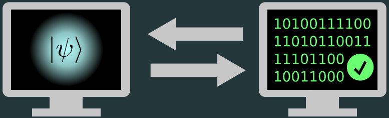


Classical verification of quantum computational advantage

Gregory D. Kahanamoku-Meyer

February 9, 2022

arXiv:2104.00687 (theory)
arXiv:2112.05156 (expt.)

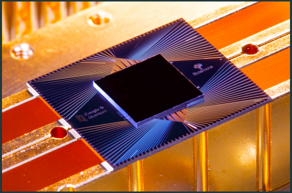
QUANTUM SYSTEMS ACCELERATOR
Catalyzing the Quantum Ecosystem

Berkeley
UNIVERSITY OF CALIFORNIA

BERKELEY LAB

Quantum computational advantage

Recent experimental demonstrations:



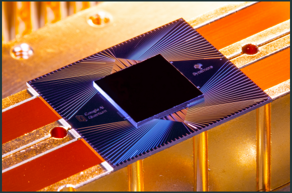
Random circuit sampling
[Arute et al., Nature '19]

Gaussian boson sampling
[Zhong et al., Science '20]

•••

Quantum computational advantage

Recent experimental demonstrations:



Random circuit sampling
[Arute et al., Nature '19]

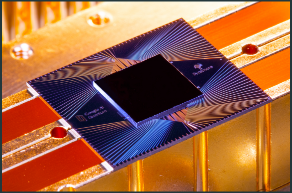
Gaussian boson sampling
[Zhong et al., Science '20]

• • •

Largest experiments → impossible to classically simulate

Quantum computational advantage

Recent experimental demonstrations:



Random circuit sampling
[Arute et al., Nature '19]

Gaussian boson sampling
[Zhong et al., Science '20]

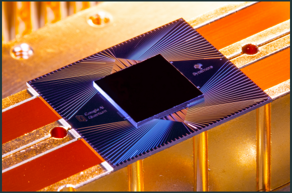
• • •

Largest experiments → impossible to classically simulate

"... [Rule] out alternative [classical] hypotheses that might be plausible in this experiment" [Zhong et al.]

Quantum computational advantage

Recent experimental demonstrations:



Random circuit sampling
[Arute et al., Nature '19]

Gaussian boson sampling
[Zhong et al., Science '20]

• • •

Largest experiments → impossible to classically simulate

"... [Rule] out alternative [classical] hypotheses that might be plausible in this experiment" [Zhong et al.]
Quantum is the only reasonable explanation for observed behavior

“Black-box” quantum computational advantage

Stronger: rule out all classical hypotheses, even pathological!

“Black-box” quantum computational advantage

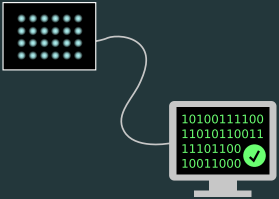
Stronger: rule out all classical hypotheses, even pathological!

Explicitly perform a “proof of quantumness”

“Black-box” quantum computational advantage

Stronger: rule out all classical hypotheses, even pathological!

Explicitly perform a “proof of quantumness”

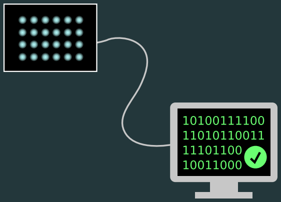


Local: rigorously refute
extended Church-Turing thesis

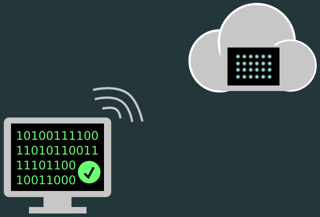
“Black-box” quantum computational advantage

Stronger: rule out all classical hypotheses, even pathological!

