Low-degree testing for quantum states
arXiv: 1710.03062 & 1801.03821

Anand Natarajan [1] Thomas Vidick [2]

[1] MIT

[2] Caltech

January 16, 2018

Introduction

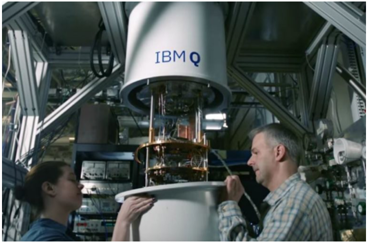
- Motivating question: how to **classically** verify an **untrusted** quantum device?

Introduction

- Motivating question: how to **classically** verify an **untrusted** quantum device?

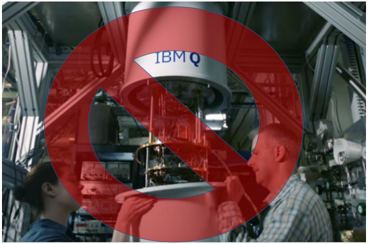
Introduction

- Motivating question: how to **classically** verify an **untrusted** quantum device?



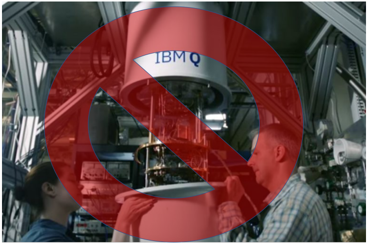
Introduction

- Motivating question: how to **classically** verify an **untrusted** quantum device?



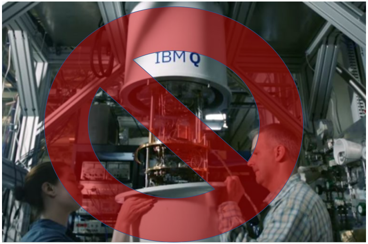
Introduction

- Motivating question: how to **classically** verify an **untrusted** quantum device?
- In this talk: testing for entanglement between **spatially separated, noncommunicating** quantum devices



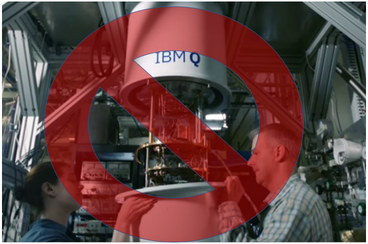
Introduction

- Motivating question: how to **classically** verify an **untrusted** quantum device?
- In this talk: testing for entanglement between **spatially separated, noncommunicating** quantum devices
  - Two servers on opposite sides of the world,



Introduction

- Motivating question: how to **classically** verify an **untrusted** quantum device?
- In this talk: testing for entanglement between **spatially separated, noncommunicating** quantum devices
  - Two servers on opposite sides of the world,
  - Or far-apart regions on a single chip



The model

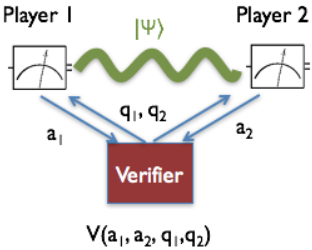
- Classical **verifier** interacts with k (≥ 2) noncommunicating quantum **players**

The model

- Classical **verifier** interacts with k ($\geq$ 2) noncommunicating quantum **players**
- Players' **strategy**:

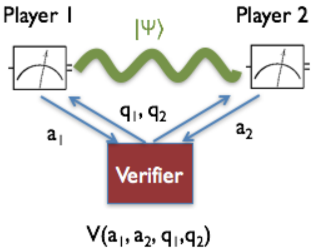
The model

- Classical **verifier** interacts with k (≥ 2) noncommunicating quantum **players**
- Players' **strategy**: k-partite state $|\psi\rangle$, measurements $\{M^a_{q,i}\}_a$.



