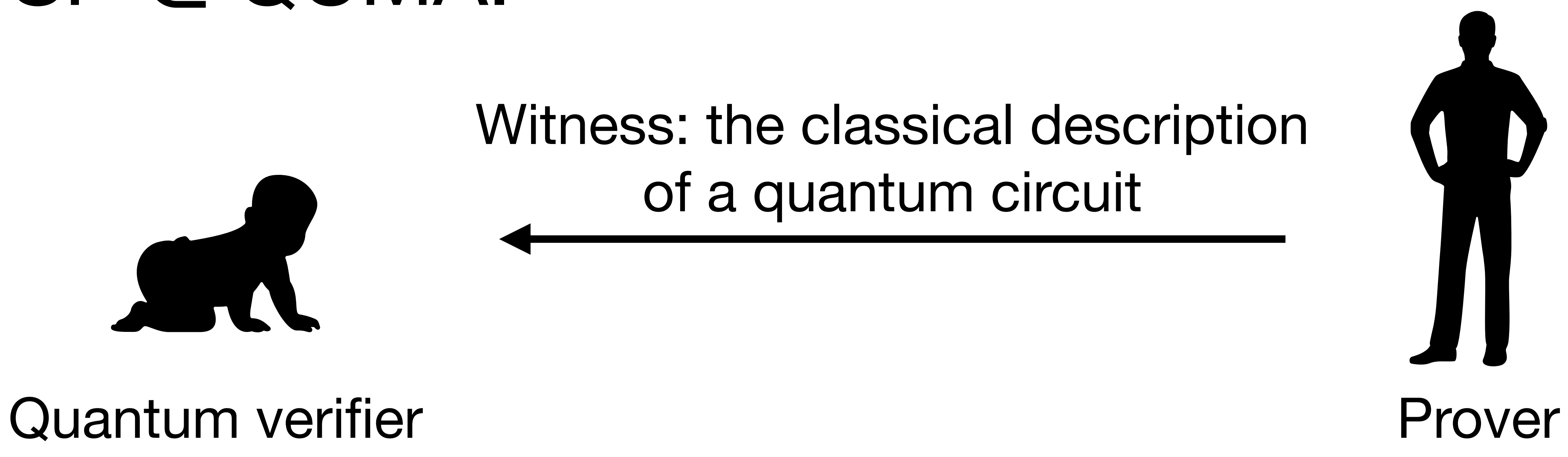
Basic Complexity Results

- **Upper bound:** MQCSP $\in$ QCMA.



Basic Complexity Results

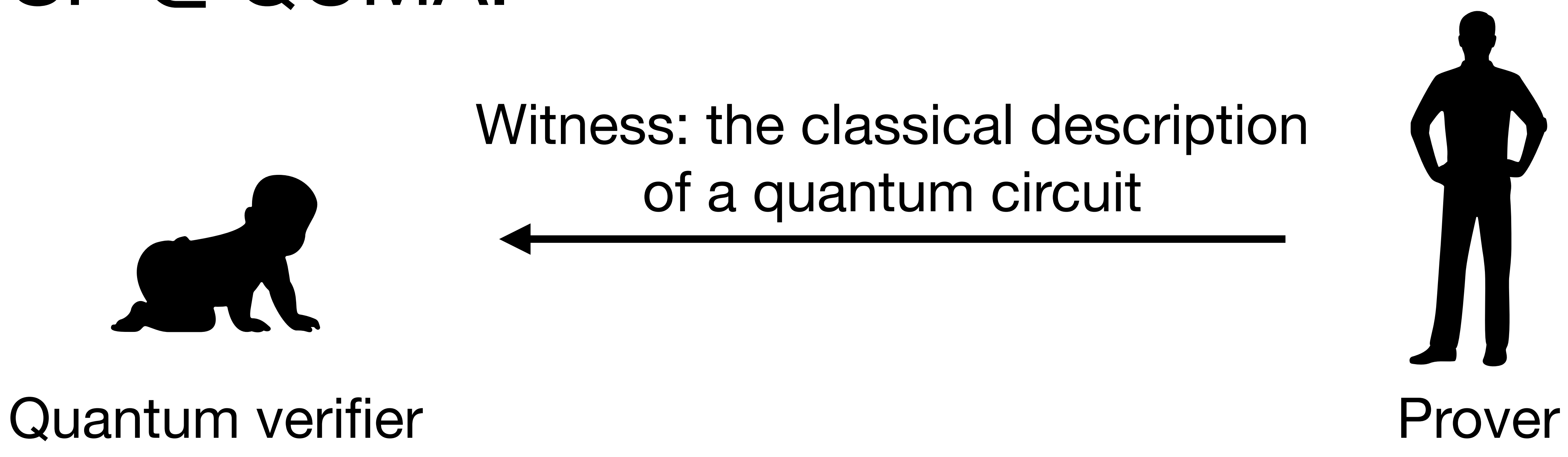
- **Upper bound:** MQCSP $\in$ QCMA.



- **Unconditional lower bound:** Multi-output MQCSP is NP-hard under randomized reduction. Quantize a classical result by [Ilango-Loff-Oliveria'20].

Basic Complexity Results

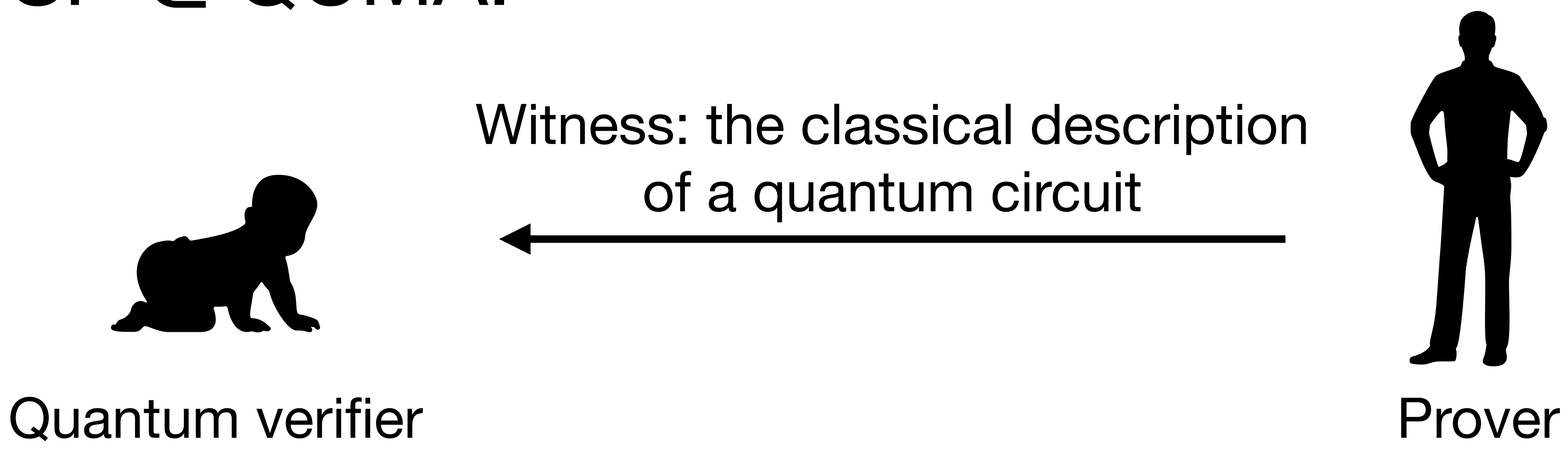
- **Upper bound:** MQCSP $\in$ QCMA.



- **Unconditional lower bound:** Multi-output MQCSP is NP-hard under randomized reduction. Quantize a classical result by [Ilango-Loff-Oliveria'20].
- **Condition lower bound:**

Basic Complexity Results

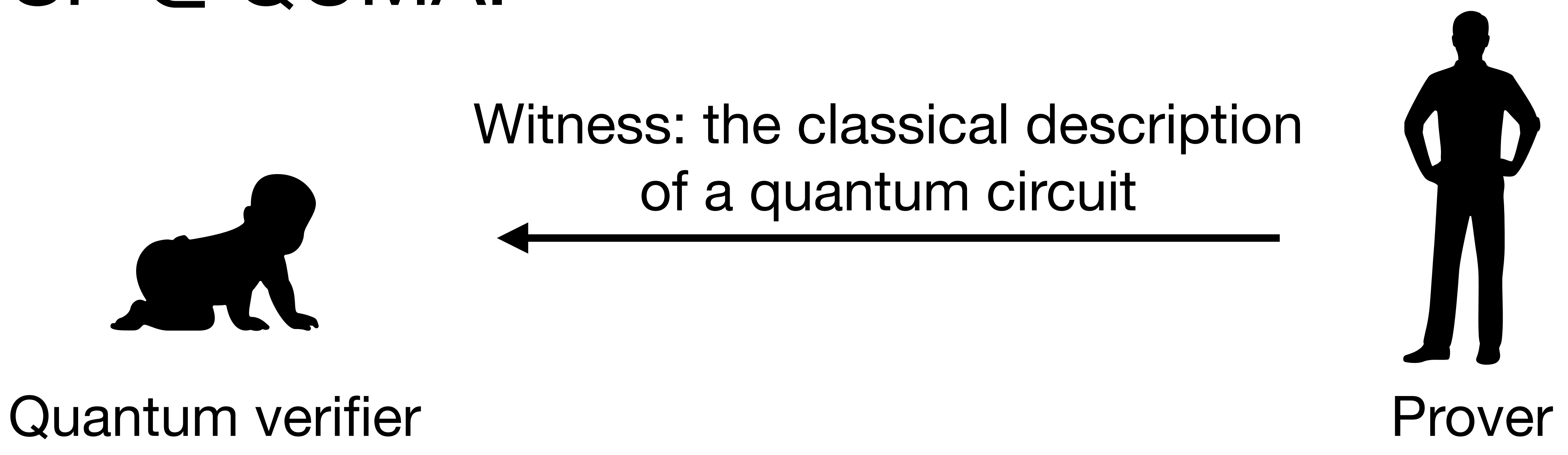
- **Upper bound:** MQCSP ∈ QCMA.



- **Unconditional lower bound:** Multi-output MQCSP is NP-hard under randomized reduction. Quantize a classical result by [Ilango-Loff-Oliveria’20].
- **Condition lower bound:**
  - ∃ One-way function ⇒ MQCSP ∉ BQP.

Basic Complexity Results

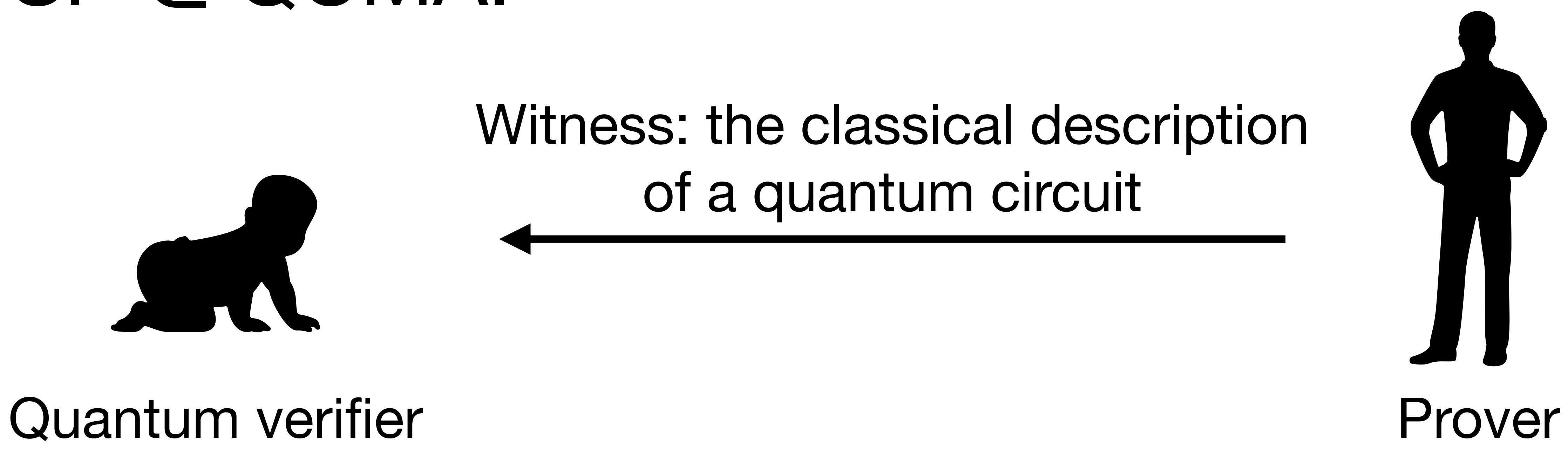
- **Upper bound:** MQCSP $\in$ QCMA.



- **Unconditional lower bound:** Multi-output MQCSP is NP-hard under randomized reduction. Quantize a classical result by [Ilango-Loff-Oliveria’20].
- **Condition lower bound:**
  - $\exists$ One-way function $\Rightarrow$ MQCSP $\notin$ BQP.
  - MQCSP is not easier than SZK.

Basic Complexity Results

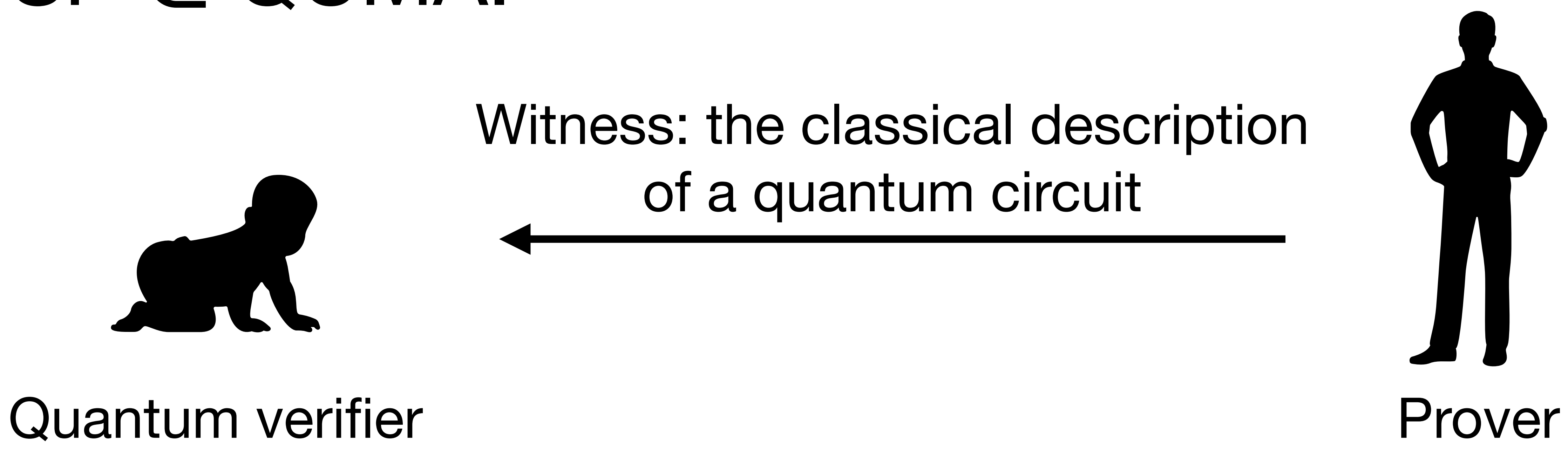
- **Upper bound:** MQCSP $\in$ QCMA.



- **Unconditional lower bound:** Multi-output MQCSP is NP-hard under randomized reduction. Quantize a classical result by [Ilango-Loff-Oliveria'20].
- **Condition lower bound:**
  - $\exists$ One-way function $\Rightarrow$ MQCSP $\notin$ BQP.
  - MQCSP is not easier than SZK.
  - …

Basic Complexity Results

- **Upper bound:** MQCSP ∈ QCMA.



- **Unconditional lower bound:** Multi-output MQCSP is NP-hard under randomized reduction. Quantize a classical result by [Ilango-Loff-Oliveria'20].
- **Condition lower bound:**
  - ∃ One-way function ⇒ MQCSP ∉ BQP.
  - MQCSP is not easier than SZK.
  - …

Quantize classical results!

A Bird-Eye View on Our Results

A Bird-Eye View

	Results	Informal Theorem Index (Formal Theorem Index)
MQCSP (Def. 3.2)	MQCSP $\in$ QCMA	Theorem 1.4 (Theorem 3.9)
	MQCSP $\in$ BQP $\Rightarrow$ No qOWF	Theorem 1.4 (Theorem 4.8)
	SZK $\leq$ MQCSP	Theorem 1.4 (Theorem 3.13)
	multiMQCSP is NP-hard under a natural gate set	Theorem 1.4 (Theorem 3.14)
	$i\mathcal{O}$ + MQCSP $\in$ BQP $\Rightarrow$ NP $\subseteq$ coRQP	Theorem 1.4 (Theorem 4.10)
	PAC learning for BQP/poly $\Leftrightarrow$ MQCSP $\in$ BPP	Theorem 1.5 (Theorem 4.12)
	BQP learning $\Leftrightarrow$ MQCSP $\in$ BQP	Theorem 1.6 (Theorem 4.14)
	MQCSP $\in$ BQP $\Rightarrow$ BQE $\not\subset$ BQC$[n^k]$, $\forall k \in \mathbb{N}_+$	Theorem 1.7 (Theorem 4.19)
	MQCSP $\in$ BQP $\Rightarrow$ BQP$^{\mathsf{QCMA}}$ $\not\subset$ BQC$[n^k]$, $\forall k \in \mathbb{N}_+$	Theorem 1.7 (Theorem 4.22)
	MQCSP $\in$ BQP $\Rightarrow$ Hardness amplification	Theorem 1.8 (Theorem 4.20)
	Hardness magnification for MQCSP	Theorem 1.9 (Theorem 4.22)
	QETH $\Rightarrow$ quantum hardness of MQCSP*	Theorem 1.10 (Theorem 4.27)
UMCSP (Def. 5.1)	UMCSP $\in$ QCMA	Theorem 1.11 (Theorem 5.5)
	Search-to-decision reduction for UMCSP	Theorem 1.12 (Theorem 5.16)
	gap-MQCSP $\leq$ UMCSP	Theorem 1.12 (Theorem 5.23)
	UMCSP $\in$ BQP $\Rightarrow$ No pseudorandom unitaries and no qOWF	(Theorem 5.24, Corollary 5.25)
	$i\mathcal{O}$ + UMCSP $\in$ BQP $\Rightarrow$ NP $\subseteq$ coRQP	(Corollary 5.26)
	UMCSP $\in$ BQP $\Rightarrow$ Hardness amplification for BQP	(Corollary 5.27)
	UMCSP $\in$ BQP $\Rightarrow$ BQE $\not\subset$ BQP$[n^k]$, $\forall k \in \mathbb{N}$	(Corollary 5.28)
SMCSP (Def. 5.2)	SMCSP can be verified via QCMA	Theorem 1.11 (Theorem 5.9)
	Search-to-decision reduction for SMCSP	Theorem 1.12 (Theorem 5.18)
	Self-reduction for SMCSP	Theorem 1.12 (Theorem 5.20)
	SMCSP $\in$ BQP $\Rightarrow$ No pseudorandom states and no qOWF	Theorem 1.13 (Theorem 5.30)
	Assume conjectures from physics SMCSP $\Rightarrow$ Estimating wormhole's volume	Theorem 1.13 (Theorem 5.31)
	Succinct state tomography $\leq$ SMCSP	Theorem 1.13 (Theorem 5.33)

Table 1: Summary of our results. A result with color Blue is a direct extension from its classical analog. A result with color Yellow requires additional techniques. A result with color Red is unique in the quantum setting.