Explicitly perform a “proof of quantumness”



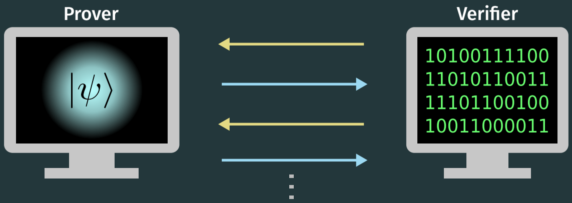
Local: rigorously refute extended Church-Turing thesis



Remote: validate an untrusted quantum cloud service

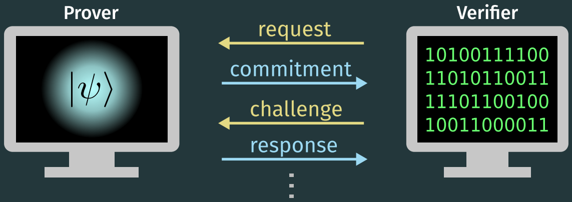
Interactive proofs

Multiple rounds of interaction between the prover and verifier



Interactive proofs

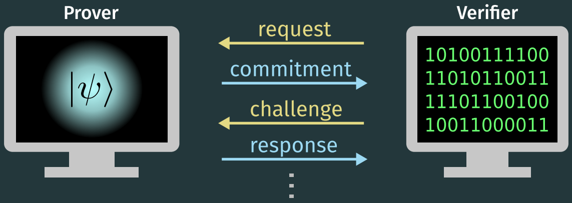
Multiple rounds of interaction between the prover and verifier



Prover must commit data before learning the challenge

Interactive proofs

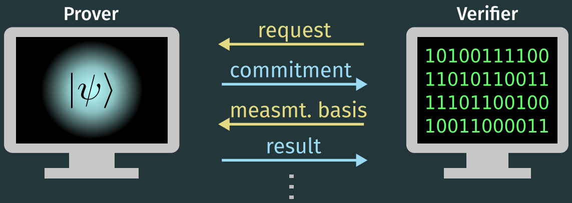
Multiple rounds of interaction between the prover and verifier



Prover must commit data before learning the challenge

Via repetition can establish that prover can respond correctly to *any* challenge.

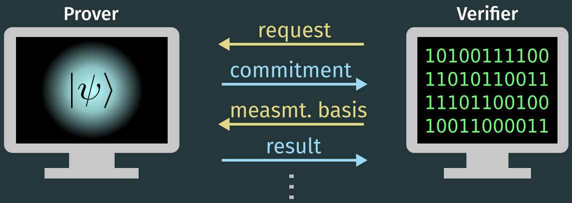
Interactive proofs of quantumness



Round 1: Prover commits to a specific quantum state

Round 2: Verifier asks for measurement in specific basis

Interactive proofs of quantumness



Round 1: Prover commits to a specific quantum state

Round 2: Verifier asks for measurement in specific basis

> By randomizing choice of basis and repeating interaction, can ensure prover would respond correctly in *any* basis

Brakerski, Christiano, Mahadev, Vazirani, Vidick '18 (arXiv:1804.00640).

Can be extended to verify arbitrary quantum computations! (arXiv:1804.01082)

State commitment (round 1): trapdoor claw-free functions

How does the prover commit to a state?

Consider a **2-to-1** function f:
for all y in range of f, there exist (x_0, x_1) such that $y = f(x_0) = f(x_1)$.

State commitment (round 1): trapdoor claw-free functions

How does the prover commit to a state?

Consider a **2-to-1** function f:
for all y in range of f, there exist (x_0, x_1) such that $y = f(x_0) = f(x_1)$.

Evaluate f on uniform superposition $\sum_x |x\rangle\,|f(x)\rangle$ $\xleftarrow{\quad f \quad}$ Pick 2-to-1 function f

Measure 2$^{\text{nd}}$ register as y $\xrightarrow{\quad y \quad}$ Store y as commitment

Prover has committed to the state $(|x_0\rangle + |x_1\rangle)\,|y\rangle$

State commitment (round 1): trapdoor claw-free functions

Prover has committed to $(|x_0\rangle + |x_1\rangle)\,|y\rangle$ with $y = f(x_0) = f(x_1)$

State commitment (round 1): trapdoor claw-free functions

Prover has committed to $(|x_0\rangle + |x_1\rangle)\,|y\rangle$ with $y = f(x_0) = f(x_1)$

Source of power: cryptographic properties of 2-to-1 function f

State commitment (round 1): trapdoor claw-free functions

Prover has committed to $(|x_0\rangle + |x_1\rangle)\,|y\rangle$ with $y = f(x_0) = f(x_1)$

Source of power: cryptographic properties of 2-to-1 function f

- **Claw-free**: It is cryptographically hard to find any pair of colliding inputs