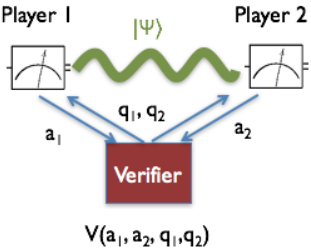
The model

- Classical **verifier** interacts with k (≥ 2) noncommunicating quantum **players**
- Players' **strategy**: k-partite state $|\psi\rangle$, measurements $\{M^a_{q,i}\}_a$.
  - On receiving question q from verifier, player i applies $\{M^a_{q,i}\}_a$ to its share of $|\psi\rangle$ and returns outcome a



The model

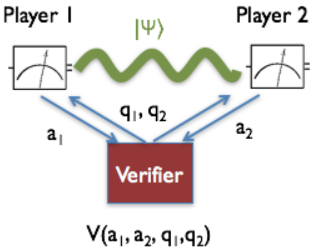
- Classical **verifier** interacts with k (≥ 2) noncommunicating quantum **players**
- Players' **strategy**: k-partite state $|\psi\rangle$, measurements $\{M_{q,i}^a\}_a$.
  - On receiving question q from verifier, player i applies $\{M_{q,i}^a\}_a$ to its share of $|\psi\rangle$ and returns outcome a
- At the end, verifier decides to *accept* or *reject*.



The model

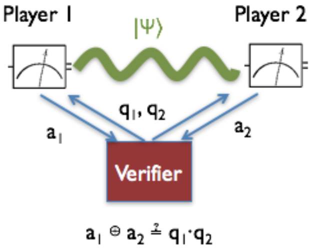
- Classical **verifier** interacts with k (≥ 2) noncommunicating quantum **players**
- Players' **strategy**: k-partite state $|\psi\rangle$, measurements $\{M^a_{q,i}\}_a$.
  - On receiving question q from verifier, player i applies $\{M^a_{q,i}\}_a$ to its share of $|\psi\rangle$ and returns outcome a
- At the end, verifier decides to *accept* or *reject*.
- Test strategies up to local isometry :

$$|\psi\rangle \mapsto (U_1 \otimes U_2)|\psi\rangle$$
$$M^a_{q,i} \mapsto U_i M^a_{q,1} U_i^\dagger$$



Example: CHSH

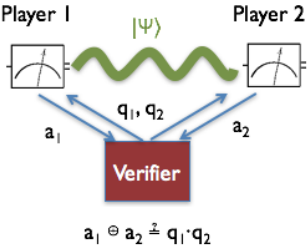
CHSH test: 1 round, 2 players, 1-bit messages



Example: CHSH

CHSH test: 1 round, 2 players, 1-bit messages

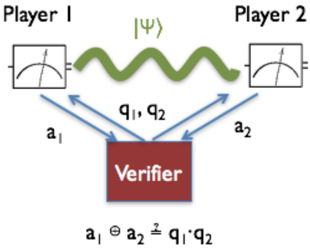
- If players are classical, succeed with $p \leq 3/4$.



Example: CHSH

CHSH test: 1 round, 2 players, 1-bit messages

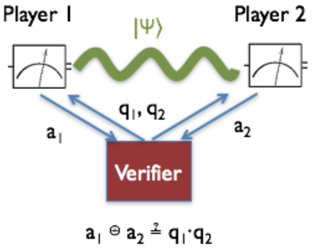
- If players are classical, succeed with $p \leq 3/4$.
- Optimal entangled strategy succeeds with $p = \omega^*_{CHSH} \approx 0.85$, with shared state $|\psi\rangle = |\text{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$



Example: CHSH

CHSH test: 1 round, 2 players, 1-bit messages

- If players are classical, succeed with $p \leq 3/4$.
- Optimal entangled strategy succeeds with $p = \omega^*_{CHSH} \approx 0.85$, with shared state $|\psi\rangle = |\text{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$



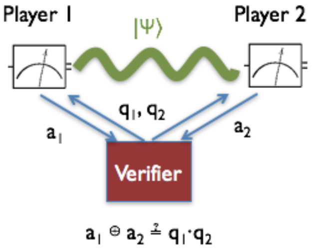
Theorem (SW88, MYS12)

Any strategy succeeding with $p = \omega^*_{CHSH} - \varepsilon$ must be $\delta(\varepsilon) = O(\sqrt{\varepsilon})$-close to the optimal strategy under local isometry.

Example: CHSH

CHSH test: 1 round, 2 players, 1-bit messages

- If players are classical, succeed with $p \leq 3/4$.
- Optimal entangled strategy succeeds with $p = \omega^*_{CHSH} \approx 0.85$, with shared state $|\psi\rangle = |\text{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$



Theorem (SW88, MYS12)

Any strategy succeeding with $p = \omega^*_{CHSH} - \varepsilon$ *must be* $\delta(\varepsilon) = O(\sqrt{\varepsilon})$*-close to the optimal strategy under local isometry.*

CHSH game is a "**self-test**" for the state $|\text{EPR}\rangle$ with **robustness** $\delta(\varepsilon)$.