A Bird-Eye View

	Results	Informal Theorem Index (Formal Theorem Index)
MQCSP (Def. 3.2)	MQCSP $\in$ QCMA	Theorem 1.4 (Theorem 3.9)
	MQCSP $\in$ BQP $\Rightarrow$ No qOWF	Theorem 1.4 (Theorem 4.8)
	SZK $\leq$ MQCSP	Theorem 1.4 (Theorem 3.13)
	multiMQCSP is NP-hard under a natural gate set	Theorem 1.4 (Theorem 3.14)
	$i\mathcal{O}$ + MQCSP $\in$ BQP $\Rightarrow$ NP $\subseteq$ coRQP	Theorem 1.4 (Theorem 4.10)
	PAC learning for BQP/poly $\Leftrightarrow$ MQCSP $\in$ BPP	Theorem 1.5 (Theorem 4.12)
	BQP learning $\Leftrightarrow$ MQCSP $\in$ BQP	Theorem 1.6 (Theorem 4.14)
	MQCSP $\in$ BQP $\Rightarrow$ BQE $\not\subset$ BQC$[n^k]$, $\forall k \in \mathbb{N}_+$	Theorem 1.7 (Theorem 4.19)
	MQCSP $\in$ BQP $\Rightarrow$ BQP$^{\mathsf{QCMA}}$ $\not\subset$ BQC$[n^k]$, $\forall k \in \mathbb{N}_+$	Theorem 1.7 (Theorem 4.22)
	MQCSP $\in$ BQP $\Rightarrow$ Hardness amplification	Theorem 1.8 (Theorem 4.20)
	Hardness magnification for MQCSP	Theorem 1.9 (Theorem 4.22)
	QETH $\Rightarrow$ quantum hardness of MQCSP*	Theorem 1.10 (Theorem 4.27)
UMCSP (Def. 5.1)	UMCSP $\in$ QCMA	Theorem 1.11 (Theorem 5.5)
	Search-to-decision reduction for UMCSP	Theorem 1.12 (Theorem 5.16)
	gap-MQCSP $\leq$ UMCSP	Theorem 1.12 (Theorem 5.23)
	UMCSP $\in$ BQP $\Rightarrow$ No pseudorandom unitaries and no qOWF	(Theorem 5.24, Corollary 5.25)
	$i\mathcal{O}$ + UMCSP $\in$ BQP $\Rightarrow$ NP $\subseteq$ coRQP	(Corollary 5.26)
	UMCSP $\in$ BQP $\Rightarrow$ Hardness amplification for BQP	(Corollary 5.27)
	UMCSP $\in$ BQP $\Rightarrow$ BQE $\not\subset$ BQP$[n^k]$, $\forall k \in \mathbb{N}$	(Corollary 5.28)
SMCSP (Def. 5.2)	SMCSP can be verified via QCMA	Theorem 1.11 (Theorem 5.9)
	Search-to-decision reduction for SMCSP	Theorem 1.12 (Theorem 5.18)
	Self-reduction for SMCSP	Theorem 1.12 (Theorem 5.20)
	SMCSP $\in$ BQP $\Rightarrow$ No pseudorandom states and no qOWF	Theorem 1.13 (Theorem 5.30)
	Assume conjectures from physics SMCSP $\Rightarrow$ Estimating wormhole's volume	Theorem 1.13 (Theorem 5.31)
	Succinct state tomography $\leq$ SMCSP	Theorem 1.13 (Theorem 5.33)

Table 1: Summary of our results. A result with color Blue is a direct extension from its classical analog. A result with color Yellow requires additional techniques. A result with color Red is unique in the quantum setting.

- Cryptography.

A Bird-Eye View

	Results	Informal Theorem Index (Formal Theorem Index)
MQCSP (Def. 3.2)	MQCSP $\in$ QCMA	Theorem 1.4 (Theorem 3.9)
	MQCSP $\in$ BQP $\Rightarrow$ No qOWF	Theorem 1.4 (Theorem 4.8)
	SZK $\leq$ MQCSP	Theorem 1.4 (Theorem 3.13)
	multiMQCSP is NP-hard under a natural gate set	Theorem 1.4 (Theorem 3.14)
	$i\mathcal{O}$ + MQCSP $\in$ BQP $\Rightarrow$ NP $\subseteq$ coRQP	Theorem 1.4 (Theorem 4.10)
	PAC learning for BQP/poly $\Leftrightarrow$ MQCSP $\in$ BPP	Theorem 1.5 (Theorem 4.12)
	BQP learning $\Leftrightarrow$ MQCSP $\in$ BQP	Theorem 1.6 (Theorem 4.14)
	MQCSP $\in$ BQP $\Rightarrow$ BQE $\not\subset$ BQC$[n^k]$, $\forall k \in \mathbb{N}_+$	Theorem 1.7 (Theorem 4.19)
	MQCSP $\in$ BQP $\Rightarrow$ BQP$^{\text{QCMA}}$ $\not\subset$ BQC$[n^k]$, $\forall k \in \mathbb{N}_+$	Theorem 1.7 (Theorem 4.22)
	MQCSP $\in$ BQP $\Rightarrow$ Hardness amplification	Theorem 1.8 (Theorem 4.20)
	Hardness magnification for MQCSP	Theorem 1.9 (Theorem 4.22)
	QETH $\Rightarrow$ quantum hardness of MQCSP*	Theorem 1.10 (Theorem 4.27)
UMCSP (Def. 5.1)	UMCSP $\in$ QCMA	Theorem 1.11 (Theorem 5.5)
	Search-to-decision reduction for UMCSP	Theorem 1.12 (Theorem 5.16)
	gap-MQCSP $\leq$ UMCSP	Theorem 1.12 (Theorem 5.23)
	UMCSP $\in$ BQP $\Rightarrow$ No pseudorandom unitaries and no qOWF	(Theorem 5.24, Corollary 5.25)
	$i\mathcal{O}$ + UMCSP $\in$ BQP $\Rightarrow$ NP $\subseteq$ coRQP	(Corollary 5.26)
	UMCSP $\in$ BQP $\Rightarrow$ Hardness amplification for BQP	(Corollary 5.27)
	UMCSP $\in$ BQP $\Rightarrow$ BQE $\not\subset$ BQP$[n^k]$, $\forall k \in \mathbb{N}$	(Corollary 5.28)
SMCSP (Def. 5.2)	SMCSP can be verified via QCMA	Theorem 1.11 (Theorem 5.9)
	Search-to-decision reduction for SMCSP	Theorem 1.12 (Theorem 5.18)
	Self-reduction for SMCSP	Theorem 1.12 (Theorem 5.20)
	SMCSP $\in$ BQP $\Rightarrow$ No pseudorandom states and no qOWF	Theorem 1.13 (Theorem 5.30)
	Assume conjectures from physics SMCSP $\Rightarrow$ Estimating wormhole's volume	Theorem 1.13 (Theorem 5.31)
	Succinct state tomography $\leq$ SMCSP	Theorem 1.13 (Theorem 5.33)

Table 1: Summary of our results. A result with color Blue is a direct extension from its classical analog. A result with color Yellow requires additional techniques. A result with color Red is unique in the quantum setting.

- Cryptography.
- Learning theory.

A Bird-Eye View

	Results	Informal Theorem Index (Formal Theorem Index)
MQCSP (Def. 3.2)	$\mathsf{MQCSP} \in \mathsf{QCMA}$	Theorem 1.4 (Theorem 3.9)
	$\mathsf{MQCSP} \in \mathsf{BQP} \Rightarrow$ No qOWF	Theorem 1.4 (Theorem 4.8)
	$\mathsf{SZK} \leq \mathsf{MQCSP}$	Theorem 1.4 (Theorem 3.13)
	multiMQCSP is NP-hard under a natural gate set	Theorem 1.4 (Theorem 3.14)
	$i\mathcal{O} + \mathsf{MQCSP} \in \mathsf{BQP} \Rightarrow \mathsf{NP} \subseteq \mathsf{coRQP}$	Theorem 1.4 (Theorem 4.10)
	PAC learning for $\mathsf{BQP/poly} \Leftrightarrow \mathsf{MQCSP} \in \mathsf{BPP}$	Theorem 1.5 (Theorem 4.12)
	BQP learning $\Leftrightarrow \mathsf{MQCSP} \in \mathsf{BQP}$	Theorem 1.6 (Theorem 4.14)
	$\mathsf{MQCSP} \in \mathsf{BQP} \Rightarrow \mathsf{BQE} \not\subset \mathsf{BQC}[n^k], \forall k \in \mathbb{N}_+$	Theorem 1.7 (Theorem 4.19)
	$\mathsf{MQCSP} \in \mathsf{BQP} \Rightarrow \mathsf{BQP}^{\mathsf{QCMA}} \not\subset \mathsf{BQC}[n^k], \forall k \in \mathbb{N}_+$	Theorem 1.7 (Theorem 4.22)
	$\mathsf{MQCSP} \in \mathsf{BQP} \Rightarrow$ Hardness amplification	Theorem 1.8 (Theorem 4.20)
	Hardness magnification for MQCSP	Theorem 1.9 (Theorem 4.22)
	$\mathsf{QETH} \Rightarrow$ quantum hardness of MQCSP^*	Theorem 1.10 (Theorem 4.27)
UMCSP (Def. 5.1)	$\mathsf{UMCSP} \in \mathsf{QCMA}$	Theorem 1.11 (Theorem 5.5)
	Search-to-decision reduction for UMCSP	Theorem 1.12 (Theorem 5.16)
	$\mathsf{gap\text{-}MQCSP} \leq \mathsf{UMCSP}$	Theorem 1.12 (Theorem 5.23)
	$\mathsf{UMCSP} \in \mathsf{BQP}$ $\Rightarrow$ No pseudorandom unitaries and no qOWF	(Theorem 5.24, Corollary 5.25)
	$i\mathcal{O} + \mathsf{UMCSP} \in \mathsf{BQP} \Rightarrow \mathsf{NP} \subseteq \mathsf{coRQP}$	(Corollary 5.26)
	$\mathsf{UMCSP} \in \mathsf{BQP} \Rightarrow$ Hardness amplification for BQP	(Corollary 5.27)
	$\mathsf{UMCSP} \in \mathsf{BQP} \Rightarrow \mathsf{BQE} \not\subset \mathsf{BQP}[n^k], \forall k \in \mathbb{N}$	(Corollary 5.28)
SMCSP (Def. 5.2)	SMCSP can be verified via QCMA	Theorem 1.11 (Theorem 5.9)
	Search-to-decision reduction for SMCSP	Theorem 1.12 (Theorem 5.18)
	Self-reduction for SMCSP	Theorem 1.12 (Theorem 5.20)
	$\mathsf{SMCSP} \in \mathsf{BQP}$ $\Rightarrow$ No pseudorandom states and no qOWF	Theorem 1.13 (Theorem 5.30)
	Assume conjectures from physics SMCSP $\Rightarrow$ Estimating wormhole's volume	Theorem 1.13 (Theorem 5.31)
	Succinct state tomography $\leq$ SMCSP	Theorem 1.13 (Theorem 5.33)

Table 1: Summary of our results. A result with color Blue is a direct extension from its classical analog. A result with color Yellow requires additional techniques. A result with color Red is unique in the quantum setting.

- Cryptography.
- Learning theory.
- Circuit lower bounds.

A Bird-Eye View

	Results	Informal Theorem Index (Formal Theorem Index)
MQCSP (Def. 3.2)	MQCSP $\in$ QCMA	Theorem 1.4 (Theorem 3.9)
	MQCSP $\in$ BQP $\Rightarrow$ No qOWF	Theorem 1.4 (Theorem 4.8)
	SZK $\leq$ MQCSP	Theorem 1.4 (Theorem 3.13)
	multiMQCSP is NP-hard under a natural gate set	Theorem 1.4 (Theorem 3.14)
	$i\mathcal{O}$ + MQCSP $\in$ BQP $\Rightarrow$ NP $\subseteq$ coRQP	Theorem 1.4 (Theorem 4.10)
	PAC learning for BQP/poly $\Leftrightarrow$ MQCSP $\in$ BPP	Theorem 1.5 (Theorem 4.12)
	BQP learning $\Leftrightarrow$ MQCSP $\in$ BQP	Theorem 1.6 (Theorem 4.14)
	MQCSP $\in$ BQP $\Rightarrow$ BQE $\not\subset$ BQC$[n^k]$, $\forall k \in \mathbb{N}_+$	Theorem 1.7 (Theorem 4.19)
	MQCSP $\in$ BQP $\Rightarrow$ BQP$^{\mathsf{QCMA}}$ $\not\subset$ BQC$[n^k]$, $\forall k \in \mathbb{N}_+$	Theorem 1.7 (Theorem 4.22)
	MQCSP $\in$ BQP $\Rightarrow$ Hardness amplification	Theorem 1.8 (Theorem 4.20)
	Hardness magnification for MQCSP	Theorem 1.9 (Theorem 4.22)
	QETH $\Rightarrow$ quantum hardness of MQCSP*	Theorem 1.10 (Theorem 4.27)
UMCSP (Def. 5.1)	UMCSP $\in$ QCMA	Theorem 1.11 (Theorem 5.5)
	Search-to-decision reduction for UMCSP	Theorem 1.12 (Theorem 5.16)
	gap-MQCSP $\leq$ UMCSP	Theorem 1.12 (Theorem 5.23)
	UMCSP $\in$ BQP $\Rightarrow$ No pseudorandom unitaries and no qOWF	(Theorem 5.24, Corollary 5.25)
	$i\mathcal{O}$ + UMCSP $\in$ BQP $\Rightarrow$ NP $\subseteq$ coRQP	(Corollary 5.26)
	UMCSP $\in$ BQP $\Rightarrow$ Hardness amplification for BQP	(Corollary 5.27)
	UMCSP $\in$ BQP $\Rightarrow$ BQE $\not\subset$ BQP$[n^k]$, $\forall k \in \mathbb{N}$	(Corollary 5.28)
SMCSP (Def. 5.2)	SMCSP can be verified via QCMA	Theorem 1.11 (Theorem 5.9)
	Search-to-decision reduction for SMCSP	Theorem 1.12 (Theorem 5.18)
	Self-reduction for SMCSP	Theorem 1.12 (Theorem 5.20)
	SMCSP $\in$ BQP $\Rightarrow$ No pseudorandom states and no qOWF	Theorem 1.13 (Theorem 5.30)
	Assume conjectures from physics SMCSP $\Rightarrow$ Estimating wormhole's volume	Theorem 1.13 (Theorem 5.31)
	Succinct state tomography $\leq$ SMCSP	Theorem 1.13 (Theorem 5.33)

Table 1: Summary of our results. A result with color Blue is a direct extension from its classical analog. A result with color Yellow requires additional techniques. A result with color Red is unique in the quantum setting.

- Cryptography.
- Learning theory.
- Circuit lower bounds.
- Fine-grained complexity.

A Bird-Eye View

	Results	Informal Theorem Index (Formal Theorem Index)
MQCSP (Def. 3.2)	MQCSP $\in$ QCMA	Theorem 1.4 (Theorem 3.9)
	MQCSP $\in$ BQP $\Rightarrow$ No qOWF	Theorem 1.4 (Theorem 4.8)
	SZK $\leq$ MQCSP	Theorem 1.4 (Theorem 3.13)
	multiMQCSP is NP-hard under a natural gate set	Theorem 1.4 (Theorem 3.14)
	$i\mathcal{O}$ + MQCSP $\in$ BQP $\Rightarrow$ NP $\subseteq$ coRQP	Theorem 1.4 (Theorem 4.10)
	PAC learning for BQP/poly $\Leftrightarrow$ MQCSP $\in$ BPP	Theorem 1.5 (Theorem 4.12)
	BQP learning $\Leftrightarrow$ MQCSP $\in$ BQP	Theorem 1.6 (Theorem 4.14)
	MQCSP $\in$ BQP $\Rightarrow$ BQE $\not\subset$ BQC$[n^k]$, $\forall k \in \mathbb{N}_+$	Theorem 1.7 (Theorem 4.19)
	MQCSP $\in$ BQP $\Rightarrow$ $\mathsf{BQP}^{\mathsf{QCMA}} \not\subset$ BQC$[n^k]$, $\forall k \in \mathbb{N}_+$	Theorem 1.7 (Theorem 4.22)
	MQCSP $\in$ BQP $\Rightarrow$ Hardness amplification	Theorem 1.8 (Theorem 4.20)
	Hardness magnification for MQCSP	Theorem 1.9 (Theorem 4.22)
	QETH $\Rightarrow$ quantum hardness of MQCSP*	Theorem 1.10 (Theorem 4.27)
UMCSP (Def. 5.1)	UMCSP $\in$ QCMA	Theorem 1.11 (Theorem 5.5)
	Search-to-decision reduction for UMCSP	Theorem 1.12 (Theorem 5.16)
	gap-MQCSP $\leq$ UMCSP	Theorem 1.12 (Theorem 5.23)
	UMCSP $\in$ BQP $\Rightarrow$ No pseudorandom unitaries and no qOWF	(Theorem 5.24, Corollary 5.25)
	$i\mathcal{O}$ + UMCSP $\in$ BQP $\Rightarrow$ NP $\subseteq$ coRQP	(Corollary 5.26)
	UMCSP $\in$ BQP $\Rightarrow$ Hardness amplification for BQP	(Corollary 5.27)
	UMCSP $\in$ BQP $\Rightarrow$ BQE $\not\subset$ BQP$[n^k]$, $\forall k \in \mathbb{N}$	(Corollary 5.28)
SMCSP (Def. 5.2)	SMCSP can be verified via QCMA	Theorem 1.11 (Theorem 5.9)
	Search-to-decision reduction for SMCSP	Theorem 1.12 (Theorem 5.18)
	Self-reduction for SMCSP	Theorem 1.12 (Theorem 5.20)
	SMCSP $\in$ BQP $\Rightarrow$ No pseudorandom states and no qOWF	Theorem 1.13 (Theorem 5.30)
	Assume conjectures from physics SMCSP $\Rightarrow$ Estimating wormhole's volume	Theorem 1.13 (Theorem 5.31)
	Succinct state tomography $\leq$ SMCSP	Theorem 1.13 (Theorem 5.33)

Table 1: Summary of our results. A result with color Blue is a direct extension from its classical analog. A result with color Yellow requires additional techniques. A result with color Red is unique in the quantum setting.

- Cryptography.
- Learning theory.
- Circuit lower bounds.
- Fine-grained complexity.

Mostly quantize classical results!

A Bird-Eye View

	Results	Informal Theorem Index (Formal Theorem Index)
MQCSP (Def. 3.2)	MQCSP $\in$ QCMA	Theorem 1.4 (Theorem 3.9)
	MQCSP $\in$ BQP $\Rightarrow$ No qOWF	Theorem 1.4 (Theorem 4.8)
	SZK $\leq$ MQCSP	Theorem 1.4 (Theorem 3.13)
	multiMQCSP is NP-hard under a natural gate set	Theorem 1.4 (Theorem 3.14)
	$i\mathcal{O}$ + MQCSP $\in$ BQP $\Rightarrow$ NP $\subseteq$ coRQP	Theorem 1.4 (Theorem 4.10)
	PAC learning for BQP/poly $\Leftrightarrow$ MQCSP $\in$ BPP	Theorem 1.5 (Theorem 4.12)
	BQP learning $\Leftrightarrow$ MQCSP $\in$ BQP	Theorem 1.6 (Theorem 4.14)
	MQCSP $\in$ BQP $\Rightarrow$ BQE $\not\subset$ BQC$[n^k]$, $\forall k \in \mathbb{N}_+$	Theorem 1.7 (Theorem 4.19)
	MQCSP $\in$ BQP $\Rightarrow$ BQP$^{\mathsf{QCMA}}$ $\not\subset$ BQC$[n^k]$, $\forall k \in \mathbb{N}_+$	Theorem 1.7 (Theorem 4.22)
	MQCSP $\in$ BQP $\Rightarrow$ Hardness amplification	Theorem 1.8 (Theorem 4.20)
	Hardness magnification for MQCSP	Theorem 1.9 (Theorem 4.22)
	QETH $\Rightarrow$ quantum hardness of MQCSP*	Theorem 1.10 (Theorem 4.27)
UMCSP (Def. 5.1)	UMCSP $\in$ QCMA	Theorem 1.11 (Theorem 5.5)
	Search-to-decision reduction for UMCSP	Theorem 1.12 (Theorem 5.16)
	gap-MQCSP $\leq$ UMCSP	Theorem 1.12 (Theorem 5.23)
	UMCSP $\in$ BQP $\Rightarrow$ No pseudorandom unitaries and no qOWF	(Theorem 5.24, Corollary 5.25)
	$i\mathcal{O}$ + UMCSP $\in$ BQP $\Rightarrow$ NP $\subseteq$ coRQP	(Corollary 5.26)
	UMCSP $\in$ BQP $\Rightarrow$ Hardness amplification for BQP	(Corollary 5.27)
	UMCSP $\in$ BQP $\Rightarrow$ BQE $\not\subset$ BQP$[n^k]$, $\forall k \in \mathbb{N}$	(Corollary 5.28)
SMCSP (Def. 5.2)	SMCSP can be verified via QCMA	Theorem 1.11 (Theorem 5.9)
	Search-to-decision reduction for SMCSP	Theorem 1.12 (Theorem 5.18)
	Self-reduction for SMCSP	Theorem 1.12 (Theorem 5.20)
	SMCSP $\in$ BQP $\Rightarrow$ No pseudorandom states and no qOWF	Theorem 1.13 (Theorem 5.30)
	Assume conjectures from physics SMCSP $\Rightarrow$ Estimating wormhole's volume	Theorem 1.13 (Theorem 5.31)
	Succinct state tomography $\leq$ SMCSP	Theorem 1.13 (Theorem 5.33)

Table 1: Summary of our results. A result with color Blue is a direct extension from its classical analog. A result with color Yellow requires additional techniques. A result with color Red is unique in the quantum setting.

- Cryptography.
- Learning theory.
- Circuit lower bounds.
- Fine-grained complexity.
- Reductions:

Mostly quantize classical results!