State commitment (round 1): trapdoor claw-free functions

Prover has committed to $(|x_0\rangle + |x_1\rangle)\,|y\rangle$ with $y = f(x_0) = f(x_1)$

Source of power: cryptographic properties of 2-to-1 function f

- **Claw-free**: It is cryptographically hard to find any pair of colliding inputs
- **Trapdoor**: With the secret key, easy to classically compute the two inputs mapping to any output

State commitment (round 1): trapdoor claw-free functions

Prover has committed to $(|x_0\rangle + |x_1\rangle)\,|y\rangle$ with $y = f(x_0) = f(x_1)$

Source of power: cryptographic properties of 2-to-1 function f

- **Claw-free**: It is cryptographically hard to find any pair of colliding inputs
- **Trapdoor**: With the secret key, easy to classically compute the two inputs mapping to any output

Cheating classical prover can't forge the state;
classical verifier can determine state using trapdoor.

State commitment (round 1): trapdoor claw-free functions

Prover has committed to $(|x_0\rangle + |x_1\rangle)\,|y\rangle$ with $y = f(x_0) = f(x_1)$

Source of power: cryptographic properties of 2-to-1 function f

- **Claw-free**: It is cryptographically hard to find any pair of colliding inputs
- **Trapdoor**: With the secret key, easy to classically compute the two inputs mapping to any output

Cheating classical prover can't forge the state;
classical verifier can determine state using trapdoor.

The only path to a valid state without trapdoor is by superposition + wavefunction collapse—inherently quantum!

[BCMVV ’18] protocol

Prover

Verifier

Pick trapdoor claw-free function f $\xleftarrow{f}$ Evaluate f on uniform superposition: $\sum_x |x\rangle |f(x)\rangle$

Measure 2nd register as y $\xrightarrow{y}$ Compute x_0, x_1 from y using trapdoor

Brakerski, Christiano, Mahadev, Vazirani, Vidick ’18 (arXiv:1804.00640)

[BCMVV '18] protocol

Prover

Verifier

Evaluate f on uniform superposition: $\sum_x |x\rangle |f(x)\rangle$	$\xleftarrow{f}$	Pick trapdoor claw-free function f
Measure 2nd register as y	$\xrightarrow{y}$	Compute x_0, x_1 from y using trapdoor
	$\xleftarrow{\text{basis}}$	Pick Z or X basis
Measure qubits of $|x_0\rangle + |x_1\rangle$ in given basis		
	$\xrightarrow{\text{result}}$	Validate result against x_0, x_1

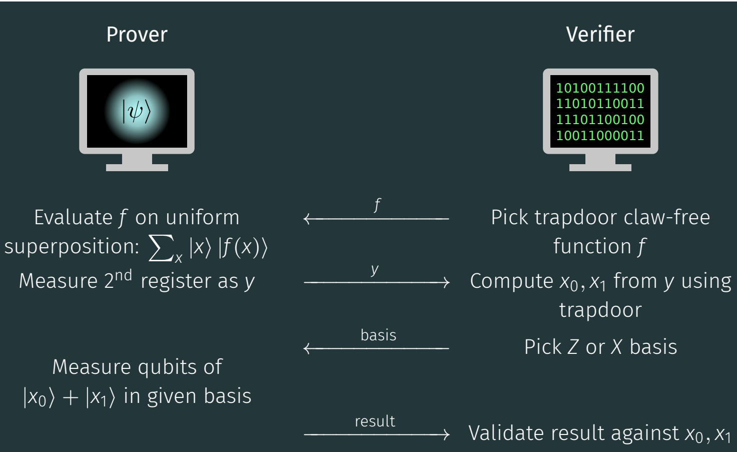
Brakerski, Christiano, Mahadev, Vazirani, Vidick '18 (arXiv:1804.00640)

[BCMVV ’18] protocol

Prover		Verifier
Evaluate f on uniform superposition: $\sum_x \|x\rangle \|f(x)\rangle$	$\xleftarrow{\quad f \quad}$	Pick trapdoor claw-free function f
Measure 2nd register as y	$\xrightarrow{\quad y \quad}$	Compute x_0, x_1 from y using trapdoor
	$\xleftarrow{\text{basis}}$	Pick Z or X basis
Measure qubits of $\|x_0\rangle + \|x_1\rangle$ in given basis		
	$\xrightarrow{\text{result}}$	Validate result against x_0, x_1

Perform experiment many times,
let p_Z, p_X be success rate in respective basis.