Example: Magic Square

Magic Square game: 1 round, 2 players, 2-bit messages

Example: Magic Square

Magic Square game: 1 round, 2 players, 2-bit messages

- If players are classical, succeed with $p \leq 8/9$.

Example: Magic Square

Magic Square game: 1 round, 2 players, 2-bit messages

- If players are classical, succeed with $p \leq 8/9$.
- Optimal entangled strategy succeeds with $p = \omega^*_{MS} = 1$, using state $|\psi\rangle = |\mathrm{EPR}\rangle^{\otimes 2}$.

Example: Magic Square

Magic Square game: 1 round, 2 players, 2-bit messages

- If players are classical, succeed with $p \leq 8/9$.
- Optimal entangled strategy succeeds with $p = \omega^*_{MS} = 1$, using state $|\psi\rangle = |\mathrm{EPR}\rangle^{\otimes 2}$.

Theorem (WBMS15)

Any strategy succeeding with $p = \omega^*_{MS} - \varepsilon$ must be $\delta(\varepsilon) = O(\sqrt{\varepsilon})$-close to the optimal strategy under local isometry.

Example: Magic Square

Magic Square game: 1 round, 2 players, 2-bit messages

- If players are classical, succeed with $p \leq 8/9$.
- Optimal entangled strategy succeeds with $p = \omega^*_{MS} = 1$, using state $|\psi\rangle = |\mathrm{EPR}\rangle^{\otimes 2}$.

Theorem (WBMS15)

Any strategy succeeding with $p = \omega^*_{MS} - \varepsilon$ must be $\delta(\varepsilon) = O(\sqrt{\varepsilon})$-close to the optimal strategy under local isometry.

Magic Square game is a **self-test** for the state $|\mathrm{EPR}\rangle^{\otimes 2}$ with **robustness** $\delta(\varepsilon)$ and **perfect completeness**.

Self-testing

- A **self-test** for $|\psi\rangle$ is a multiplayer interactive protocol with

Self-testing

- A **self-test** for $|\psi\rangle$ is a multiplayer interactive protocol with
  - Completeness: Players sharing $|\psi\rangle$ can succeed with **optimal** probability p^*.

Self-testing

- A **self-test** for $|\psi\rangle$ is a multiplayer interactive protocol with
  - Completeness: Players sharing $|\psi\rangle$ can succeed with **optimal** probability p^*.
  - Robustness: Players succeeding with probability $p^* - \varepsilon$ **must** share a state $\delta(\varepsilon)$ **close** to $|\psi\rangle$ (up to local isometry).

Self-testing

- A **self-test** for $|\psi\rangle$ is a multiplayer interactive protocol with
  - Completeness: Players sharing $|\psi\rangle$ can succeed with **optimal** probability p^*.
  - Robustness: Players succeeding with probability $p^* - \varepsilon$ **must** share a state $\delta(\varepsilon)$ **close** to $|\psi\rangle$ (up to local isometry).
- To test a qubit, test **Pauli operators** X, Z acting on it:

Self-testing

- A **self-test** for $|\psi\rangle$ is a multiplayer interactive protocol with
  - Completeness: Players sharing $|\psi\rangle$ can succeed with **optimal** probability p^*.
  - Robustness: Players succeeding with probability $p^* - \varepsilon$ **must** share a state $\delta(\varepsilon)$ **close** to $|\psi\rangle$ (up to local isometry).
- To test a qubit, test **Pauli operators** X, Z acting on it:
  - Any nontrivial representation of Pauli relations

$$X^2 = Z^2 = \mathrm{Id}, XZ = -ZX$$

requires dimension at least 2 $\Longrightarrow$ 1 qubit.