A Bird-Eye View

	Results	Informal Theorem Index (Formal Theorem Index)
MQCSP (Def. 3.2)	MQCSP $\in$ QCMA	Theorem 1.4 (Theorem 3.9)
	MQCSP $\in$ BQP $\Rightarrow$ No qOWF	Theorem 1.4 (Theorem 4.8)
	SZK $\leq$ MQCSP	Theorem 1.4 (Theorem 3.13)
	multiMQCSP is NP-hard under a natural gate set	Theorem 1.4 (Theorem 3.14)
	$i\mathcal{O}$ + MQCSP $\in$ BQP $\Rightarrow$ NP $\subseteq$ coRQP	Theorem 1.4 (Theorem 4.10)
	PAC learning for BQP/poly $\Leftrightarrow$ MQCSP $\in$ BPP	Theorem 1.5 (Theorem 4.12)
	BQP learning $\Leftrightarrow$ MQCSP $\in$ BQP	Theorem 1.6 (Theorem 4.14)
	MQCSP $\in$ BQP $\Rightarrow$ BQE $\not\subset$ BQC$[n^k]$, $\forall k \in \mathbb{N}_+$	Theorem 1.7 (Theorem 4.19)
	MQCSP $\in$ BQP $\Rightarrow$ BQP$^{\mathsf{QCMA}}$ $\not\subset$ BQC$[n^k]$, $\forall k \in \mathbb{N}_+$	Theorem 1.7 (Theorem 4.22)
	MQCSP $\in$ BQP $\Rightarrow$ Hardness amplification	Theorem 1.8 (Theorem 4.20)
	Hardness magnification for MQCSP	Theorem 1.9 (Theorem 4.22)
	QETH $\Rightarrow$ quantum hardness of MQCSP*	Theorem 1.10 (Theorem 4.27)
UMCSP (Def. 5.1)	UMCSP $\in$ QCMA	Theorem 1.11 (Theorem 5.5)
	Search-to-decision reduction for UMCSP	Theorem 1.12 (Theorem 5.16)
	gap-MQCSP $\leq$ UMCSP	Theorem 1.12 (Theorem 5.23)
	UMCSP $\in$ BQP $\Rightarrow$ No pseudorandom unitaries and no qOWF	(Theorem 5.24, Corollary 5.25)
	$i\mathcal{O}$ + UMCSP $\in$ BQP $\Rightarrow$ NP $\subseteq$ coRQP	(Corollary 5.26)
	UMCSP $\in$ BQP $\Rightarrow$ Hardness amplification for BQP	(Corollary 5.27)
	UMCSP $\in$ BQP $\Rightarrow$ BQE $\not\subset$ BQP$[n^k]$, $\forall k \in \mathbb{N}$	(Corollary 5.28)
SMCSP (Def. 5.2)	SMCSP can be verified via QCMA	Theorem 1.11 (Theorem 5.9)
	Search-to-decision reduction for SMCSP	Theorem 1.12 (Theorem 5.18)
	Self-reduction for SMCSP	Theorem 1.12 (Theorem 5.20)
	SMCSP $\in$ BQP $\Rightarrow$ No pseudorandom states and no qOWF	Theorem 1.13 (Theorem 5.30)
	Assume conjectures from physics SMCSP $\Rightarrow$ Estimating wormhole's volume	Theorem 1.13 (Theorem 5.31)
	Succinct state tomography $\leq$ SMCSP	Theorem 1.13 (Theorem 5.33)

Table 1: Summary of our results. A result with color Blue is a direct extension from its classical analog. A result with color Yellow requires additional techniques. A result with color Red is unique in the quantum setting.

- Cryptography.
- Learning theory.
- Circuit lower bounds.
- Fine-grained complexity.
- Reductions:
  - Among different objects.

Mostly quantize classical results!

A Bird-Eye View

	Results	Informal Theorem Index (Formal Theorem Index)
MQCSP (Def. 3.2)	MQCSP $\in$ QCMA	Theorem 1.4 (Theorem 3.9)
	MQCSP $\in$ BQP $\Rightarrow$ No qOWF	Theorem 1.4 (Theorem 4.8)
	SZK $\leq$ MQCSP	Theorem 1.4 (Theorem 3.13)
	multiMQCSP is NP-hard under a natural gate set	Theorem 1.4 (Theorem 3.14)
	$i\mathcal{O}$ + MQCSP $\in$ BQP $\Rightarrow$ NP $\subseteq$ coRQP	Theorem 1.4 (Theorem 4.10)
	PAC learning for BQP/poly $\Leftrightarrow$ MQCSP $\in$ BPP	Theorem 1.5 (Theorem 4.12)
	BQP learning $\Leftrightarrow$ MQCSP $\in$ BQP	Theorem 1.6 (Theorem 4.14)
	MQCSP $\in$ BQP $\Rightarrow$ BQE $\not\subset$ BQC$[n^k]$, $\forall k \in \mathbb{N}_+$	Theorem 1.7 (Theorem 4.19)
	MQCSP $\in$ BQP $\Rightarrow$ BQP$^{\text{QCMA}}$ $\not\subset$ BQC$[n^k]$, $\forall k \in \mathbb{N}_+$	Theorem 1.7 (Theorem 4.22)
	MQCSP $\in$ BQP $\Rightarrow$ Hardness amplification	Theorem 1.8 (Theorem 4.20)
	Hardness magnification for MQCSP	Theorem 1.9 (Theorem 4.22)
	QETH $\Rightarrow$ quantum hardness of MQCSP*	Theorem 1.10 (Theorem 4.27)
UMCSP (Def. 5.1)	UMCSP $\in$ QCMA	Theorem 1.11 (Theorem 5.5)
	Search-to-decision reduction for UMCSP	Theorem 1.12 (Theorem 5.16)
	gap-MQCSP $\leq$ UMCSP	Theorem 1.12 (Theorem 5.23)
	UMCSP $\in$ BQP $\Rightarrow$ No pseudorandom unitaries and no qOWF	(Theorem 5.24, Corollary 5.25)
	$i\mathcal{O}$ + UMCSP $\in$ BQP $\Rightarrow$ NP $\subseteq$ coRQP	(Corollary 5.26)
	UMCSP $\in$ BQP $\Rightarrow$ Hardness amplification for BQP	(Corollary 5.27)
	UMCSP $\in$ BQP $\Rightarrow$ BQE $\not\subset$ BQP$[n^k]$, $\forall k \in \mathbb{N}$	(Corollary 5.28)
SMCSP (Def. 5.2)	SMCSP can be verified via QCMA	Theorem 1.11 (Theorem 5.9)
	Search-to-decision reduction for SMCSP	Theorem 1.12 (Theorem 5.18)
	Self-reduction for SMCSP	Theorem 1.12 (Theorem 5.20)
	SMCSP $\in$ BQP $\Rightarrow$ No pseudorandom states and no qOWF	Theorem 1.13 (Theorem 5.30)
	Assume conjectures from physics SMCSP $\Rightarrow$ Estimating wormhole's volume	Theorem 1.13 (Theorem 5.31)
	Succinct state tomography $\leq$ SMCSP	Theorem 1.13 (Theorem 5.33)

Table 1: Summary of our results. A result with color Blue is a direct extension from its classical analog. A result with color Yellow requires additional techniques. A result with color Red is unique in the quantum setting.

- Cryptography.
- Learning theory.
- Circuit lower bounds.
- Fine-grained complexity.
- Reductions:
  - Among different objects.
  - Self-reduction.

Mostly quantize classical results!

A Bird-Eye View

	Results	Informal Theorem Index (Formal Theorem Index)
MQCSP (Def. 3.2)	MQCSP $\in$ QCMA	Theorem 1.4 (Theorem 3.9)
	MQCSP $\in$ BQP $\Rightarrow$ No qOWF	Theorem 1.4 (Theorem 4.8)
	SZK $\leq$ MQCSP	Theorem 1.4 (Theorem 3.13)
	multiMQCSP is NP-hard under a natural gate set	Theorem 1.4 (Theorem 3.14)
	$i\mathcal{O}$ + MQCSP $\in$ BQP $\Rightarrow$ NP $\subseteq$ coRQP	Theorem 1.4 (Theorem 4.10)
	PAC learning for BQP/poly $\Leftrightarrow$ MQCSP $\in$ BPP	Theorem 1.5 (Theorem 4.12)
	BQP learning $\Leftrightarrow$ MQCSP $\in$ BQP	Theorem 1.6 (Theorem 4.14)
	MQCSP $\in$ BQP $\Rightarrow$ BQE $\not\subset$ BQC$[n^k]$, $\forall k \in \mathbb{N}_+$	Theorem 1.7 (Theorem 4.19)
	MQCSP $\in$ BQP $\Rightarrow$ BQP$^{\mathsf{QCMA}}$ $\not\subset$ BQC$[n^k]$, $\forall k \in \mathbb{N}_+$	Theorem 1.7 (Theorem 4.22)
	MQCSP $\in$ BQP $\Rightarrow$ Hardness amplification	Theorem 1.8 (Theorem 4.20)
	Hardness magnification for MQCSP	Theorem 1.9 (Theorem 4.22)
	QETH $\Rightarrow$ quantum hardness of MQCSP*	Theorem 1.10 (Theorem 4.27)
UMCSP (Def. 5.1)	UMCSP $\in$ QCMA	Theorem 1.11 (Theorem 5.5)
	Search-to-decision reduction for UMCSP	Theorem 1.12 (Theorem 5.16)
	gap-MQCSP $\leq$ UMCSP	Theorem 1.12 (Theorem 5.23)
	UMCSP $\in$ BQP $\Rightarrow$ No pseudorandom unitaries and no qOWF	(Theorem 5.24, Corollary 5.25)
	$i\mathcal{O}$ + UMCSP $\in$ BQP $\Rightarrow$ NP $\subseteq$ coRQP	(Corollary 5.26)
	UMCSP $\in$ BQP $\Rightarrow$ Hardness amplification for BQP	(Corollary 5.27)
	UMCSP $\in$ BQP $\Rightarrow$ BQE $\not\subset$ BQP$[n^k]$, $\forall k \in \mathbb{N}$	(Corollary 5.28)
SMCSP (Def. 5.2)	SMCSP can be verified via QCMA	Theorem 1.11 (Theorem 5.9)
	Search-to-decision reduction for SMCSP	Theorem 1.12 (Theorem 5.18)
	Self-reduction for SMCSP	Theorem 1.12 (Theorem 5.20)
	SMCSP $\in$ BQP $\Rightarrow$ No pseudorandom states and no qOWF	Theorem 1.13 (Theorem 5.30)
	Assume conjectures from physics SMCSP $\Rightarrow$ Estimating wormhole's volume	Theorem 1.13 (Theorem 5.31)
	Succinct state tomography $\leq$ SMCSP	Theorem 1.13 (Theorem 5.33)

Table 1: Summary of our results. A result with color Blue is a direct extension from its classical analog. A result with color Yellow requires additional techniques. A result with color Red is unique in the quantum setting.

- Cryptography.
- Learning theory.
- Circuit lower bounds.
- Fine-grained complexity.

Mostly quantize classical results!

- Reductions:
  - Among different objects.
  - Self-reduction.
  - Search-to-decision reduction.

A Bird-Eye View

	Results	Informal Theorem Index (Formal Theorem Index)
MQCSP (Def. 3.2)	MQCSP $\in$ QCMA	Theorem 1.4 (Theorem 3.9)
	MQCSP $\in$ BQP $\Rightarrow$ No qOWF	Theorem 1.4 (Theorem 4.8)
	SZK $\leq$ MQCSP	Theorem 1.4 (Theorem 3.13)
	multiMQCSP is NP-hard under a natural gate set	Theorem 1.4 (Theorem 3.14)
	$i\mathcal{O}$ + MQCSP $\in$ BQP $\Rightarrow$ NP $\subseteq$ coRQP	Theorem 1.4 (Theorem 4.10)
	PAC learning for BQP/poly $\Leftrightarrow$ MQCSP $\in$ BPP	Theorem 1.5 (Theorem 4.12)
	BQP learning $\Leftrightarrow$ MQCSP $\in$ BQP	Theorem 1.6 (Theorem 4.14)
	MQCSP $\in$ BQP $\Rightarrow$ BQE $\not\subset$ BQC$[n^k]$, $\forall k \in \mathbb{N}_+$	Theorem 1.7 (Theorem 4.19)
	MQCSP $\in$ BQP $\Rightarrow$ BQP$^{\text{QCMA}}$ $\not\subset$ BQC$[n^k]$, $\forall k \in \mathbb{N}_+$	Theorem 1.7 (Theorem 4.22)
	MQCSP $\in$ BQP $\Rightarrow$ Hardness amplification	Theorem 1.8 (Theorem 4.20)
	Hardness magnification for MQCSP	Theorem 1.9 (Theorem 4.22)
	QETH $\Rightarrow$ quantum hardness of MQCSP*	Theorem 1.10 (Theorem 4.27)
UMCSP (Def. 5.1)	UMCSP $\in$ QCMA	Theorem 1.11 (Theorem 5.5)
	Search-to-decision reduction for UMCSP	Theorem 1.12 (Theorem 5.16)
	gap-MQCSP $\leq$ UMCSP	Theorem 1.12 (Theorem 5.23)
	UMCSP $\in$ BQP $\Rightarrow$ No pseudorandom unitaries and no qOWF	(Theorem 5.24, Corollary 5.25)
	$i\mathcal{O}$ + UMCSP $\in$ BQP $\Rightarrow$ NP $\subseteq$ coRQP	(Corollary 5.26)
	UMCSP $\in$ BQP $\Rightarrow$ Hardness amplification for BQP	(Corollary 5.27)
	UMCSP $\in$ BQP $\Rightarrow$ BQE $\not\subset$ BQP$[n^k]$, $\forall k \in \mathbb{N}$	(Corollary 5.28)
SMCSP (Def. 5.2)	SMCSP can be verified via QCMA	Theorem 1.11 (Theorem 5.9)
	Search-to-decision reduction for SMCSP	Theorem 1.12 (Theorem 5.18)
	Self-reduction for SMCSP	Theorem 1.12 (Theorem 5.20)
	SMCSP $\in$ BQP $\Rightarrow$ No pseudorandom states and no qOWF	Theorem 1.13 (Theorem 5.30)
	Assume conjectures from physics SMCSP $\Rightarrow$ Estimating wormhole's volume	Theorem 1.13 (Theorem 5.31)
	Succinct state tomography $\leq$ SMCSP	Theorem 1.13 (Theorem 5.33)

Table 1: Summary of our results. A result with color Blue is a direct extension from its classical analog. A result with color Yellow requires additional techniques. A result with color Red is unique in the quantum setting.

- Cryptography.
- Learning theory.
- Circuit lower bounds.
- Fine-grained complexity.

Mostly quantize classical results!

- Reductions:
  - Among different objects.
  - Self-reduction.
  - Search-to-decision reduction.
- Pseudorandom state, wormhole's volume, succinct state tomography…

Challenges and Difficulties in the Quantum Setting

Challenges and Difficulties in the Quantum Setting

- Quantum computation is generally erroneous and random.

Challenges and Difficulties in the Quantum Setting

- Quantum computation is generally erroneous and random.
  - This makes the definition of MCSP in the quantum setting subtle, e.g., promise problem.

Challenges and Difficulties in the Quantum Setting

- Quantum computation is generally erroneous and random.
  - This makes the definition of MCSP in the quantum setting subtle, e.g., promise problem.
  - The classical “fixing random string” trick does not work in quantum.

Challenges and Difficulties in the Quantum Setting

- Quantum computation is generally erroneous and random.
  - This makes the definition of MCSP in the quantum setting subtle, e.g., promise problem.
  - The classical “fixing random string” trick does not work in quantum.
- The introduction of ancilla qubits.

Challenges and Difficulties in the Quantum Setting

- Quantum computation is generally erroneous and random.
  - This makes the definition of MCSP in the quantum setting subtle, e.g., promise problem.
  - The classical "fixing random string" trick does not work in quantum.
- The introduction of ancilla qubits.
  - Different number of ancilla qubits gives different circuit complexity!

Challenges and Difficulties in the Quantum Setting

- Quantum computation is generally erroneous and random.
  - This makes the definition of MCSP in the quantum setting subtle, e.g., promise problem.
  - The classical “fixing random string” trick does not work in quantum.
- The introduction of ancilla qubits.
  - Different number of ancilla qubits gives different circuit complexity!
  - When the number of ancilla qubits is super-linear, a direct classical simulation becomes super-polynomial!

Challenges and Difficulties in the Quantum Setting

- Quantum computation is generally erroneous and random.
  - This makes the definition of MCSP in the quantum setting subtle, e.g., promise problem.
  - The classical “fixing random string” trick does not work in quantum.
- The introduction of ancilla qubits.
  - Different number of ancilla qubits gives different circuit complexity!
  - When the number of ancilla qubits is super-linear, a direct classical simulation becomes super-polynomial!
- Various universal quantum gate sets.

Challenges and Difficulties in the Quantum Setting

- Quantum computation is generally erroneous and random.
  - This makes the definition of MCSP in the quantum setting subtle, e.g., promise problem.
  - The classical “fixing random string” trick does not work in quantum.
- The introduction of ancilla qubits.
  - Different number of ancilla qubits gives different circuit complexity!
  - When the number of ancilla qubits is super-linear, a direct classical simulation becomes super-polynomial!
- Various universal quantum gate sets.
  - For some results we only know how to start with a certain gate set.

Challenges and Difficulties in the Quantum Setting

- Quantum computation is generally erroneous and random.
    - This makes the definition of MCSP in the quantum setting subtle, e.g., promise problem.
    - The classical "fixing random string" trick does not work in quantum.
- The introduction of ancilla qubits.
    - Different number of ancilla qubits gives different circuit complexity!
    - When the number of ancilla qubits is super-linear, a direct classical simulation becomes super-polynomial!
- Various universal quantum gate sets.
    - For some results we only know how to start with a certain gate set.
    - Although we can use Solovay-Kitaev theorem to generalize other gate sets, this causes overhead in circuit complexity.

Special Properties in the Quantum Setting

Special Properties in the Quantum Setting

With a focus on quantum states

SMCSP

SMCSP

- **Input:**

SMCSP

- **Input:**
  - Arbitrarily many copies of an n-qubit state $|\psi\rangle$.

SMCSP

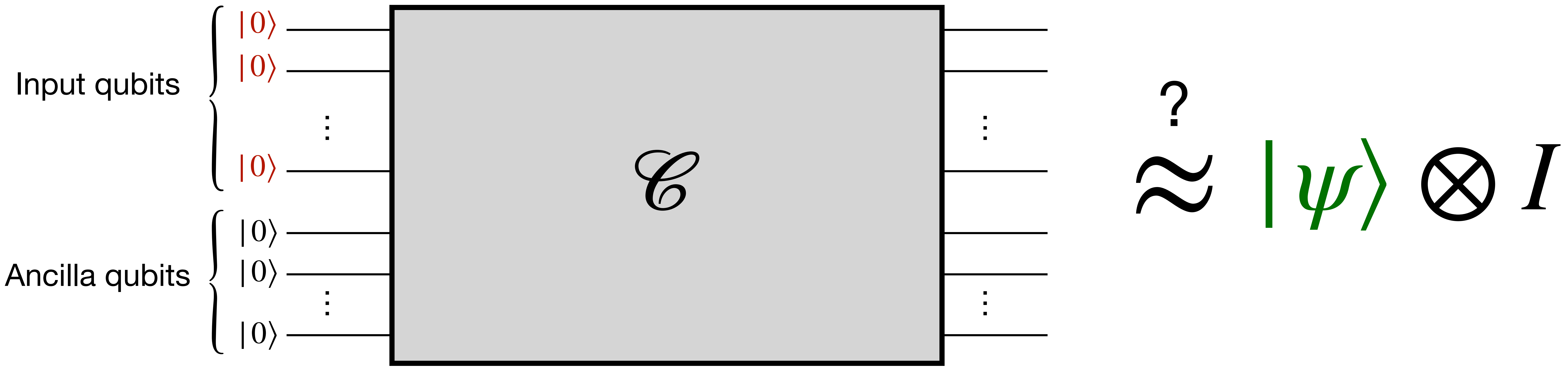
- **Input:**
  - Arbitrarily many copies of an n-qubit state $|\psi\rangle$.
  - Size parameter: s.

SMCSP

- **Input:**
  - Arbitrarily many copies of an n-qubit state $|\psi\rangle$.
  - Size parameter: s.
- **Goal:** Determine if ∃ circuit $\mathscr{C}$ of size $\leq s$, s.t. $\|(\langle\psi| \otimes I)\mathscr{C}\,|0^{n+t}\rangle\| \approx 1$.

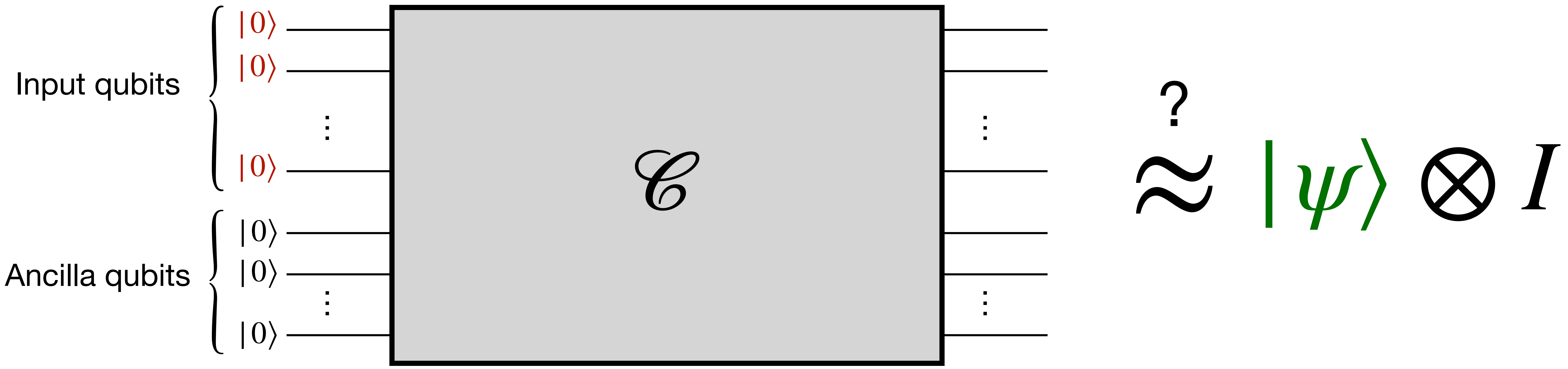
SMCSP

- **Input:**
  - Arbitrarily many copies of an n-qubit state $|\psi\rangle$.
  - Size parameter: s.
- **Goal:** Determine if $\exists$ circuit $\mathscr{C}$ of size $\leq s$, s.t. $\|(\langle\psi| \otimes I)\mathscr{C}\,|0^{n+t}\rangle\| \approx 1$.