[BCMVV ’18] protocol



Prover

Verifier

Pick trapdoor claw-free function f

$\xleftarrow{\quad f \quad}$

Evaluate f on uniform superposition: $\sum_x |x\rangle\,|f(x)\rangle$

Measure 2nd register as y

$\xrightarrow{\quad y \quad}$

Compute x_0, x_1 from y using trapdoor

Pick Z or X basis

$\xleftarrow{\text{basis}}$

Measure qubits of $|x_0\rangle + |x_1\rangle$ in given basis

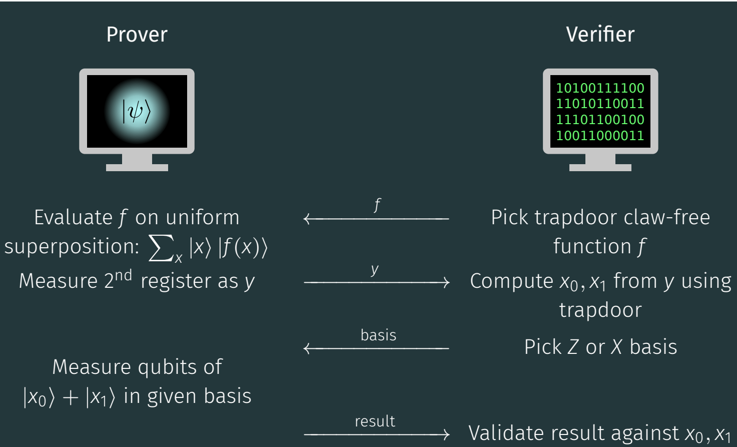
$\xrightarrow{\text{result}}$

Validate result against x_0, x_1

Classical bound: $p_Z + 2p_X < 2 + \epsilon$

Ideal quantum: $p_Z + 2p_X = 3$

[BCMVV ’18] protocol



Prover

Verifier

Evaluate f on uniform superposition: $\sum_x |x\rangle\,|f(x)\rangle$ $\xleftarrow{\quad f \quad}$ Pick trapdoor claw-free function f

Measure 2nd register as y $\xrightarrow{\quad y \quad}$ Compute x_0, x_1 from y using trapdoor

$\xleftarrow{\quad \text{basis} \quad}$ Pick Z or X basis

Measure qubits of $|x_0\rangle + |x_1\rangle$ in given basis

$\xrightarrow{\quad \text{result} \quad}$ Validate result against x_0, x_1

Subtlety: claw-free alone does *not* imply classical bound!
Learning-with-Errors TCF has adaptive hardcore bit

Trapdoor claw-free functions

TCF	Trapdoor	Claw-free	Adaptive hard-core bit
LWE [1]	✓	✓	✓
Ring-LWE [2]	✓	✓	✗
$x^2 \bmod N$ [3]	✓	✓	✗
Diffie-Hellman [3]	✓	✓	✗

[1] Brakerski, Christiano, Mahadev, Vidick, Vazirani ’18 (arXiv:1804.00640)

[2] Brakerski, Koppula, Vazirani, Vidick ’20 (arXiv:2005.04826)

[3] GDKM, Choi, Vazirani, Yao ’21 (arXiv:2104.00687)

Trapdoor claw-free functions

TCF	Trapdoor	Claw-free	Adaptive hard-core bit
LWE [1]	✓	✓	✓
Ring-LWE [2]	✓	✓	✗
$x^2 \bmod N$ [3]	✓	✓	✗
Diffie-Hellman [3]	✓	✓	✗

BKVV '20 removes need for AHCB in **random oracle model**. [2]

[1] Brakerski, Christiano, Mahadev, Vidick, Vazirani '18 (arXiv:1804.00640)

[2] Brakerski, Koppula, Vazirani, Vidick '20 (arXiv:2005.04826)

[3] GDKM, Choi, Vazirani, Yao '21 (arXiv:2104.00687)

Trapdoor claw-free functions

TCF	Trapdoor	Claw-free	Adaptive hard-core bit
LWE [1]	✓	✓	✓
Ring-LWE [2]	✓	✓	✗
$x^2 \mod N$ [3]	✓	✓	✗
Diffie-Hellman [3]	✓	✓	✗

BKVV '20 removes need for AHCB in **random oracle model**. [2]

Can we do the same in **standard model**?