Self-testing

- A **self-test** for $|\psi\rangle$ is a multiplayer interactive protocol with
  - Completeness: Players sharing $|\psi\rangle$ can succeed with **optimal** probability p^*.
  - Robustness: Players succeeding with probability $p^* - \varepsilon$ **must** share a state $\delta(\varepsilon)$ **close** to $|\psi\rangle$ (up to local isometry).
- To test a qubit, test **Pauli operators** X, Z acting on it:
  - Any nontrivial representation of Pauli relations

$$X^2 = Z^2 = \mathrm{Id}, XZ = -ZX$$

    requires dimension at least 2 $\implies$ 1 qubit.
  - $\langle\psi|\frac{1}{2}(XX + ZZ)|\psi\rangle \approx 1 \implies |\psi\rangle \approx |\mathrm{EPR}\rangle$.

More qubits?

- What if we want to test n qubits of entanglement, e.g. the state $|\mathrm{EPR}\rangle^{\otimes n}$?

More qubits?

- What if we want to test n qubits of entanglement, e.g. the state $|\text{EPR}\rangle^{\otimes n}$?
- To test n qubits, test n**-qubit tensor products of Paulis** acting on them

More qubits?

- What if we want to test n qubits of entanglement, e.g. the state $|\mathrm{EPR}\rangle^{\otimes n}$?
- To test n qubits, test **n-qubit tensor products of Paulis** acting on them
  - Any nontrivial representation of Pauli relations

$$X(a)X(b) = X(a+b), Z(a)Z(b) = Z(a+b),$$
$$X(a)Z(b) = (-1)^{a\cdot b} Z(b)X(a).$$

requires dimension at least $2^n \implies n$ qubits.

More qubits?

- What if we want to test n qubits of entanglement, e.g. the state $|\text{EPR}\rangle^{\otimes n}$?
- To test n qubits, test **n-qubit tensor products of Paulis** acting on them
    - Any nontrivial representation of Pauli relations

$$X(a)X(b) = X(a+b), Z(a)Z(b) = Z(a+b),$$
$$X(a)Z(b) = (-1)^{a\cdot b}Z(b)X(a).$$

      requires dimension at least $2^n \implies n$ qubits.
    - Expectation values $\langle\psi|X(a)Z(b)|\psi\rangle$ determine the shared state $|\psi\rangle$.

More qubits: Approach 1

- What if we want to test n qubits of entanglement as **efficiently** as possible?

More qubits: Approach 1

- What if we want to test n qubits of entanglement as **efficiently** as possible?
    - Fewest **bits of communication** between players and verifier

More qubits: Approach 1

- What if we want to test n qubits of entanglement as **efficiently** as possible?
  - Fewest **bits of communication** between players and verifier
  - Best **robustness**: smallest $\delta(\varepsilon, n)$

More qubits: Approach 1

- What if we want to test n qubits of entanglement as **efficiently** as possible?
  - Fewest **bits of communication** between players and verifier
  - Best **robustness**: smallest $\delta(\varepsilon, n)$
- Approach 1: pick 2 random Paulis acting on n qubits, and test their relations. Use *rigidity* of Pauli group:

$$M_X(a)M_Z(b) \approx (-1)^{a\cdot b} M_Z(b)M_X(a) \Longrightarrow$$
$$M_X(a) \approx X(a), M_Z(b) \approx Z(b).$$

More qubits: Approach 1

- What if we want to test n qubits of entanglement as **efficiently** as possible?
  - Fewest **bits of communication** between players and verifier
  - Best **robustness**: smallest $\delta(\varepsilon, n)$
- Approach 1: pick 2 random Paulis acting on n qubits, and test their relations. Use *rigidity* of Pauli group:

$$M_X(a)M_Z(b) \approx (-1)^{a \cdot b} M_Z(b)M_X(a) \implies$$
$$M_X(a) \approx X(a), M_Z(b) \approx Z(b).$$

More qubits: Approach 1

- What if we want to test n qubits of entanglement as **efficiently** as possible?
  - Fewest **bits of communication** between players and verifier
  - Best **robustness**: smallest $\delta(\varepsilon, n)$
- Approach 1: pick 2 random Paulis acting on n qubits, and test their relations. Use *rigidity* of Pauli group:

$$M_X(a)M_Z(b) \approx (-1)^{a \cdot b} M_Z(b) M_X(a) \implies$$
$$M_X(a) \approx X(a), M_Z(b) \approx Z(b).$$

Theorem (NV16)