SMCSP

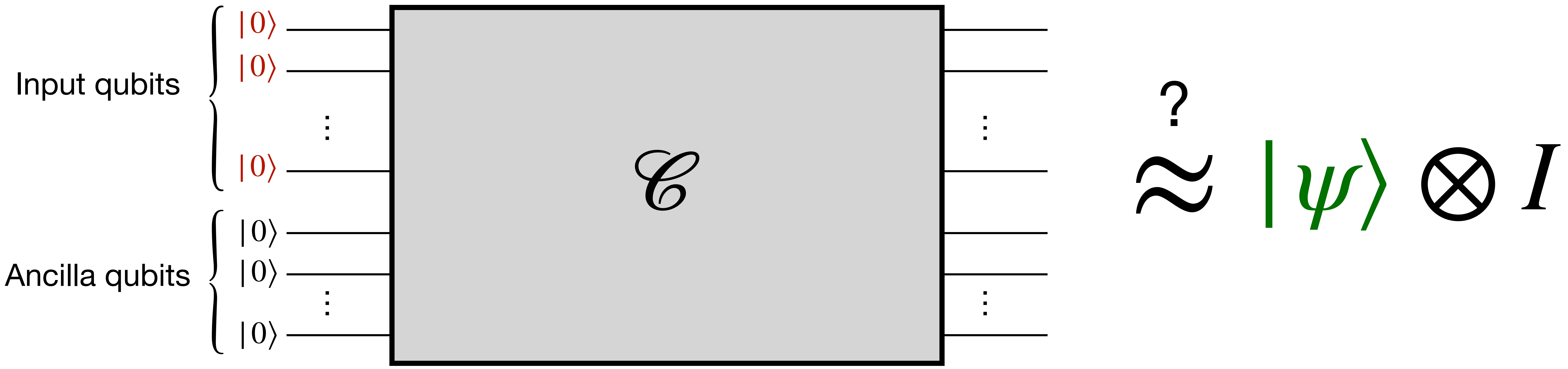
- **Input:**
  - Arbitrarily many copies of an n-qubit state $|\psi\rangle$.
  - Size parameter: s.
- **Goal:** Determine if $\exists$ circuit $\mathscr{C}$ of size $\leq s$, s.t. $\|(\langle\psi| \otimes I)\mathscr{C}\,|0^{n+t}\rangle\| \approx 1$.



- **Remark 1:** Can define a version with “classical description” of $|\psi\rangle$ as the input.

SMCSP

- **Input:**
  - Arbitrarily many copies of an n-qubit state $|\psi\rangle$.
  - Size parameter: s.
- **Goal:** Determine if $\exists$ circuit $\mathscr{C}$ of size $\leq s$, s.t. $\|(\langle\psi| \otimes I)\mathscr{C}|0^{n+t}\rangle\| \approx 1$.



- **Remark 1:** Can define a version with "classical description" of $|\psi\rangle$ as the input.
- **Remark 2:** Can define a version for unitary transformation analogously.

Quantum-Unique Reductions

Quantum-Unique Reductions

- Search-to-decision reduction for SMCSP and UMCSP.

Quantum-Unique Reductions

- Search-to-decision reduction for SMCSP and UMCSP.
- Self reduction for SMCSP.

Quantum-Unique Reductions

- Search-to-decision reduction for SMCSP and UMCSP.
- Self reduction for SMCSP.
- Gap-MQCSP reduces to UMCSP.

Quantum-Unique Reductions

- Search-to-decision reduction for SMCSP and UMCSP.
- Self reduction for SMCSP.
- Gap-MQCSP reduces to UMCSP.
- **Key ideas:** Leveraging the "reversibility" of quantum circuits!

Quantum-Unique Reductions

- Search-to-decision reduction for SMCSP and UMCSP.
- Self reduction for SMCSP.
- Gap-MQCSP reduces to UMCSP.
- **Key ideas:** Leveraging the "reversibility" of quantum circuits!

Input: $|\psi\rangle$

Quantum-Unique Reductions

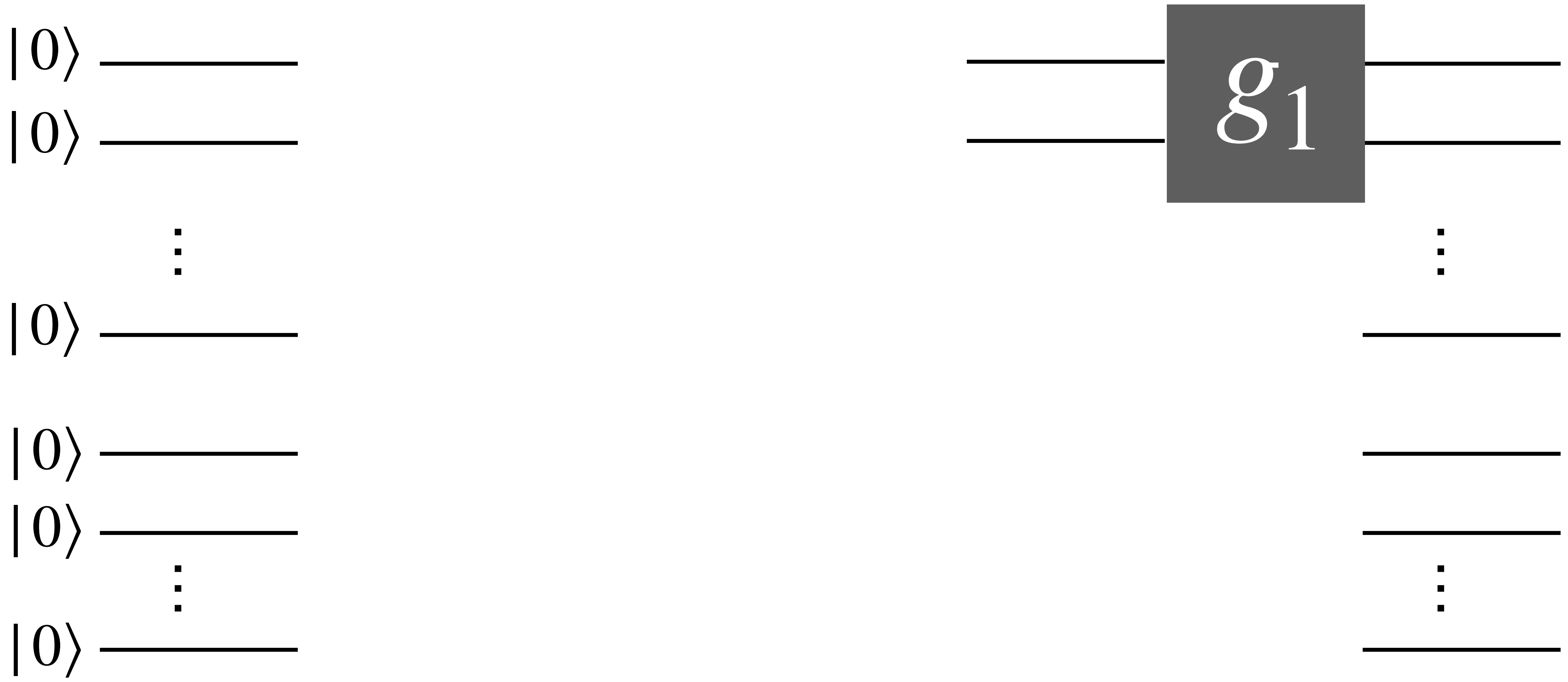
- Search-to-decision reduction for SMCSP and UMCSP.
- Self reduction for SMCSP.
- Gap-MQCSP reduces to UMCSP.
- **Key ideas:** Leveraging the "reversibility" of quantum circuits!

SMCSP

Input: $|\psi\rangle$

Quantum-Unique Reductions

- Search-to-decision reduction for SMCSP and UMCSP.
- Self reduction for SMCSP.
- Gap-MQCSP reduces to UMCSP.
- **Key ideas:** Leveraging the "reversibility" of quantum circuits!

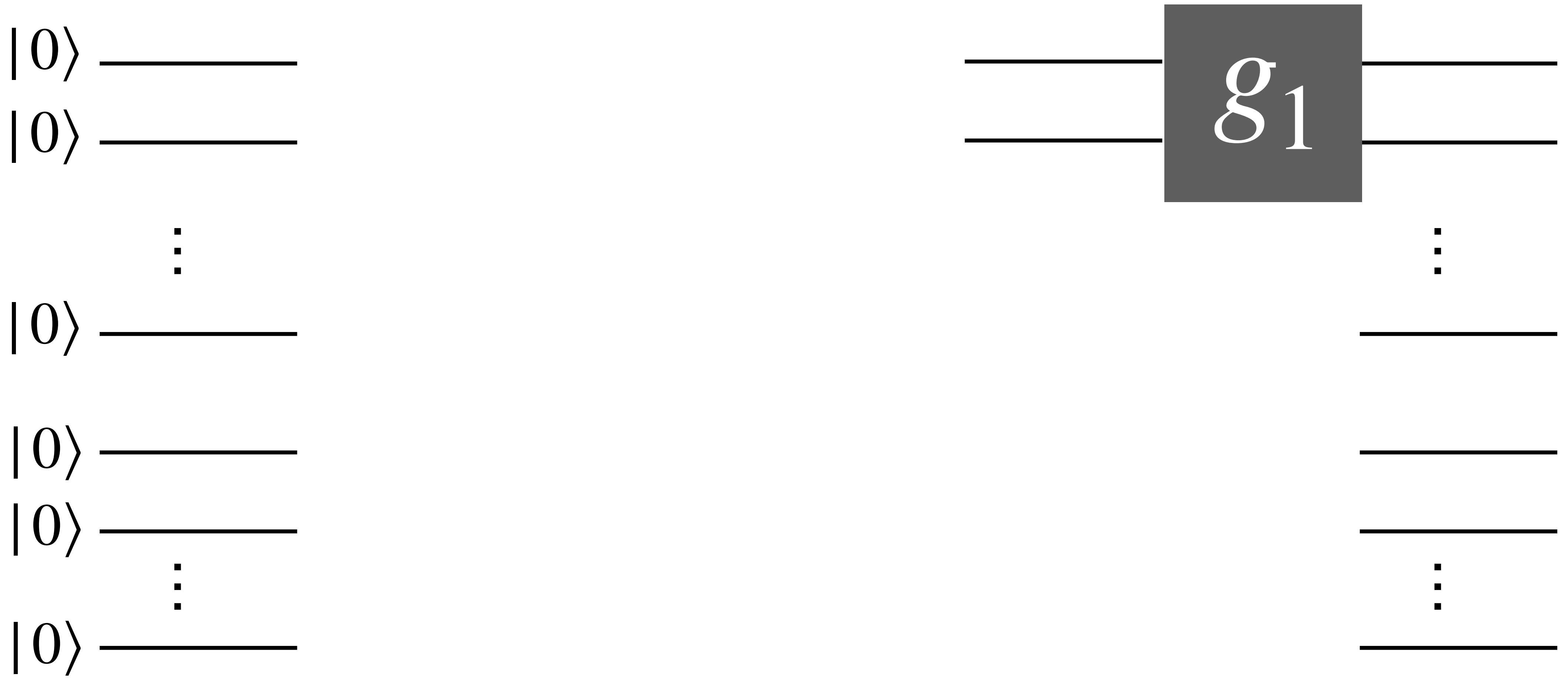


SMCSP

Input: $|\psi\rangle$

Quantum-Unique Reductions

- Search-to-decision reduction for SMCSP and UMCSP.
- Self reduction for SMCSP.
- Gap-MQCSP reduces to UMCSP.
- **Key ideas:** Leveraging the "reversibility" of quantum circuits!



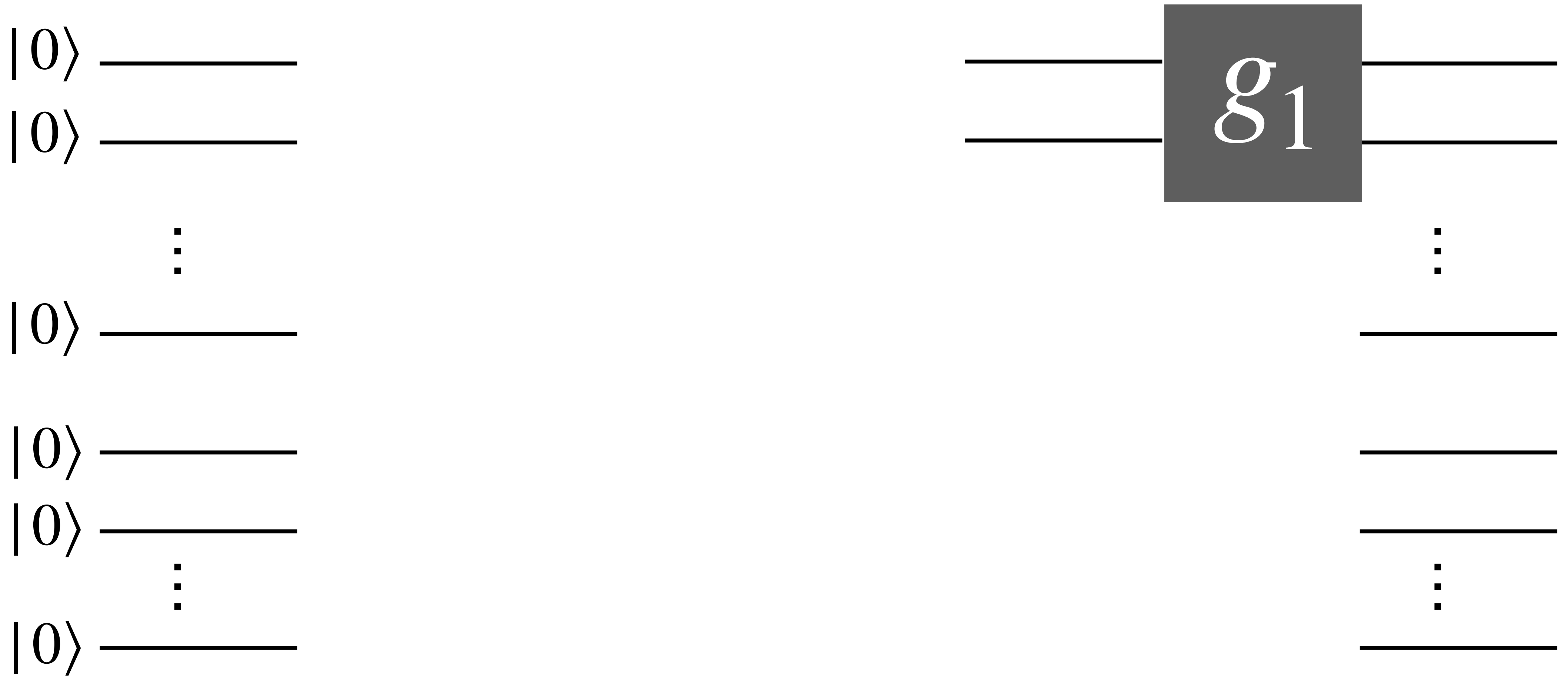
SMCSP

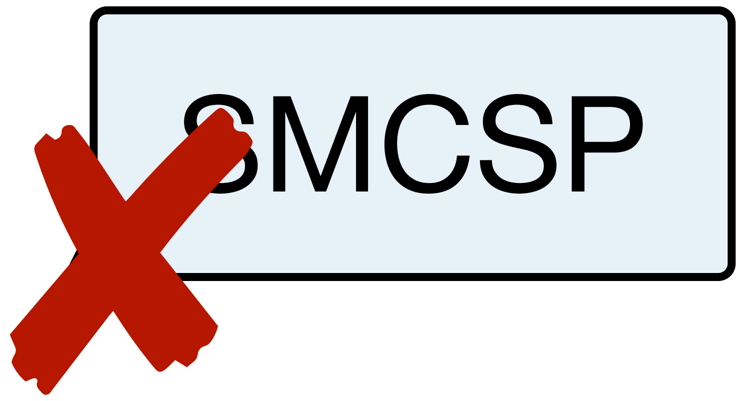
$$(g_1^{-1}|\psi\rangle, s-1)$$

Input: $|\psi\rangle$

Quantum-Unique Reductions

- Search-to-decision reduction for SMCSP and UMCSP.
- Self reduction for SMCSP.
- Gap-MQCSP reduces to UMCSP.
- **Key ideas:** Leveraging the "reversibility" of quantum circuits!



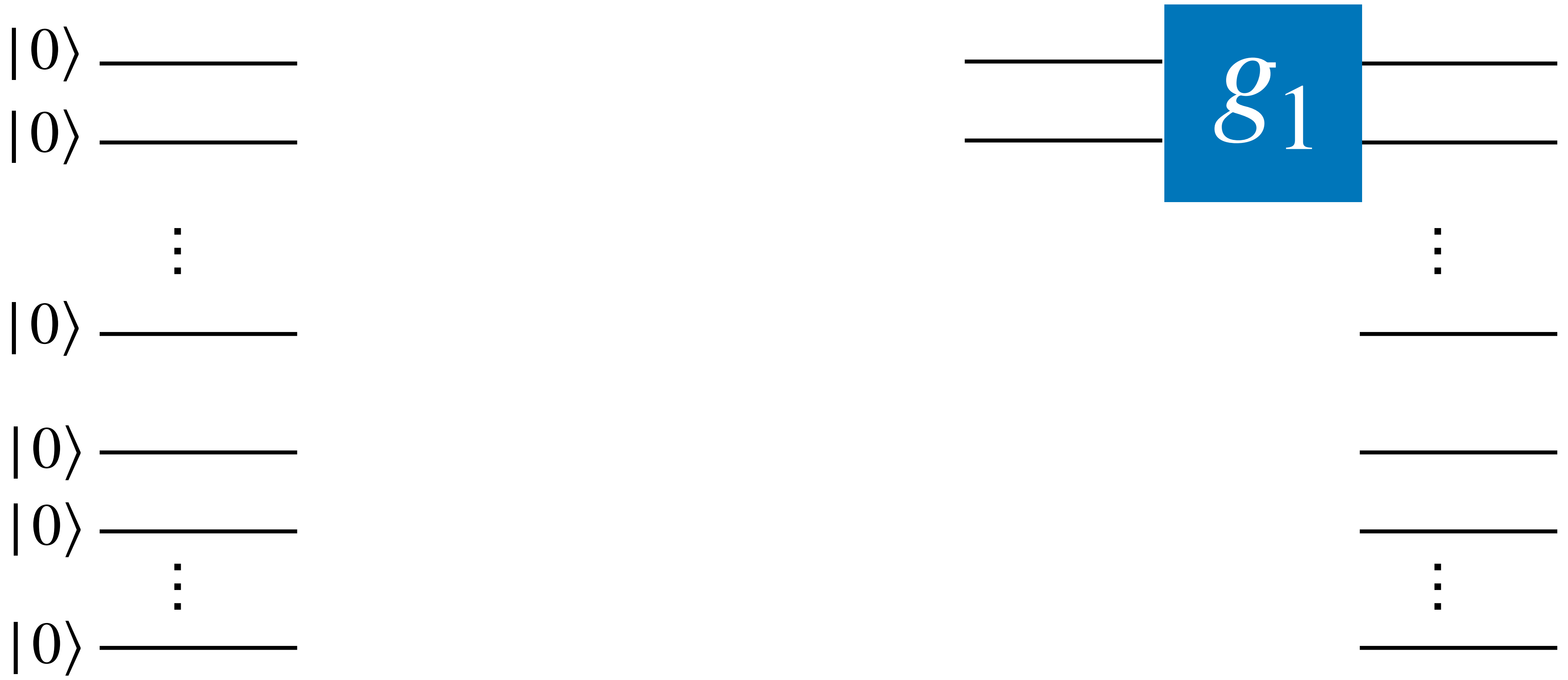


$$(g_1^{-1}|\psi\rangle, s-1)$$

Input: $|\psi\rangle$

Quantum-Unique Reductions

- Search-to-decision reduction for SMCSP and UMCSP.
- Self reduction for SMCSP.
- Gap-MQCSP reduces to UMCSP.
- **Key ideas:** Leveraging the "reversibility" of quantum circuits!