[1] Brakerski, Christiano, Mahadev, Vidick, Vazirani '18 (arXiv:1804.00640)

[2] Brakerski, Koppula, Vazirani, Vidick '20 (arXiv:2005.04826)

[3] GDKM, Choi, Vazirani, Yao '21 (arXiv:2104.00687)

Trapdoor claw-free functions

TCF	Trapdoor	Claw-free	Adaptive hard-core bit
LWE [1]	✓	✓	✓
Ring-LWE [2]	✓	✓	✗
$x^2 \bmod N$ [3]	✓	✓	✗
Diffie-Hellman [3]	✓	✓	✗

BKVV ’20 removes need for AHCB in **random oracle model**. [2]

Can we do the same in **standard model**? Yes! [3]

[1] Brakerski, Christiano, Mahadev, Vidick, Vazirani ’18 (arXiv:1804.00640)

[2] Brakerski, Koppula, Vazirani, Vidick ’20 (arXiv:2005.04826)

[3] GDKM, Choi, Vazirani, Yao ’21 (arXiv:2104.00687)

Interactive measurement: computational Bell test

Prover

Verifier

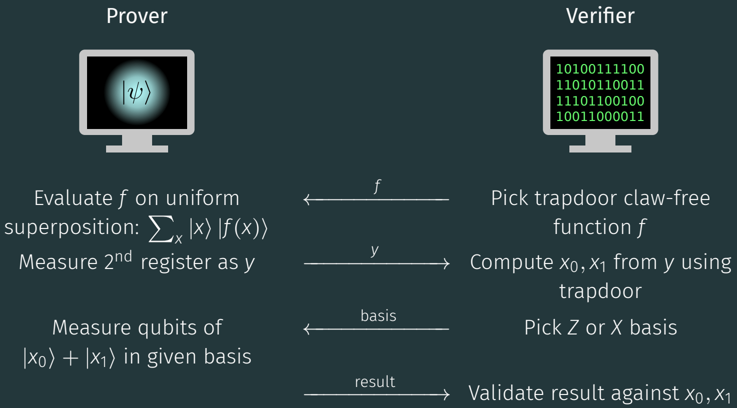
Evaluate f on uniform superposition: $\sum_x |x\rangle\,|f(x)\rangle$ $\xleftarrow{\quad f \quad}$ Pick trapdoor claw-free function f

Measure 2nd register as y $\xrightarrow{\quad y \quad}$ Compute x_0, x_1 from y using trapdoor

Measure qubits of $|x_0\rangle + |x_1\rangle$ in given basis $\xleftarrow{\text{basis}}$ Pick Z or X basis

$\xrightarrow{\text{result}}$ Validate result against x_0, x_1

Interactive measurement: computational Bell test



Prover | **Verifier**

Evaluate f on uniform superposition: $\sum_x |x\rangle |f(x)\rangle$ $\xleftarrow{f}$ Pick trapdoor claw-free function f

Measure 2nd register as y $\xrightarrow{y}$ Compute x_0, x_1 from y using trapdoor

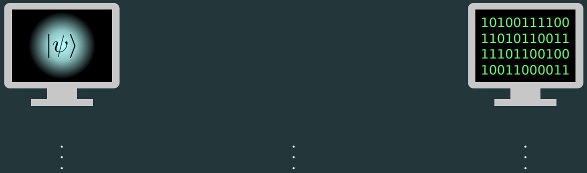
Measure qubits of $|x_0\rangle + |x_1\rangle$ in given basis $\xleftarrow{\text{basis}}$ Pick Z or X basis

$\xrightarrow{\text{result}}$ Validate result against x_0, x_1

Replace X basis measurement with “1-player CHSH game.”

Interactive measurement: computational Bell test

Replace X basis measurement with two-step process:
“condense” x_0, x_1 into a single qubit, and then do a “Bell test.”