Test for $|\mathrm{EPR}\rangle^{\otimes n}$

More qubits: Approach 1

- What if we want to test n qubits of entanglement as **efficiently** as possible?
  - Fewest **bits of communication** between players and verifier
  - Best **robustness**: smallest $\delta(\varepsilon, n)$
- Approach 1: pick 2 random Paulis acting on n qubits, and test their relations. Use *rigidity* of Pauli group:

$$M_X(a)M_Z(b) \approx (-1)^{a\cdot b} M_Z(b)M_X(a) \implies$$
$$M_X(a) \approx X(a), M_Z(b) \approx Z(b).$$

Theorem (NV16)

Test for $|\mathrm{EPR}\rangle^{\otimes n}$ with ✓robustness δ independent of n

More qubits: Approach 1

- What if we want to test n qubits of entanglement as **efficiently** as possible?
  - Fewest **bits of communication** between players and verifier
  - Best **robustness**: smallest $\delta(\varepsilon, n)$
- Approach 1: pick 2 random Paulis acting on n qubits, and test their relations. Use *rigidity* of Pauli group:

$$M_X(a)M_Z(b) \approx (-1)^{a\cdot b} M_Z(b)M_X(a) \Longrightarrow$$
$$M_X(a) \approx X(a), M_Z(b) \approx Z(b).$$

Theorem (NV16)

Test for $|\mathrm{EPR}\rangle^{\otimes n}$ with ✓robustness δ independent of n and ✗$O(n)$ bits of communication.

More qubits: Approach 2

- Approach 2: pick 2 random qubits i, j and test X_i, X_j, Z_i, Z_j.

More qubits: Approach 2

- Approach 2: pick 2 random qubits i, j and test X_i, X_j, Z_i, Z_j.

$$M_X(a) := \prod_{i=1}^{n} (M_{X_i})^{a_i} \quad , \quad M_Z(a) := \prod_{i=1}^{n} (M_{Z_i})^{a_i}$$

$$M_{X_i} M_{Z_i} \approx_\varepsilon -M_{Z_i} M_{X_i} \implies M_X(a) M_Z(b) \approx_{n\varepsilon} -M_Z(b) M_X(a).$$

More qubits: Approach 2

- Approach 2: pick 2 random qubits i, j and test X_i, X_j, Z_i, Z_j.

$$M_X(a) := \prod_{i=1}^{n} (M_{X_i})^{a_i} \quad , \quad M_Z(a) := \prod_{i=1}^{n} (M_{Z_i})^{a_i}$$

$$M_{X_i} M_{Z_i} \approx_\varepsilon -M_{Z_i} M_{X_i} \implies M_X(a) M_Z(b) \approx_{n\varepsilon} -M_Z(b) M_X(a).$$

More qubits: Approach 2

- Approach 2: pick 2 random qubits i, j and test X_i, X_j, Z_i, Z_j.

$$M_X(a) := \prod_{i=1}^{n} (M_{X_i})^{a_i} \quad , \quad M_Z(a) := \prod_{i=1}^{n} (M_{Z_i})^{a_i}$$

$$M_{X_i} M_{Z_i} \approx_\varepsilon -M_{Z_i} M_{X_i} \implies M_X(a) M_Z(b) \approx_{n\varepsilon} -M_Z(b) M_X(a).$$

Theorem (CRSV16)

Test for $|\mathrm{EPR}\rangle^{\otimes n}$

More qubits: Approach 2

- Approach 2: pick 2 random qubits i, j and test X_i, X_j, Z_i, Z_j.

$$M_X(a) := \prod_{i=1}^{n} (M_{X_i})^{a_i} \quad , \quad M_Z(a) := \prod_{i=1}^{n} (M_{Z_i})^{a_i}$$

$$M_{X_i} M_{Z_i} \approx_\varepsilon -M_{Z_i} M_{X_i} \implies M_X(a) M_Z(b) \approx_{n\varepsilon} -M_Z(b) M_X(a).$$

Theorem (CRSV16)

Test for $|\mathrm{EPR}\rangle^{\otimes n}$ with ✗robustness $\delta = O(n^{5/2}\varepsilon)$

More qubits: Approach 2

- Approach 2: pick 2 random qubits i, j and test X_i, X_j, Z_i, Z_j.

$$M_X(a) := \prod_{i=1}^{n} (M_{X_i})^{a_i} \quad , \quad M_Z(a) := \prod_{i=1}^{n} (M_{Z_i})^{a_i}$$

$$M_{X_i} M_{Z_i} \approx_\varepsilon -M_{Z_i} M_{X_i} \implies M_X(a) M_Z(b) \approx_{n\varepsilon} -M_Z(b) M_X(a).$$

Theorem (CRSV16)

Test for $|\mathrm{EPR}\rangle^{\otimes n}$ with ✗robustness $\delta = O(n^{5/2}\varepsilon)$ and ✓$O(\log(n))$ bits of communication.