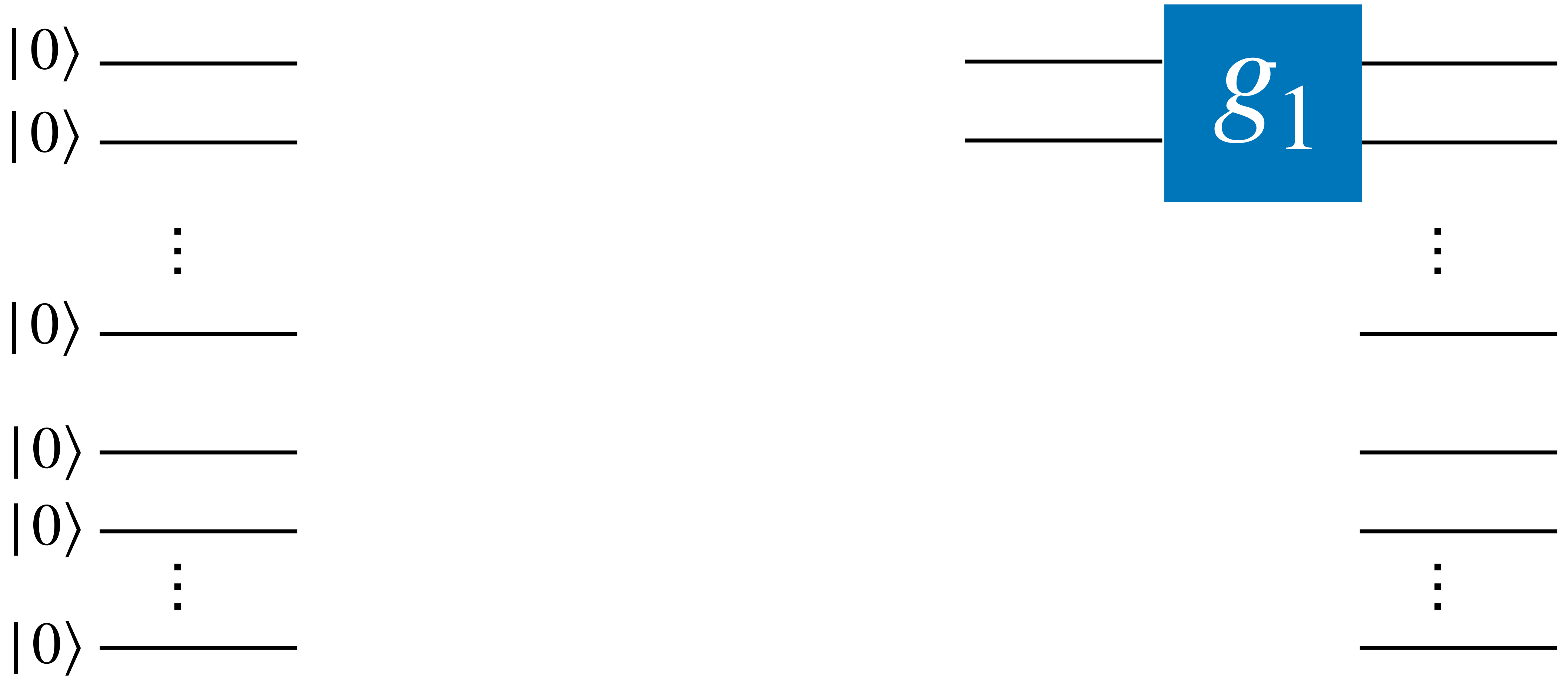
SMCSP

$(g_1^{-1}|\psi\rangle, s-1)$

Input: $|\psi\rangle$

Quantum-Unique Reductions

- Search-to-decision reduction for SMCSP and UMCSP.
- Self reduction for SMCSP.
- Gap-MQCSP reduces to UMCSP.
- **Key ideas:** Leveraging the “reversibility” of quantum circuits!



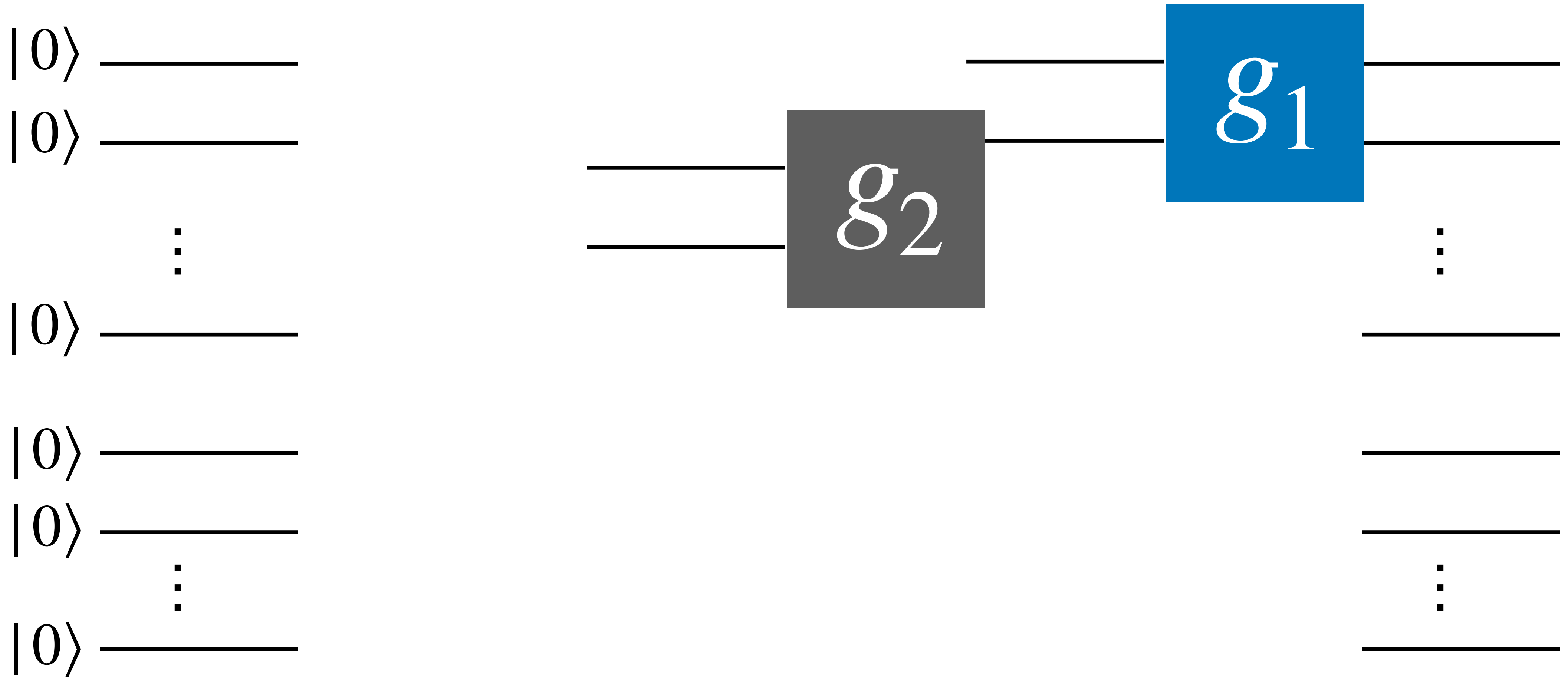
SMCSP ✓

$$(g_1^{-1}|\psi\rangle, s-1)$$

Input: $|\psi\rangle$

Quantum-Unique Reductions

- Search-to-decision reduction for SMCSP and UMCSP.
- Self reduction for SMCSP.
- Gap-MQCSP reduces to UMCSP.
- **Key ideas:** Leveraging the “reversibility” of quantum circuits!



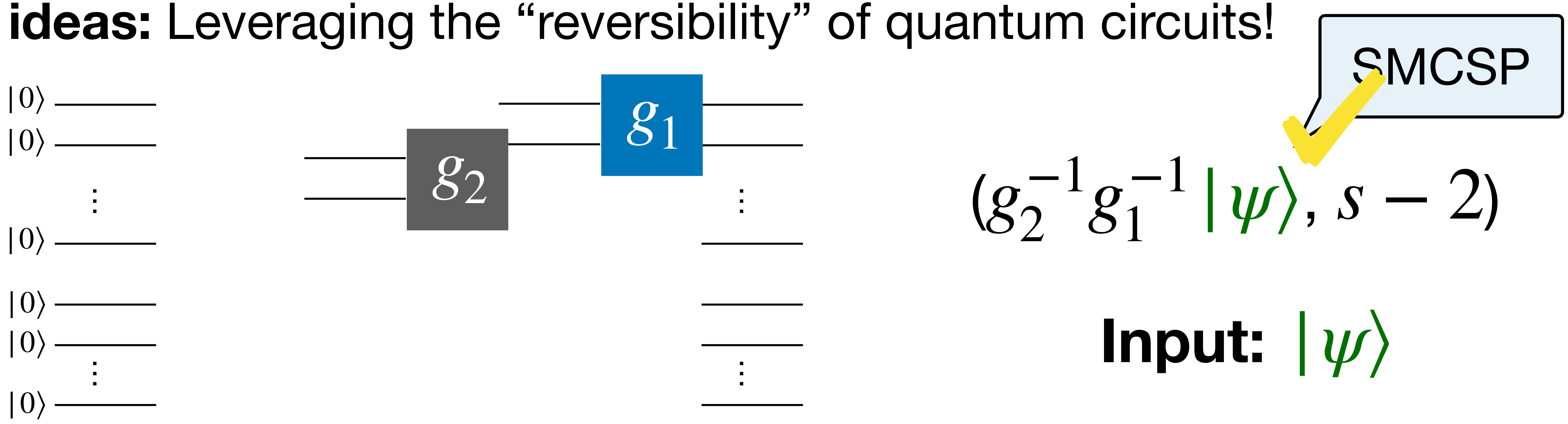
SMCSP

$$(g_2^{-1} g_1^{-1} |\psi\rangle, s - 2)$$

Input: $|\psi\rangle$

Quantum-Unique Reductions

- Search-to-decision reduction for SMCSP and UMCSP.
- Self reduction for SMCSP.
- Gap-MQCSP reduces to UMCSP.
- **Key ideas:** Leveraging the "reversibility" of quantum circuits!

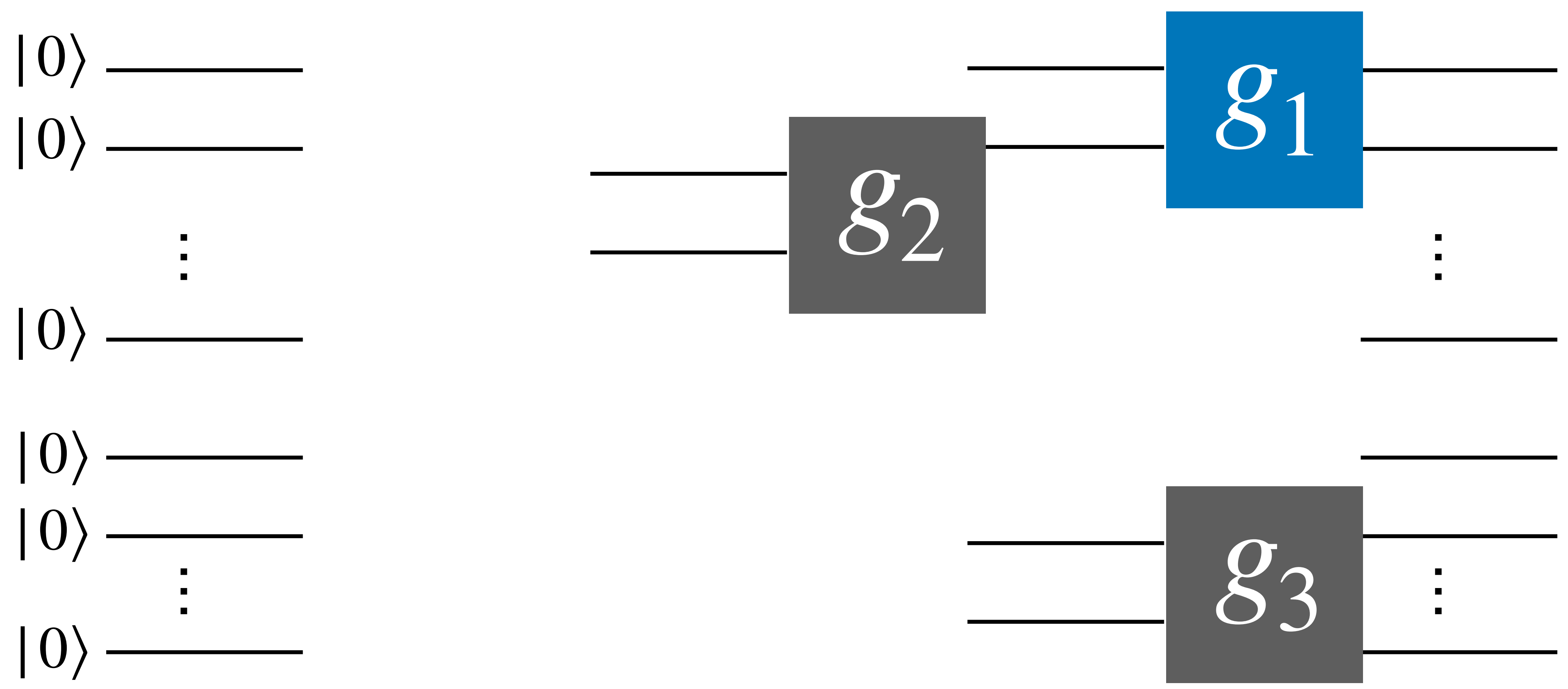


$$(g_2^{-1} g_1^{-1} |\psi\rangle, s - 2)$$

Input: $|\psi\rangle$

Quantum-Unique Reductions

- Search-to-decision reduction for SMCSP and UMCSP.
- Self reduction for SMCSP.
- Gap-MQCSP reduces to UMCSP.
- **Key ideas:** Leveraging the "reversibility" of quantum circuits!



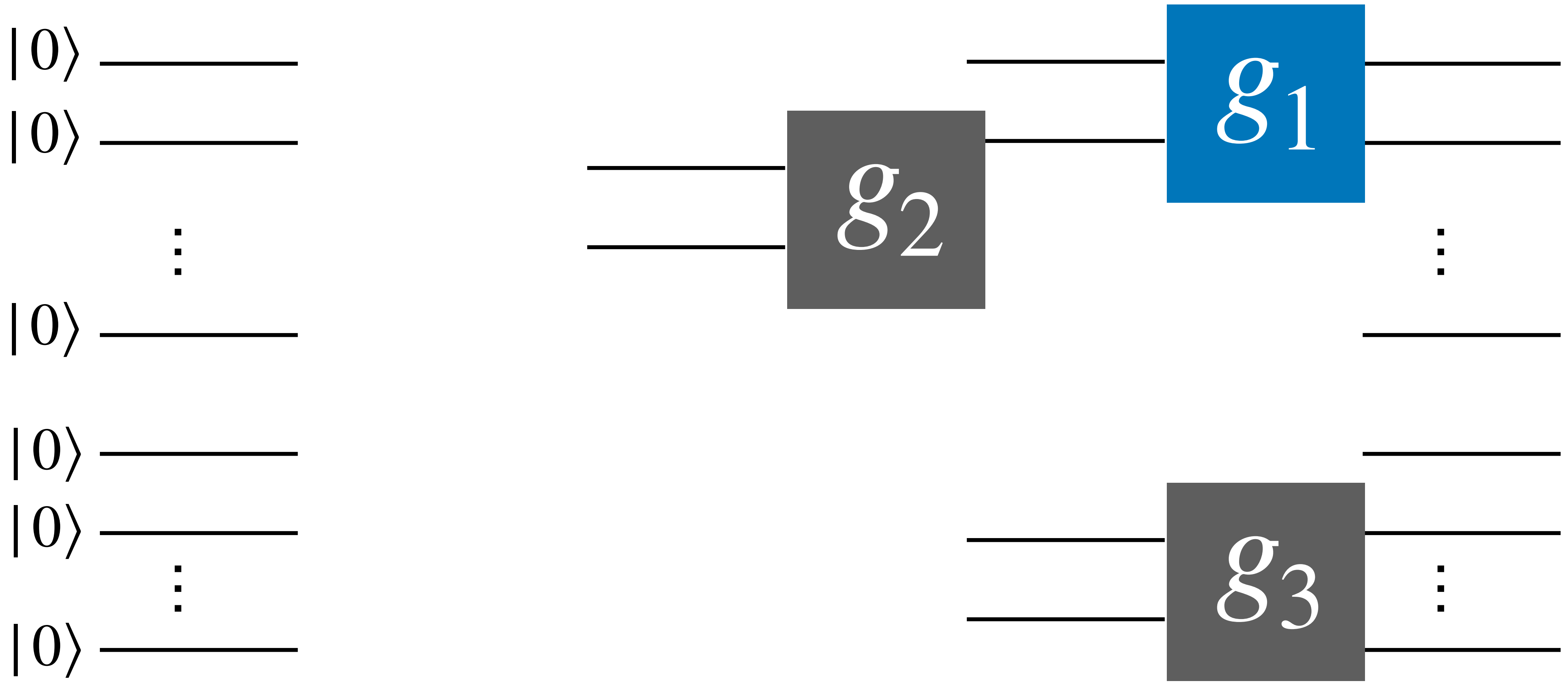
SMCSP

$$(g_3^{-1} g_2^{-1} g_1^{-1} |\psi\rangle, s - 3)$$

Input: $|\psi\rangle$

Quantum-Unique Reductions

- Search-to-decision reduction for SMCSP and UMCSP.
- Self reduction for SMCSP.
- Gap-MQCSP reduces to UMCSP.
- **Key ideas:** Leveraging the "reversibility" of quantum circuits!



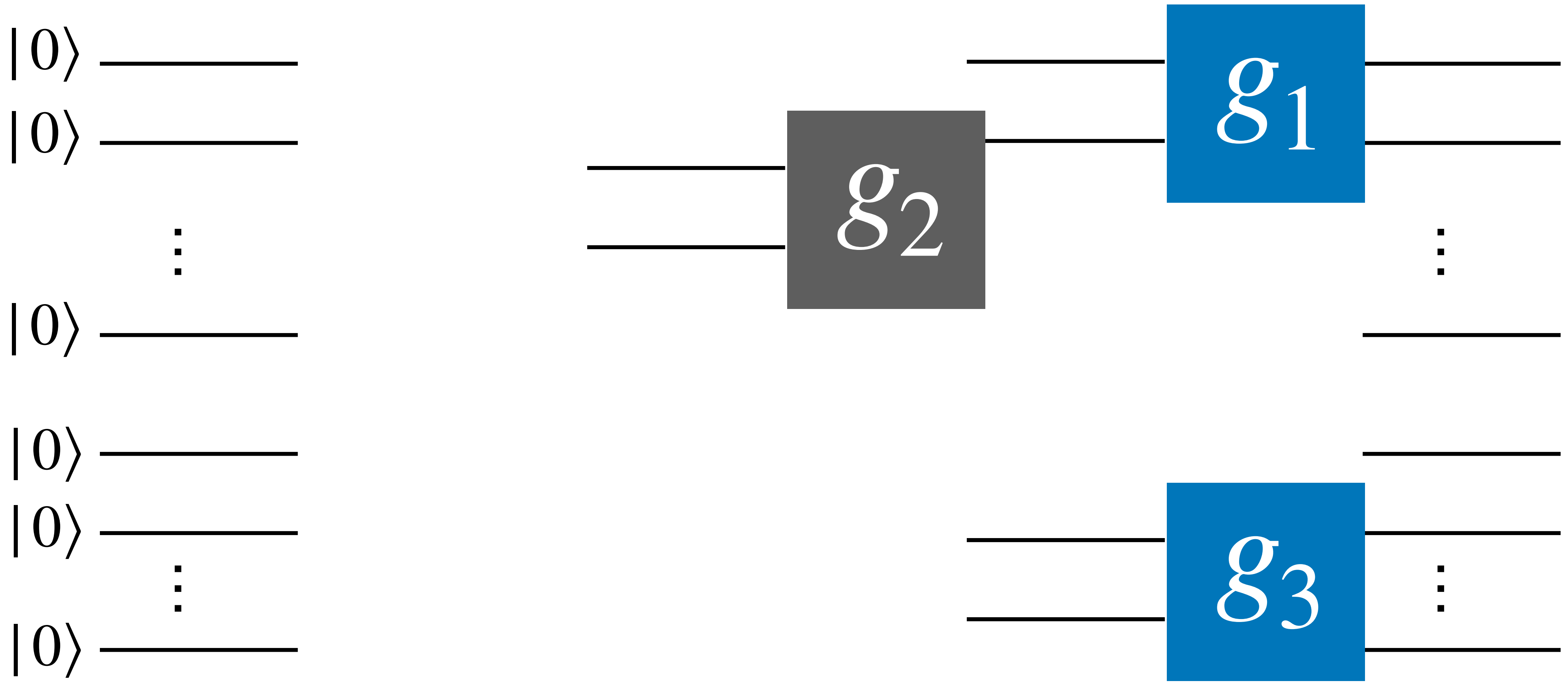
SMCSP

$$(g_3^{-1} g_2^{-1} g_1^{-1} |\psi\rangle, s - 3)$$

Input: $|\psi\rangle$

Quantum-Unique Reductions

- Search-to-decision reduction for SMCSP and UMCSP.
- Self reduction for SMCSP.
- Gap-MQCSP reduces to UMCSP.
- **Key ideas:** Leveraging the “reversibility” of quantum circuits!