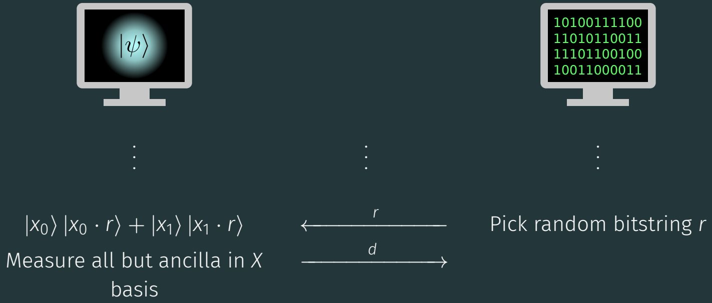
$|x_0\rangle |x_0 \cdot r\rangle + |x_1\rangle |x_1 \cdot r\rangle$ $\xleftarrow{\quad r \quad}$ Pick random bitstring r

Measure all but ancilla in X basis $\xrightarrow{\quad d \quad}$

GDKM, Choi, Vazirani, Yao ’21 (arXiv:2104.00687)

Interactive measurement: computational Bell test

Replace X basis measurement with two-step process:
"condense" x_0, x_1 into a single qubit, and then do a "Bell test."



$|x_0\rangle |x_0 \cdot r\rangle + |x_1\rangle |x_1 \cdot r\rangle$ $\xleftarrow{r}$ Pick random bitstring r

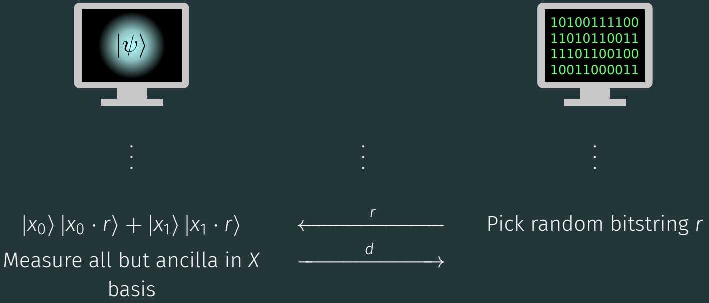
Measure all but ancilla in X basis $\xrightarrow{d}$

Now single-qubit state: $|0\rangle$ or $|1\rangle$ if $x_0 \cdot r = x_1 \cdot r$, otherwise $|+\rangle$ or $|-\rangle$.

GDKM, Choi, Vazirani, Yao '21 (arXiv:2104.00687)

Interactive measurement: computational Bell test

Replace X basis measurement with two-step process:
“condense” x_0, x_1 into a single qubit, and then do a “Bell test.”



$|x_0\rangle |x_0 \cdot r\rangle + |x_1\rangle |x_1 \cdot r\rangle$ $\xleftarrow{\quad r \quad}$ Pick random bitstring r

Measure all but ancilla in X basis $\xrightarrow{\quad d \quad}$

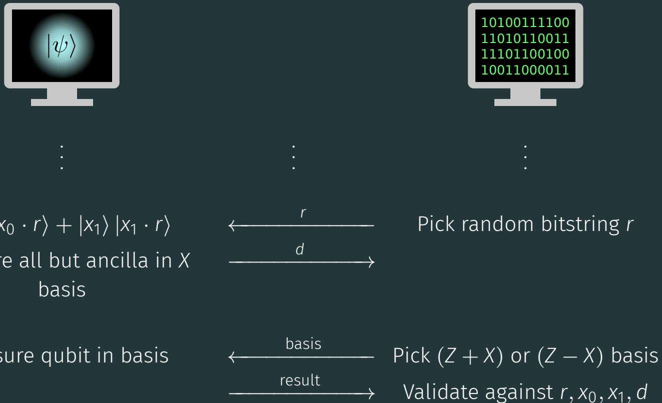
Now single-qubit state: $|0\rangle$ or $|1\rangle$ if $x_0 \cdot r = x_1 \cdot r$, otherwise $|+\rangle$ or $|-\rangle$.
Polarization hidden via:

Cryptographic secret (here) $\Leftrightarrow$ Non-communication (Bell test)

GDKM, Choi, Vazirani, Yao ’21 (arXiv:2104.00687)

Interactive measurement: computational Bell test

Replace X basis measurement with two-step process: "condense" x_0, x_1 into a single qubit, and then do a "Bell test."