More qubits: Our result

Theorem (Quantum low-degree test)

There exists a 1-round, 2-player protocol with $O(\text{poly}\log(n))$-bit questions and answers such that any players succeeding with probability $1-\varepsilon$ must share a state that is $\delta(\varepsilon)$-close to $|\text{EPR}\rangle^{\otimes n}$, where δ is **independent** *of n.*

More qubits: Our result

Theorem (Quantum low-degree test)

There exists a 1-round, 2-player protocol with $O(\mathrm{poly}\log(n))$-bit questions and answers such that any players succeeding with probability $1-\varepsilon$ must share a state that is $\delta(\varepsilon)$-close to $|\mathrm{EPR}\rangle^{\otimes n}$, where δ is **independent** *of n.*

- Test certifies $n^{\mathrm{poly}\log(n)}$-size subset of Pauli operators, arising from **low degree polynomials**.

Self-testing and complexity theory

- Motivation: what is the power of **interactive proof systems** with entangled quantum provers (MIP*)?

Self-testing and complexity theory

- Motivation: what is the power of **interactive proof systems** with entangled quantum provers (MIP*)?
  - $\approx$ hardness of approximating the **value** of a protocol (maximal success probability of any entangled strategy)

Self-testing and complexity theory

- Motivation: what is the power of **interactive proof systems** with entangled quantum provers (MIP^*)?
  - $\approx$ hardness of approximating the **value** of a protocol (maximal success probability of any entangled strategy)
- **Classically:** NP-hard to approximate unentangled value up to constant error ($\mathrm{MIP} = \mathrm{NEXP}$)

Self-testing and complexity theory

- Motivation: what is the power of **interactive proof systems** with entangled quantum provers (MIP*)?
  - $\approx$ hardness of approximating the **value** of a protocol (maximal success probability of any entangled strategy)
- **Classically:** NP-hard to approximate unentangled value up to constant error (MIP $=$ NEXP)
- **Quantumly:**

Self-testing and complexity theory

- Motivation: what is the power of **interactive proof systems** with entangled quantum provers (MIP^*)?
  - $\approx$ hardness of approximating the **value** of a protocol (maximal success probability of any entangled strategy)
- **Classically:** NP-hard to approximate unentangled value up to constant error ($\text{MIP} = \text{NEXP}$)
- **Quantumly:**
  - NP-hard to approximate entangled value up to constant error

Self-testing and complexity theory

- Motivation: what is the power of **interactive proof systems** with entangled quantum provers (MIP^*)?
  - $\approx$ hardness of approximating the **value** of a protocol (maximal success probability of any entangled strategy)
- **Classically:** NP-hard to approximate unentangled value up to constant error ($MIP = NEXP$)
- **Quantumly:**
  - NP-hard to approximate entangled value up to constant error with 3 or more players.

Self-testing and complexity theory

- Motivation: what is the power of **interactive proof systems** with entangled quantum provers (MIP^*)?
  - $\approx$ hardness of approximating the **value** of a protocol (maximal success probability of any entangled strategy)
- **Classically:** NP-hard to approximate unentangled value up to constant error ($\mathrm{MIP} = \mathrm{NEXP}$)
- **Quantumly:**
  - NP-hard to approximate entangled value up to constant error with 3 or more players.
  - Conjecture ("games QPCP"): it is QMA-hard to approximate entangled value up to constant error

Self-testing and complexity theory

- Motivation: what is the power of **interactive proof systems** with entangled quantum provers (MIP^*)?
  - $\approx$ hardness of approximating the **value** of a protocol (maximal success probability of any entangled strategy)
- **Classically:** NP-hard to approximate unentangled value up to constant error ($\mathrm{MIP} = \mathrm{NEXP}$)
- **Quantumly:**
  - NP-hard to approximate entangled value up to constant error with 3 or more players.
  - Conjecture ("games QPCP"): it is QMA-hard to approximate entangled value up to constant error
- To show QMA-hardness of entangled value, design **self-test** for a QMA witness state $|\psi\rangle$ (e.g. ground state of local Hamiltonian)