SMCSP

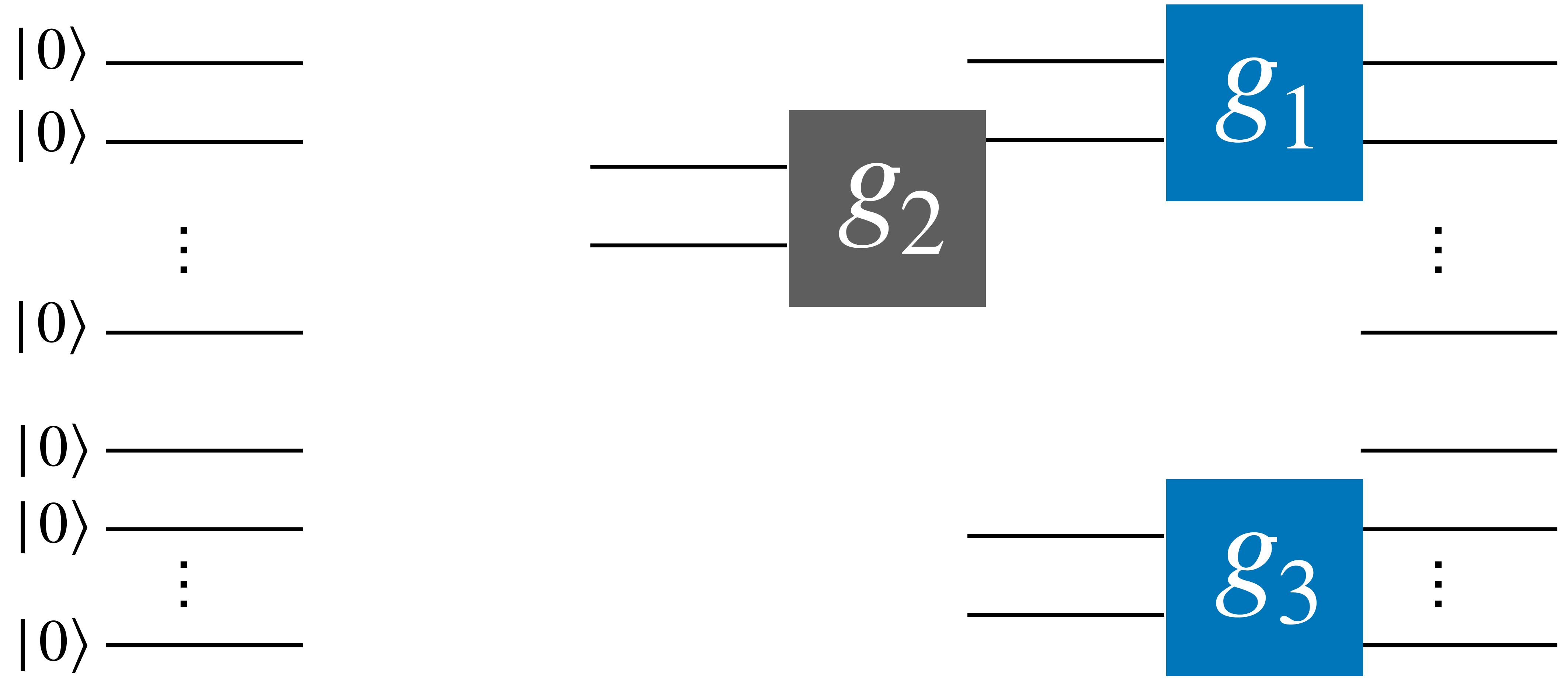
$$(g_3^{-1} g_2^{-1} g_1^{-1} |\psi\rangle, s - 3)$$

Input: $|\psi\rangle$

Quantum-Unique Reductions

- Search-to-decision reduction for SMCSP and UMCSP.
- Self reduction for SMCSP.
- Gap-MQCSP reduces to UMCSP.
- **Key ideas:** Leveraging the "reversibility" of quantum circuits!

It becomes more subtle when considering error…



SMCSP

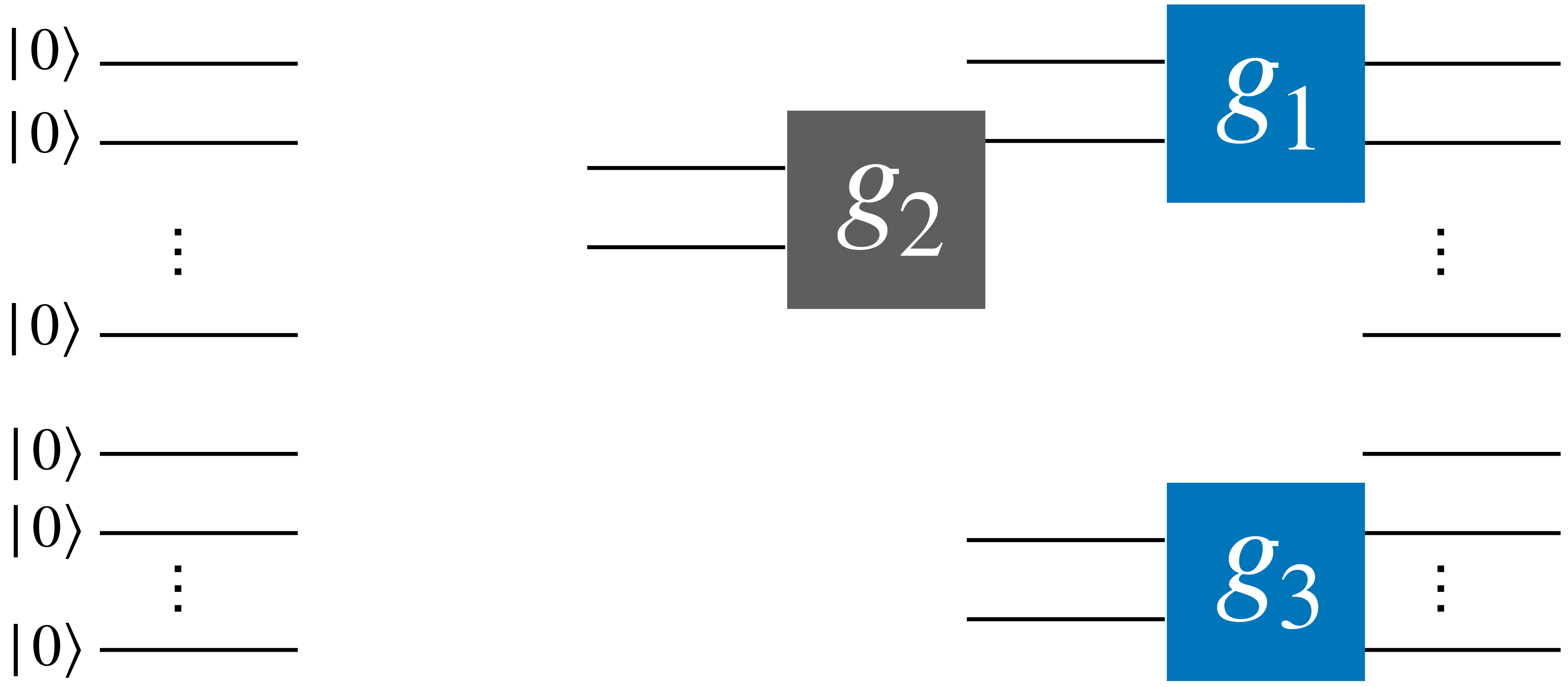
$$(g_3^{-1} g_2^{-1} g_1^{-1} |\psi\rangle, s-3)$$

Input: $|\psi\rangle$

Quantum-Unique Reductions

- Search-to-decision reduction for SMCSP and UMCSP.
- Self reduction for SMCSP.
- Gap-MQCSP reduces to UMCSP.
- **Key ideas:** Leveraging the "reversibility" of quantum circuits!

It becomes more subtle when considering error…



SMCSP

$$(g_3^{-1} g_2^{-1} g_1^{-1} |\psi\rangle, s-3)$$

Input: $|\psi\rangle$

- **Open problems:** Any application of these quantum-unique reductions?

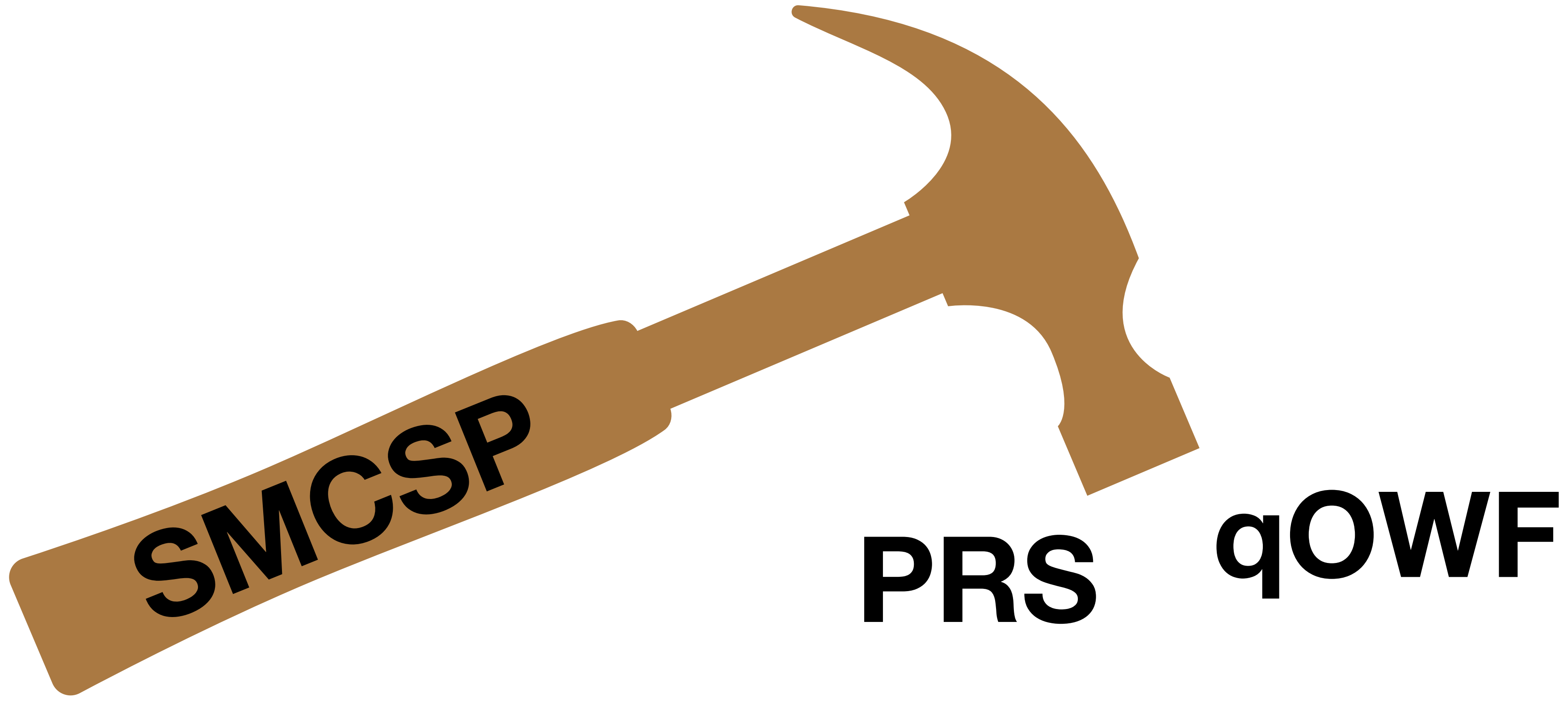
More!

More!

- SMCSP breaks pseudorandom states and quantum OWF.

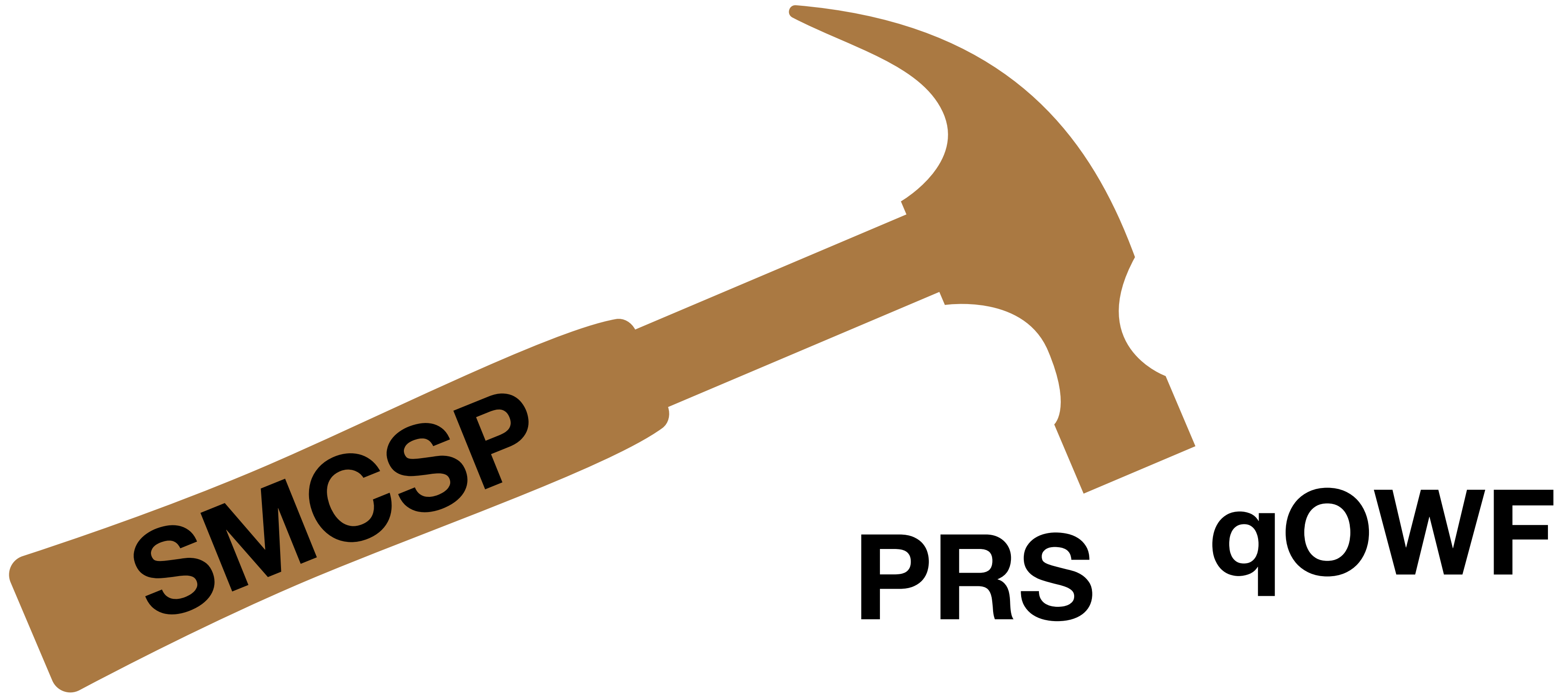
More!

- SMCSP breaks pseudorandom states and quantum OWF.



More!

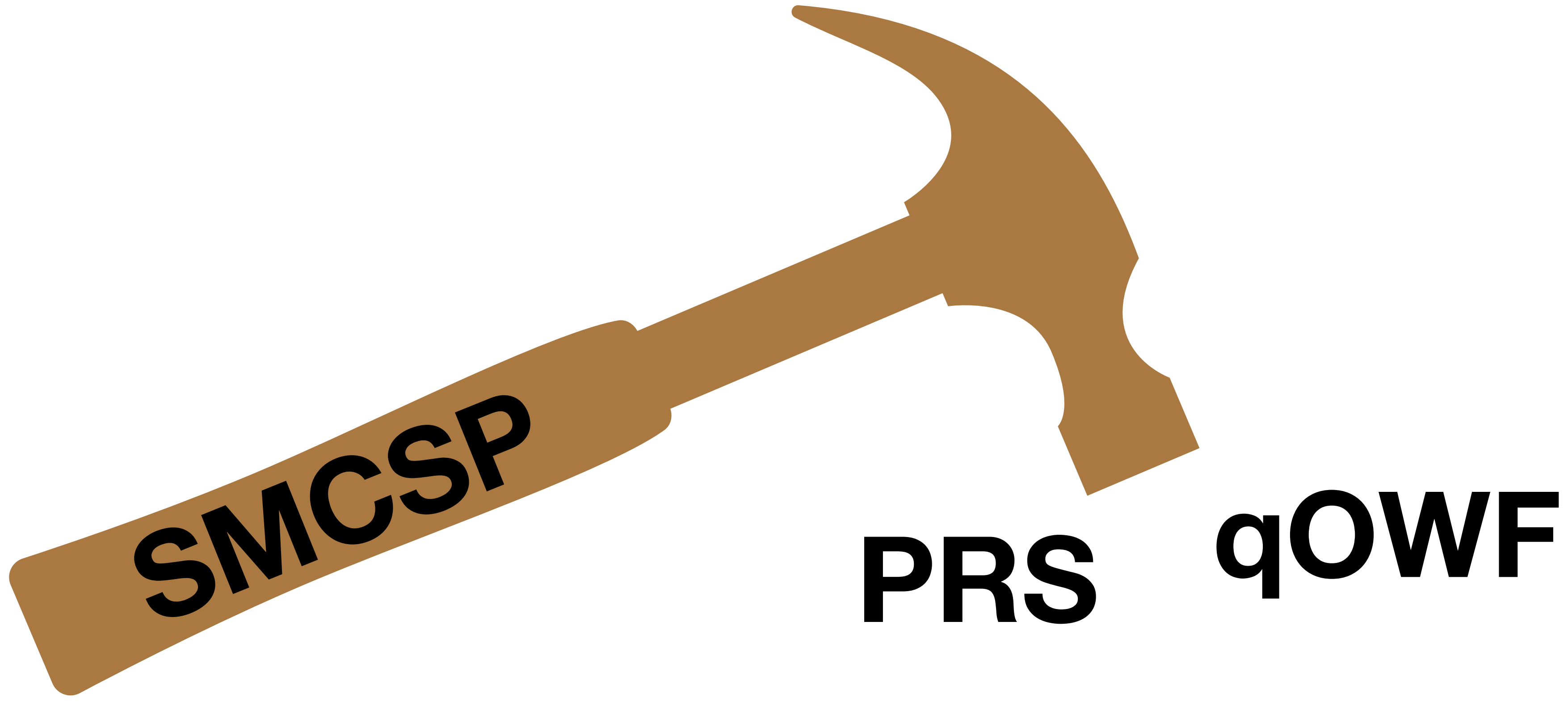
- SMCSP breaks pseudorandom states and quantum OWF.



- Solving SMCSP is “equivalent” to estimating the wormhole volume under common assumptions/conjectures.

More!

- SMCSP breaks pseudorandom states and quantum OWF.

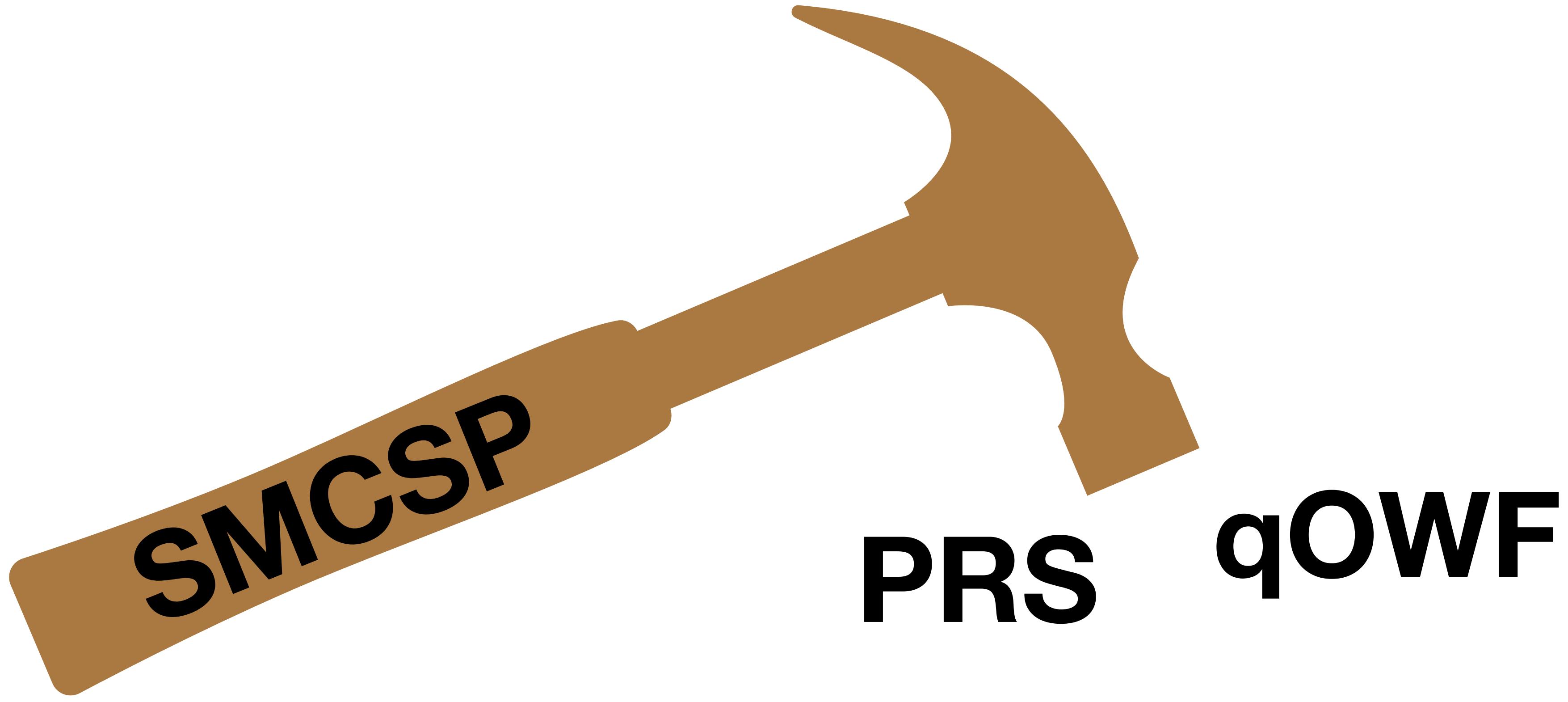


- Solving SMCSP is “equivalent” to estimating the wormhole volume under common assumptions/conjectures.