$|x_0\rangle |x_0 \cdot r\rangle + |x_1\rangle |x_1 \cdot r\rangle$ $\xleftarrow{\quad r \quad}$ Pick random bitstring r

Measure all but ancilla in X basis $\xrightarrow{\quad d \quad}$

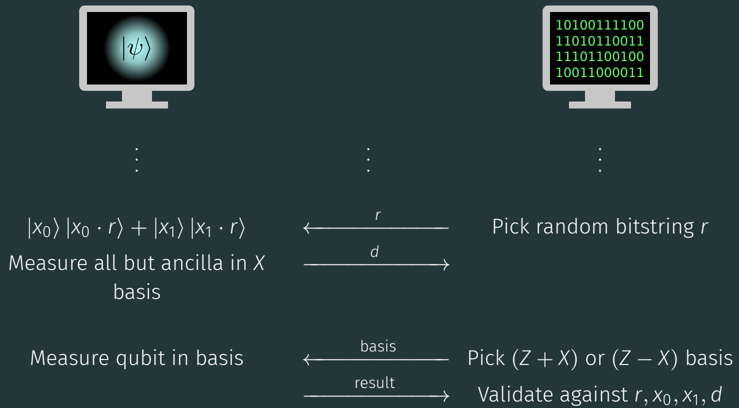
Measure qubit in basis $\xleftarrow{\text{basis}}$ Pick $(Z+X)$ or $(Z-X)$ basis

$\xrightarrow{\text{result}}$ Validate against r, x_0, x_1, d

GDKM, Choi, Vazirani, Yao '21 (arXiv:2104.00687)

Interactive measurement: computational Bell test

Replace X basis measurement with two-step process:
"condense" x_0, x_1 into a single qubit, and then do a "Bell test."



$|x_0\rangle |x_0 \cdot r\rangle + |x_1\rangle |x_1 \cdot r\rangle$ $\xleftarrow{r}$ Pick random bitstring r

Measure all but ancilla in X basis $\xrightarrow{d}$

Measure qubit in basis $\xleftarrow{\text{basis}}$ Pick $(Z + X)$ or $(Z - X)$ basis

$\xrightarrow{\text{result}}$ Validate against r, x_0, x_1, d

Now can use any trapdoor claw-free function!

GDKM, Choi, Vazirani, Yao '21 (arXiv:2104.00687)

Computational Bell test: classical bound

Run protocol many times, collect statistics.

p_Z: Success rate for Z basis measurement.

p_{CHSH}: Success rate when performing CHSH-type measurement.

Computational Bell test: classical bound

Run protocol many times, collect statistics.

p_Z: Success rate for Z basis measurement.

p_{CHSH}: Success rate when performing CHSH-type measurement.

Under assumption of claw-free function:

Classical bound: $p_Z + 4p_{\text{CHSH}} - 4 < \epsilon$

Computational Bell test: classical bound

Run protocol many times, collect statistics.

p_Z: Success rate for Z basis measurement.

p_{CHSH}: Success rate when performing CHSH-type measurement.

Under assumption of claw-free function:

Classical bound: $p_Z + 4p_{\mathsf{CHSH}} - 4 < \epsilon$

Ideal quantum: $p_Z = 1, p_{\mathsf{CHSH}} = \cos^2(\pi/8)$

Computational Bell test: classical bound

Run protocol many times, collect statistics.

p_Z: Success rate for Z basis measurement.

p_{CHSH}: Success rate when performing CHSH-type measurement.

Under assumption of claw-free function:

Classical bound: $p_Z + 4p_{\text{CHSH}} - 4 < \epsilon$

Ideal quantum: $p_Z = 1, p_{\text{CHSH}} = \cos^2(\pi/8)$

$p_Z + 4p_{\text{CHSH}} - 4 = \sqrt{2} - 1 \approx$ **0.414**

Computational Bell test: classical bound

Run protocol many times, collect statistics.

p_Z: Success rate for Z basis measurement.

p_{CHSH}: Success rate when performing CHSH-type measurement.

Under assumption of claw-free function:

Classical bound: $p_Z + 4p_{\text{CHSH}} - 4 < \epsilon$

Ideal quantum: $p_Z = 1, p_{\text{CHSH}} = \cos^2(\pi/8)$

$p_Z + 4p_{\text{CHSH}} - 4 = \sqrt{2} - 1 \approx \mathbf{0.414}$

Note: Let $p_Z = 1$. Then for p_{CHSH}:

Classical bound 75%, ideal quantum $\sim$ 85%. Same as regular CHSH!