Results: Complexity Theory

Theorem

It is NP*-hard to approximate the entangled value of a 2-player nonlocal game, up to constant additive error.*

Results: Complexity Theory

Theorem

It is NP*-hard to approximate the entangled value of a 2-player nonlocal game, up to constant additive error.*

Theorem ("Weak games QPCP")

It is QMA*-hard under randomized reductions to approximate up to constant error the value of an* MIP^* *protocol with* $\mathrm{poly}\log(n)$ *rounds and bits of communication.*

Results: Complexity Theory

Theorem

It is NP*-hard to approximate the entangled value of a 2-player nonlocal game, up to constant additive error.*

Theorem ("Weak games QPCP")

It is QMA*-hard under randomized reductions to approximate up to constant error the value of an* MIP* *protocol with* $\operatorname{poly}\log(n)$ *rounds and bits of communication.*

Theorem ("Hamiltonian QPCP $\Longrightarrow$ Games QPCP")

If it is QMA*-hard to estimate ground energy of local H up to constant fraction, then previous theorem holds under deterministic reductions.*

Designing the Test: Intuition from Codes

- Need to find a small, “robust” subset of the Pauli group to test.

Designing the Test: Intuition from Codes

- Need to find a small, “robust” subset of the Pauli group to test.
- Approach 1: **all** $X(a)$ and $Z(a)$ for $a \in \mathbb{F}_2^n$.

Designing the Test: Intuition from Codes

- Need to find a small, “robust” subset of the Pauli group to test.
- Approach 1: **all** $X(a)$ and $Z(a)$ for $a \in \mathbb{F}_2^n$. ✗–too big!

Designing the Test: Intuition from Codes

- Need to find a small, "robust" subset of the Pauli group to test.
- Approach 1: **all** $X(a)$ and $Z(a)$ for $a \in \mathbb{F}_2^n$. ✗–too big!
- Approach 2: only **constant weight** $X(a), Z(a)$ ($|a| = O(1)$).

Designing the Test: Intuition from Codes

- Need to find a small, "robust" subset of the Pauli group to test.
- Approach 1: **all** $X(a)$ and $Z(a)$ for $a \in \mathbb{F}_2^n$. ✗–too big!
- Approach 2: only **constant weight** $X(a), Z(a)$ ($|a| = O(1)$). ✗–not robust!

Designing the Test: Intuition from Codes

- Need to find a small, “robust” subset of the Pauli group to test.
- Approach 1: **all** $X(a)$ and $Z(a)$ for $a \in \mathbb{F}_2^n$. ✗–too big!
- Approach 2: only **constant weight** $X(a), Z(a)$ ($|a| = O(1)$). ✗–not robust!
- Our approach: $\{X(a), Z(a) : a \in S\}$ with S the set of columns of generator matrix for classical linear code C encoding n bits.

Designing the Test: Intuition from Codes

- Need to find a small, “robust” subset of the Pauli group to test.
- Approach 1: **all** $X(a)$ and $Z(a)$ for $a \in \mathbb{F}_2^n$. ✗–too big!
- Approach 2: only **constant weight** $X(a), Z(a)$ ($|a| = O(1)$). ✗–not robust!
- Our approach: $\{X(a), Z(a) : a \in S\}$ with S the set of columns of generator matrix for classical linear code C encoding n bits.
  - Reduces to Approach 1 ($C =$ Hadamard code)

Designing the Test: Intuition from Codes

- Need to find a small, “robust” subset of the Pauli group to test.
- Approach 1: **all** $X(a)$ and $Z(a)$ for $a \in \mathbb{F}_2^n$. ✗–too big!
- Approach 2: only **constant weight** $X(a), Z(a)$ ($|a| = O(1)$). ✗–not robust!
- Our approach: $\{X(a), Z(a) : a \in S\}$ with S the set of columns of generator matrix for classical linear code C encoding n bits.
  - Reduces to Approach 1 ($C =$ Hadamard code) and 2 ($C =$ trivial code)

Designing the Test: Intuition from Codes

- Need to find a small, “robust” subset of the Pauli group to test.
- Approach 1: **all** $X(a)$ and $Z(a)$ for $a \in \mathbb{F}_2^n$. ✗–too big!
- Approach 2: only **constant weight** $X(a), Z(a)$ ($|a| = O(1)$). ✗–not robust!
- Our approach: $\{X(a), Z(a) : a \in S\}$ with S the set of columns of generator matrix for classical linear code C encoding n bits.
  - Reduces to Approach 1 ($C =$ Hadamard code) and 2 ($C =$ trivial code)
  - S is ✓small if C has high rate.