The volume of a wormhole

More!

- SMCSP breaks pseudorandom states and quantum OWF.

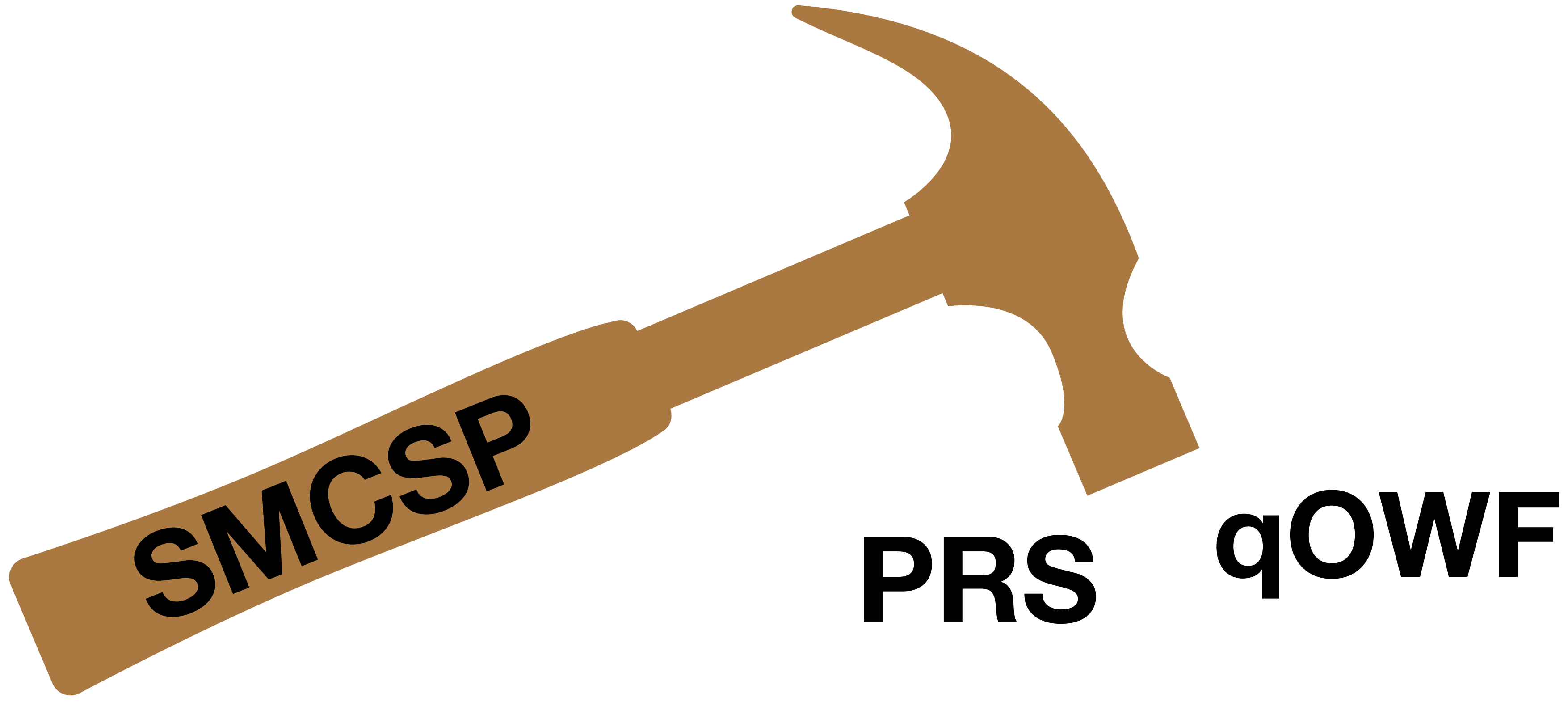


- Solving SMCSP is “equivalent” to estimating the wormhole volume under common assumptions/conjectures.

The volume of a wormhole $\approx$ (Volume=Complexity Conjecture [Susskind’16]) **The complexity of “thermalfield double state”**

More!

- SMCSP breaks pseudorandom states and quantum OWF.

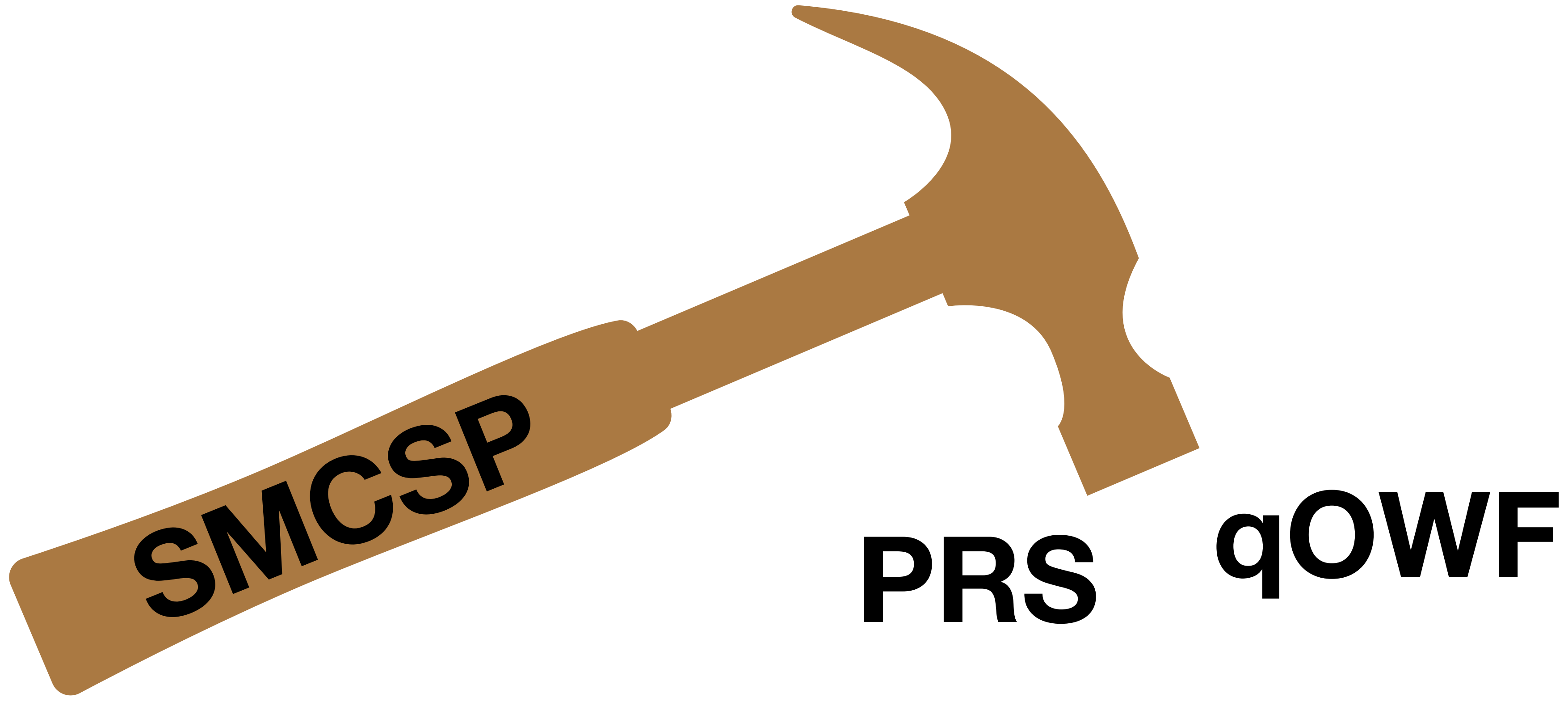


- Solving SMCSP is “equivalent” to estimating the wormhole volume under common assumptions/conjectures.

The volume of a wormhole $\approx$ (Volume=Complexity Conjecture [Susskind’16]) **The complexity of “thermalfield double state”** (Assuming a dictionary map in AdS/CFT is efficiently computable)

More!

- SMCSP breaks pseudorandom states and quantum OWF.

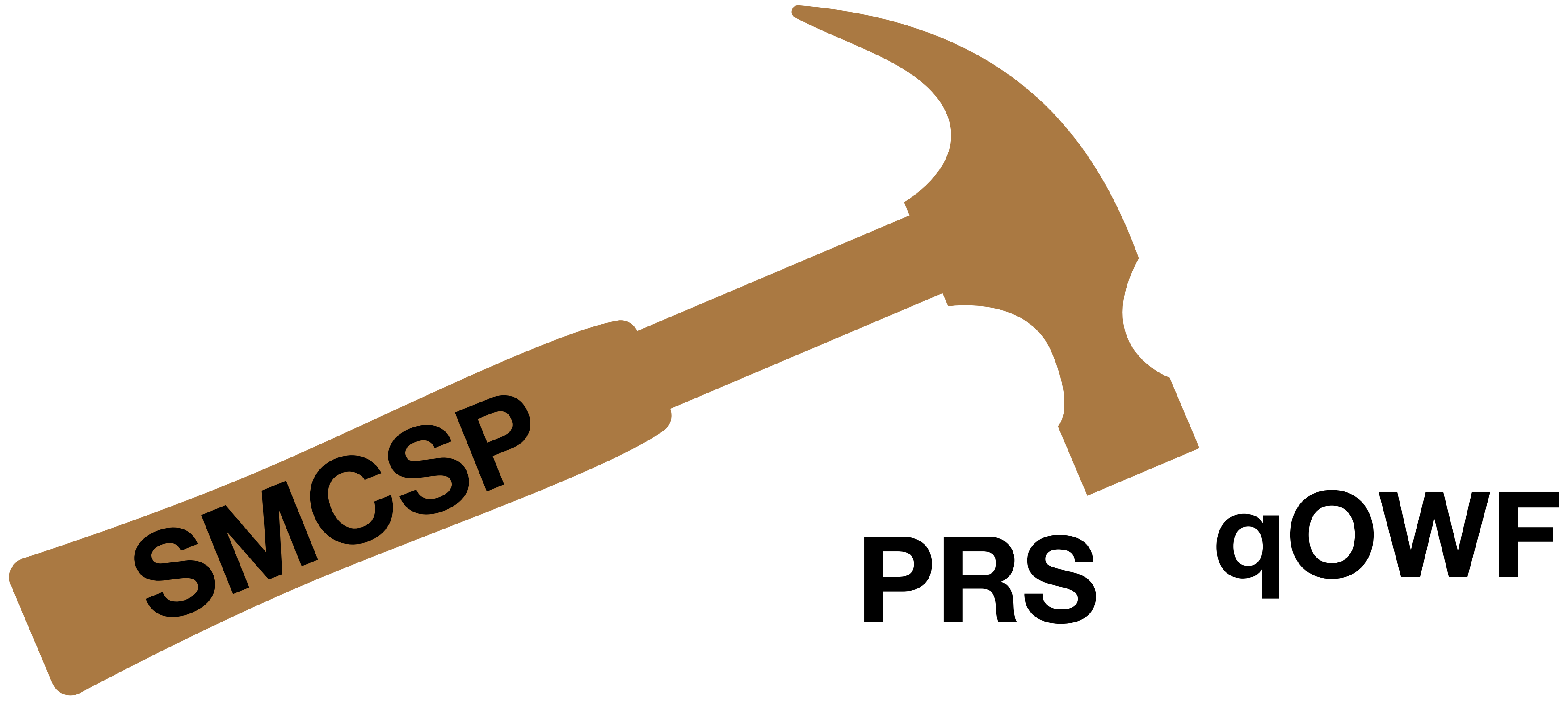


- Solving SMCSP is “equivalent” to estimating the wormhole volume under common assumptions/conjectures.

The volume of a wormhole $\approx$ (Volume=Complexity Conjecture [Susskind’16]) **The complexity of “thermalfield double state”** ← (Assuming a dictionary map in AdS/CFT is efficiently computable) **SMCSP**

More!

- SMCSP breaks pseudorandom states and quantum OWF.



- Solving SMCSP is “equivalent” to estimating the wormhole volume under common assumptions/conjectures.

The volume of a wormhole

Volume=Complexity Conjecture [Susskind’16]

$\approx$

The complexity of “thermalfield double state”

← **SMCSP**

Assuming a dictionary map in AdS/CFT is efficiently computable

→ **CFT-SMCSP**

Summary & Future Directions

Summary

Summary

Minimum quantum circuits for Boolean functions

- Formulate MQCSP.
- Basic complexity properties of MQCSP.
- Connections to other areas such as circuit lower bounds, learning theory, cryptography, etc.

Summary

Minimum quantum circuits for Boolean functions

- Formulate MQCSP.
- Basic complexity properties of MQCSP.
- Connections to other areas such as circuit lower bounds, learning theory, cryptography, etc.

Minimum quantum circuits for quantum objects

- Formulate SMCSP and UMCSP.
- Search-to-decision and self reductions.
- Quantum-related applications (e.g., pseudorandom state, quantum gravity).

Summary

Minimum quantum circuits for Boolean functions

- Formulate MQCSP.
- Basic complexity properties of MQCSP.
- Connections to other areas such as circuit lower bounds, learning theory, cryptography, etc.

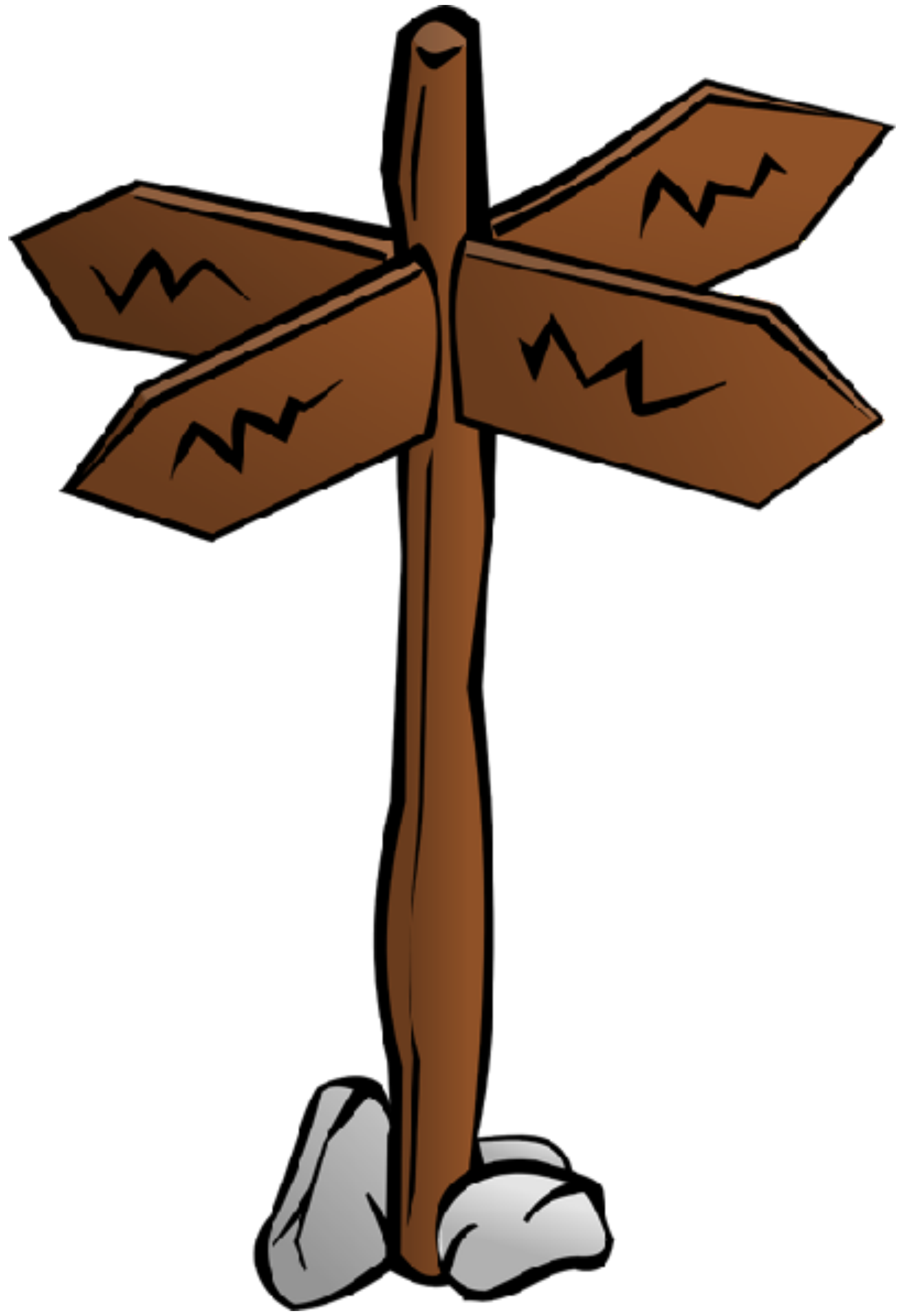
Minimum quantum circuits for quantum objects

- Formulate SMCSP and UMCSP.
- Search-to-decision and self reductions.
- Quantum-related applications (e.g., pseudorandom state, quantum gravity).

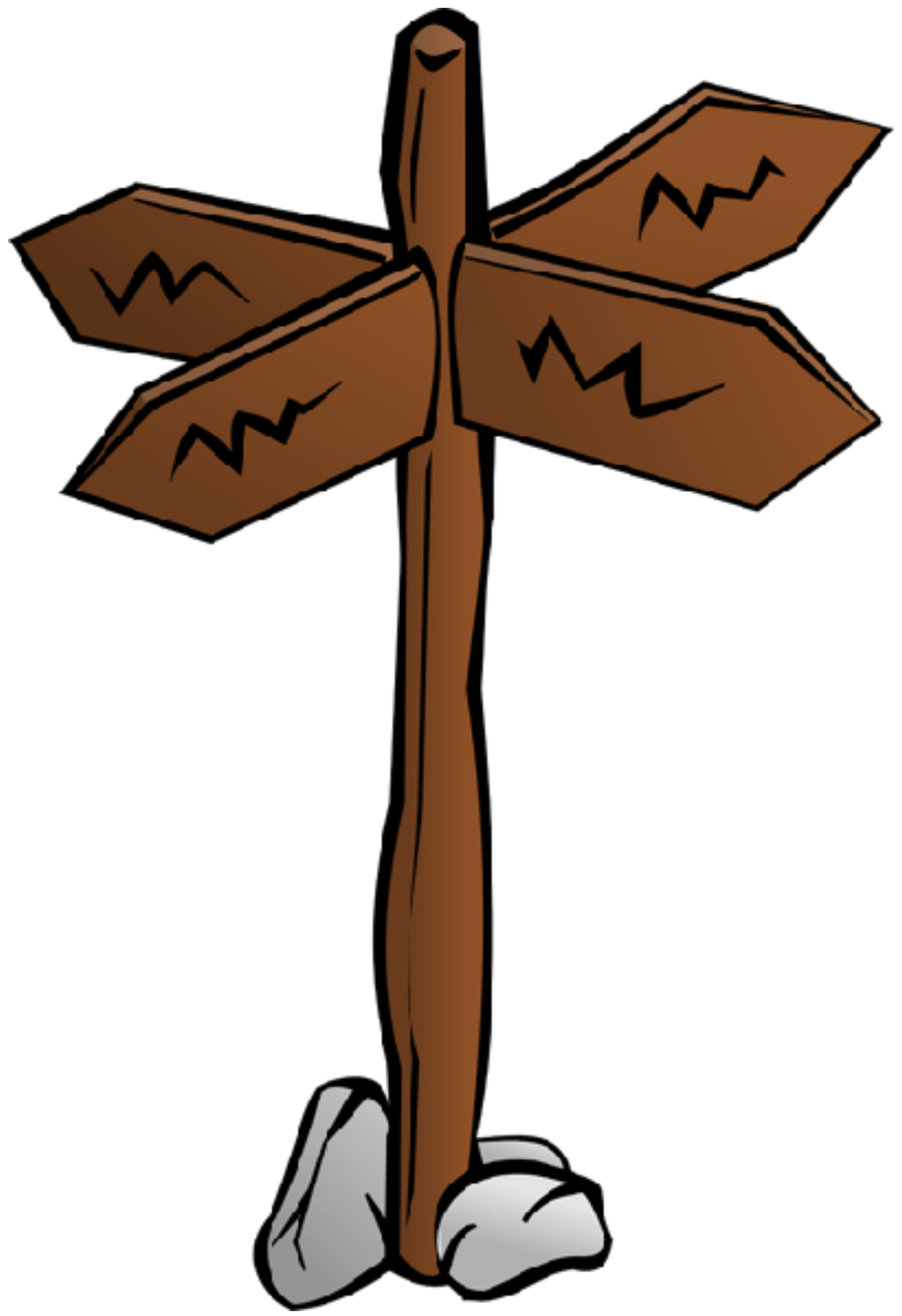
Quantum algorithms and reductions for (quantum) MCSPs

- Implications of quantum algorithms for (quantum) MCSPs.
- A quantum search-to-decision reduction for SMCSP.