GDKM, Choi, Vazirani, Yao '21 (arXiv:2104.00687)

Moving towards full efficiently-verifiable quantum adv. on NISQ

Moving towards full efficiently-verifiable quantum adv. on NISQ

Interaction

- Need to measure subsystem while maintaining coherence on other qubits

Moving towards full efficiently-verifiable quantum adv. on NISQ

Interaction

- Need to measure subsystem while maintaining coherence on other qubits
- Implemented by the experiments!!

Moving towards full efficiently-verifiable quantum adv. on NISQ

Interaction

- Need to measure subsystem while maintaining coherence on other qubits
- Implemented by the experiments!!

Moving towards full efficiently-verifiable quantum adv. on NISQ

Interaction

- Need to measure subsystem while maintaining coherence on other qubits
- Implemented by the experiments!!

Fidelity (without error correction)

- Need to pass classical threshold

Moving towards full efficiently-verifiable quantum adv. on NISQ

Interaction

- Need to measure subsystem while maintaining coherence on other qubits
- Implemented by the experiments!!

Fidelity (without error correction)

- Need to pass classical threshold
- Postselection scheme drastically improves required fidelity [arXiv:2104.00687]

Moving towards full efficiently-verifiable quantum adv. on NISQ

Interaction

- Need to measure subsystem while maintaining coherence on other qubits
- Implemented by the experiments!!

Fidelity (without error correction)

- Need to pass classical threshold
- Postselection scheme drastically improves required fidelity [arXiv:2104.00687]

Moving towards full efficiently-verifiable quantum adv. on NISQ

Interaction

- Need to measure subsystem while maintaining coherence on other qubits
- Implemented by the experiments!!

Fidelity (without error correction)

- Need to pass classical threshold
- Postselection scheme drastically improves required fidelity [arXiv:2104.00687]

Circuit sizes

- Removing need for adaptive hardcore bit allows “easier” TCFs

Moving towards full efficiently-verifiable quantum adv. on NISQ

Interaction

- Need to measure subsystem while maintaining coherence on other qubits
- Implemented by the experiments!!

Fidelity (without error correction)

- Need to pass classical threshold
- Postselection scheme drastically improves required fidelity [arXiv:2104.00687]

Circuit sizes

- Removing need for adaptive hardcore bit allows “easier” TCFs
- Measurement-based uncomputation scheme [arXiv:2104.00687]

Moving towards full efficiently-verifiable quantum adv. on NISQ

Interaction

- Need to measure subsystem while maintaining coherence on other qubits
- Implemented by the experiments!!

Fidelity (without error correction)

- Need to pass classical threshold
- Postselection scheme drastically improves required fidelity [arXiv:2104.00687]

Circuit sizes

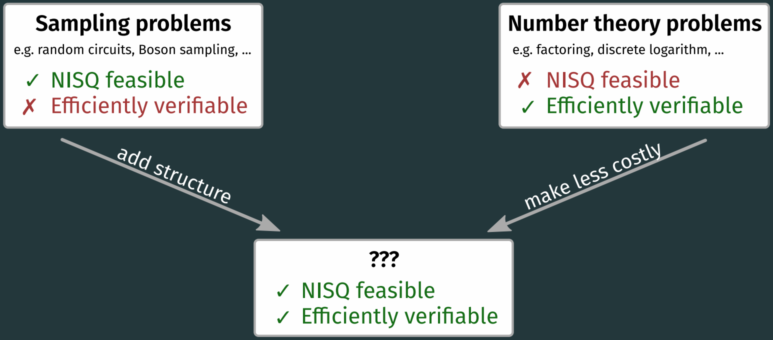
- Removing need for adaptive hardcore bit allows “easier” TCFs
- Measurement-based uncomputation scheme [arXiv:2104.00687]
- … hopefully can continue making theory improvements!

Backup

NISQ verifiable quantum advantage

Trivial solution: Shor's algorithm … but we want to do near-term!

NISQ: Noisy Intermediate-Scale Quantum devices



Sampling problems

e.g. random circuits, Boson sampling, …

✓ NISQ feasible

✗ Efficiently verifiable

Number theory problems

e.g. factoring, discrete logarithm, …

✗ NISQ feasible

✓ Efficiently verifiable

???

✓ NISQ feasible

✓ Efficiently verifiable