Future Directions



Future Directions



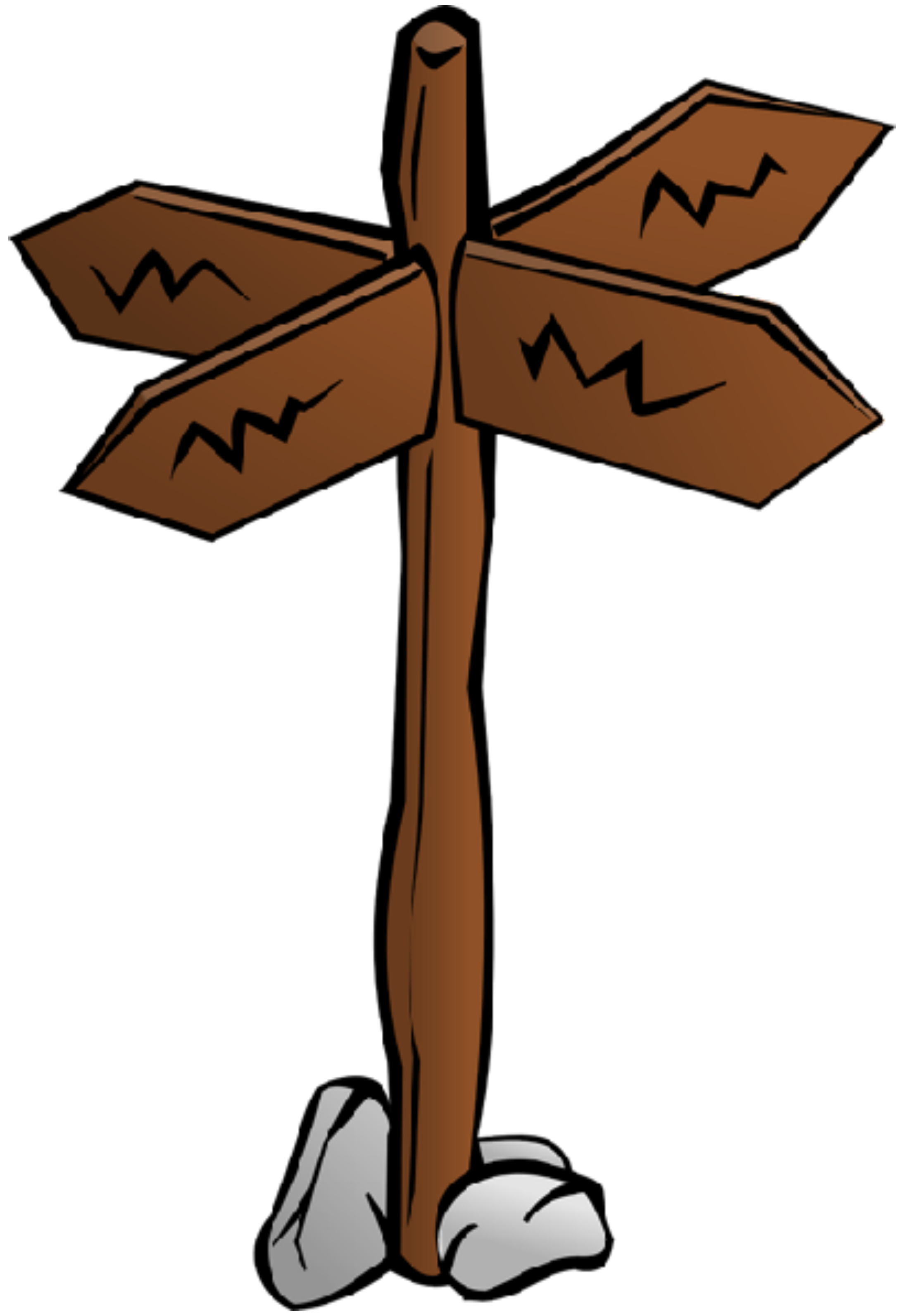
Classical upper bounds

- Is MQCSP, SMCSP, UMCSP in NP?
- It seems to be challenging to handle super-linear number of ancilla qubits.

Future Directions

Classical upper bounds

- Is MQCSP, SMCSP, UMCSP in NP?
- It seems to be challenging to handle super-linear number of ancilla qubits.



Applications of the quantum-unique reductions?

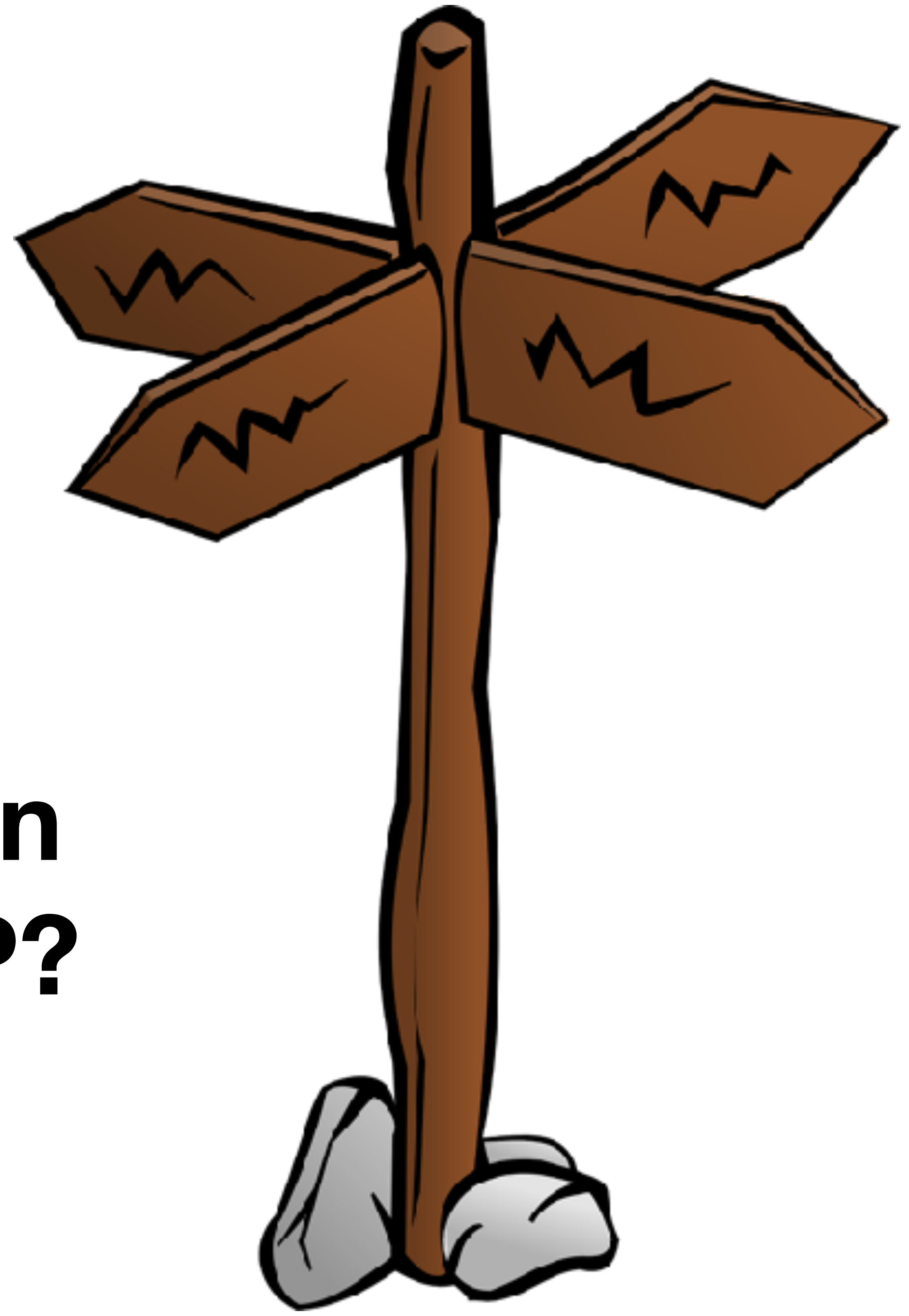
Future Directions

Classical upper bounds

- Is MQCSP, SMCSP, UMCSP in NP?
- It seems to be challenging to handle super-linear number of ancilla qubits.

Are there search-to-decision or self reduction for MQCSP?

- Due to the boolean structure, the straightforward idea doesn't work.



Applications of the quantum-unique reductions?

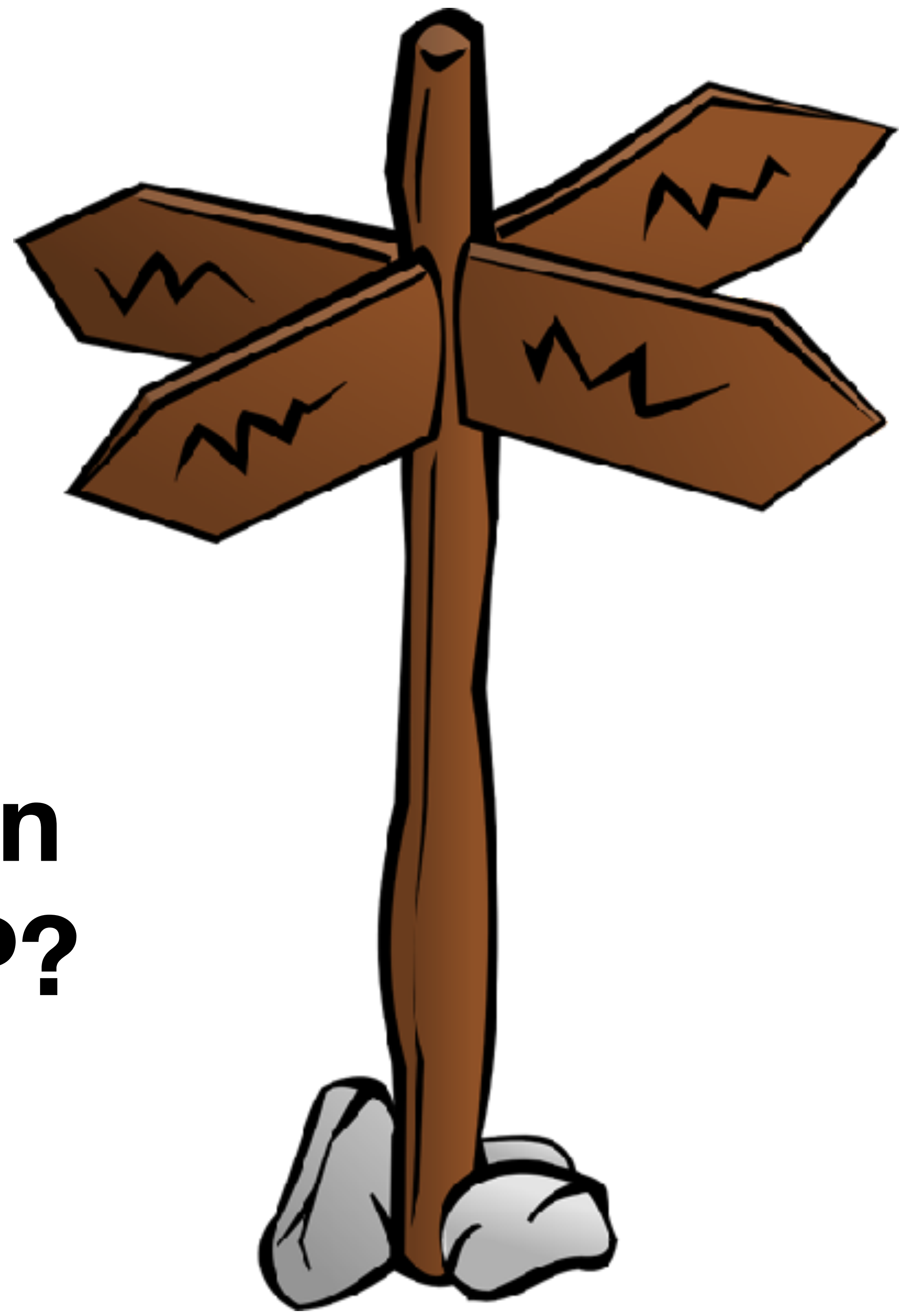
Future Directions

Classical upper bounds

- Is MQCSP, SMCSP, UMCSP in NP?
- It seems to be challenging to handle super-linear number of ancilla qubits.

Are there search-to-decision or self reduction for MQCSP?

- Due to the boolean structure, the straightforward idea doesn't work.



Applications of the quantum-unique reductions?

Can we base the security of crypto primitives on quantum MCSPs?

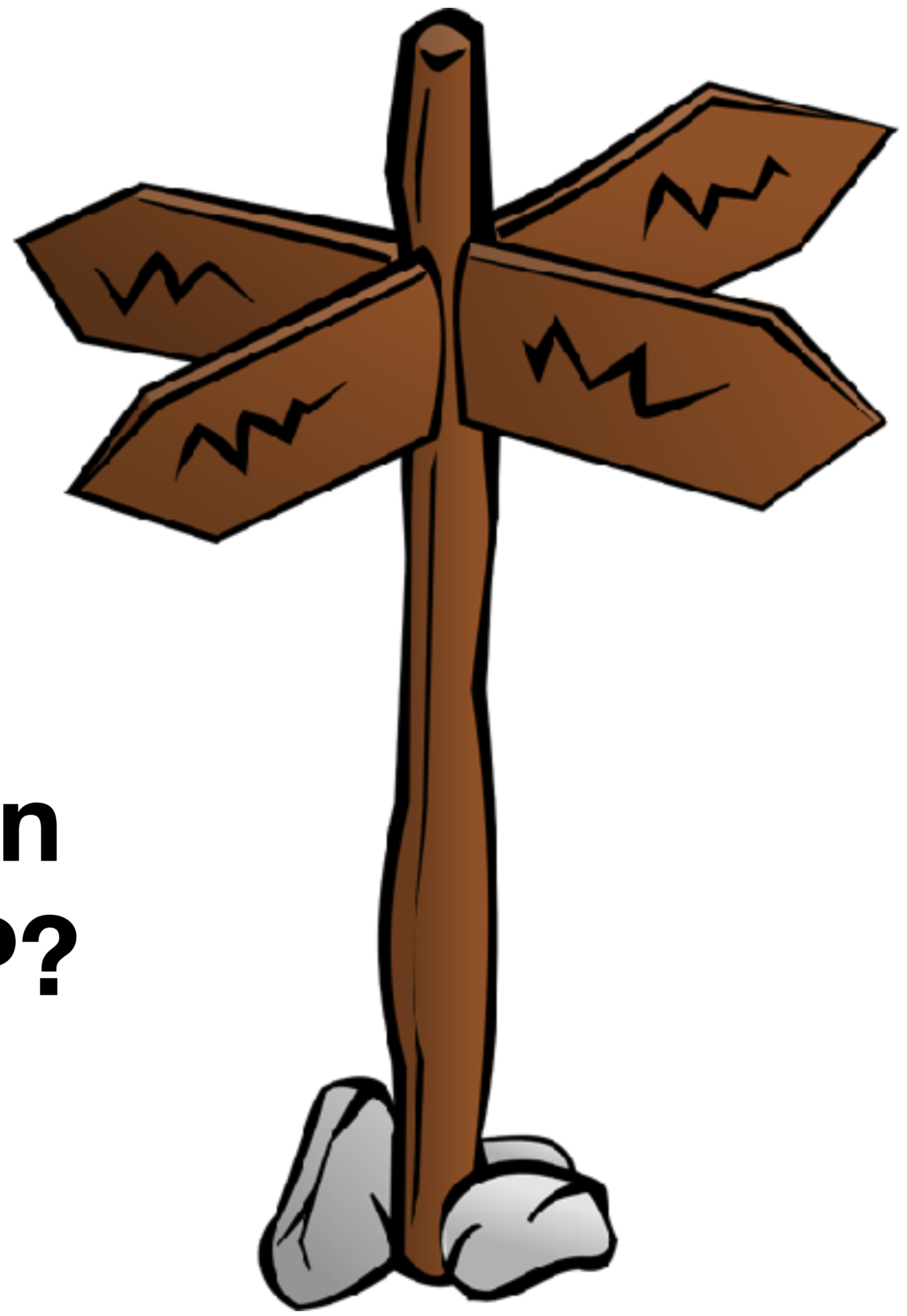
Future Directions

Classical upper bounds

- Is MQCSP, SMCSP, UMCSP in NP?
- It seems to be challenging to handle super-linear number of ancilla qubits.

Are there search-to-decision or self reduction for MQCSP?

- Due to the boolean structure, the straightforward idea doesn't work.



Applications of the quantum-unique reductions?

Can we base the security of crypto primitives on quantum MCSPs?

More connections of quantum MCSPs to other problems?

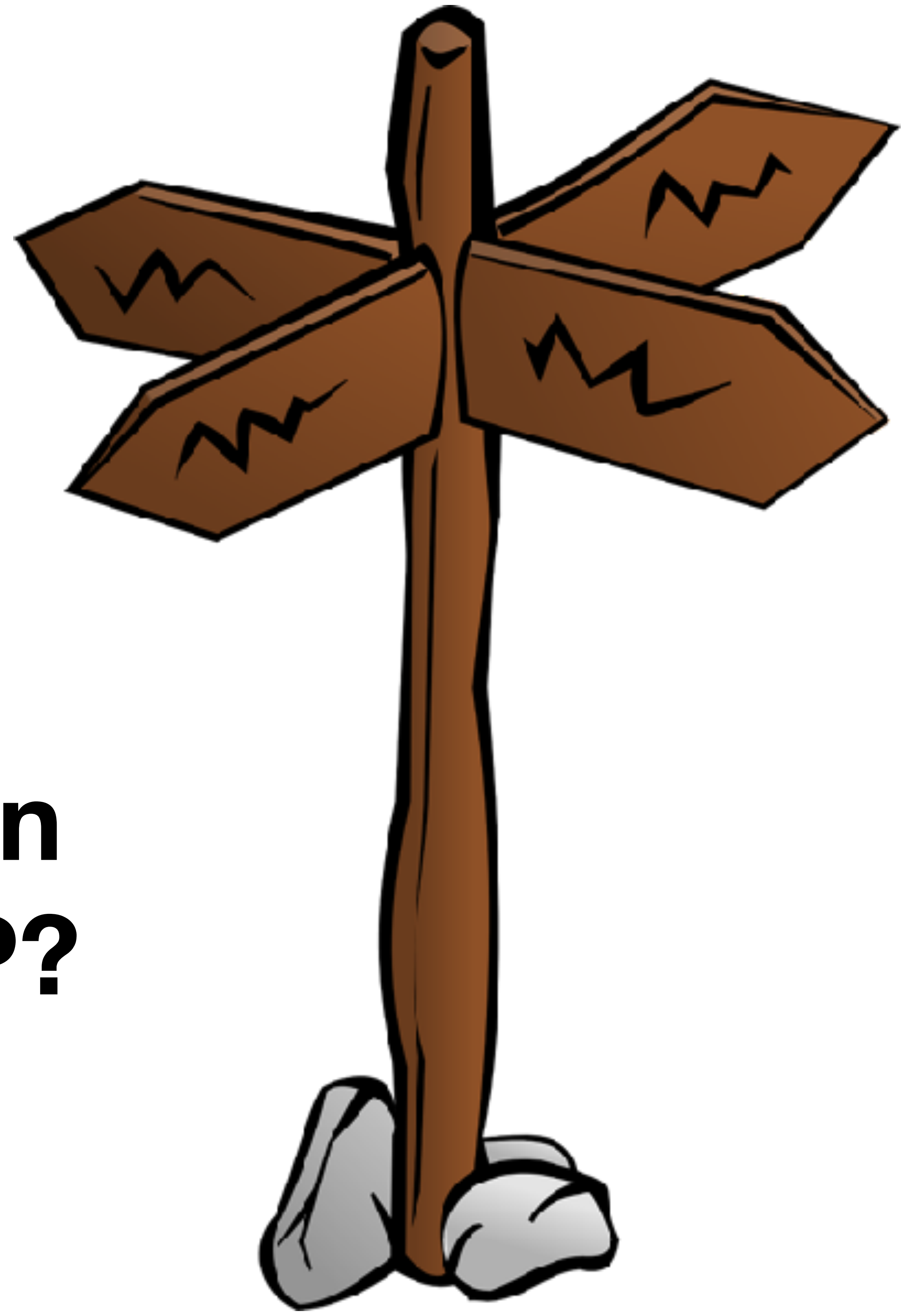
Future Directions

Classical upper bounds

- Is MQCSP, SMCSP, UMCSP in NP?
- It seems to be challenging to handle super-linear number of ancilla qubits.

Are there search-to-decision or self reduction for MQCSP?

- Due to the boolean structure, the straightforward idea doesn't work.



Applications of the quantum-unique reductions?

Can we base the security of crypto primitives on quantum MCSPs?

More connections of quantum MCSPs to other problems?

Thanks for your attention 🙂