Designing the Test: Intuition from Codes

- Need to find a small, "robust" subset of the Pauli group to test.
- Approach 1: **all** $X(a)$ and $Z(a)$ for $a \in \mathbb{F}_2^n$. ✗–too big!
- Approach 2: only **constant weight** $X(a), Z(a)$ ($|a| = O(1)$). ✗–not robust!
- Our approach: $\{X(a), Z(a) : a \in S\}$ with S the set of columns of generator matrix for classical linear code C encoding n bits.
  - Reduces to Approach 1 ($C =$ Hadamard code) and 2 ($C =$ trivial code)
  - S is ✓small if C has high rate.
  - S is ✓robust if C has high distance and is locally testable.

Designing the Test: Intuition from Codes

- Need to find a small, “robust” subset of the Pauli group to test.
- Approach 1: **all** $X(a)$ and $Z(a)$ for $a \in \mathbb{F}_2^n$. ✗–too big!
- Approach 2: only **constant weight** $X(a), Z(a)$ ($|a| = O(1)$). ✗–not robust!
- Our approach: $\{X(a), Z(a) : a \in S\}$ with S the set of columns of generator matrix for classical linear code C encoding n bits.
  - Reduces to Approach 1 ($C =$ Hadamard code)
    and 2 ($C =$ trivial code)
  - S is ✓small if C has high rate.
  - S is ✓robust if C has high distance and is locally testable.
- Take C to be Reed-Muller code, based on multivariate polynomials over finite fields. Locally testable by low-degree test [RS97]

Quantum low-degree test

With probability $1/3$ each, perform one of the following:

Quantum low-degree test

With probability $1/3$ each, perform one of the following:

- Tell both players to measure in X basis, and run RS low-degree test.

Quantum low-degree test

With probability $1/3$ each, perform one of the following:

- Tell both players to measure in X basis, and run RS low-degree test.
  - Tests $X(a)$ for $a \in S$

Quantum low-degree test

With probability $1/3$ each, perform one of the following:

- Tell both players to measure in X basis, and run RS low-degree test.
  - Tests $X(a)$ for $a \in S$
- Tell both players to measure in Z basis, and run RS low-degree test.

Quantum low-degree test

With probability $1/3$ each, perform one of the following:

- Tell both players to measure in X basis, and run RS low-degree test.
  - Tests $X(a)$ for $a \in S$
- Tell both players to measure in Z basis, and run RS low-degree test.
  - Tests $Z(b)$ for $b \in S$

Quantum low-degree test

With probability $1/3$ each, perform one of the following:

- Tell both players to measure in X basis, and run RS low-degree test.
  - Tests $X(a)$ for $a \in S$
- Tell both players to measure in Z basis, and run RS low-degree test.
  - Tests $Z(b)$ for $b \in S$
- Pick $a, b \in S$, and play Magic Square game.

Quantum low-degree test

With probability $1/3$ each, perform one of the following:

- Tell both players to measure in X basis, and run RS low-degree test.
  - Tests $X(a)$ for $a \in S$
- Tell both players to measure in Z basis, and run RS low-degree test.
  - Tests $Z(b)$ for $b \in S$
- Pick $a, b \in S$, and play Magic Square game.
  - Tests $X(a)Z(b) = (-1)^{a \cdot b} Z(b)X(a)$

Quantum low-degree test

With probability $1/3$ each, perform one of the following:

- Tell both players to measure in X basis, and run RS low-degree test.
  - Tests $X(a)$ for $a \in S$
- Tell both players to measure in Z basis, and run RS low-degree test.
  - Tests $Z(b)$ for $b \in S$
- Pick $a, b \in S$, and play Magic Square game.
  - Tests $X(a)Z(b) = (-1)^{a \cdot b} Z(b)X(a)$

Lemma (Main)

Suppose players' operators $M_X(a), M_Z(b)$ acting on $|\psi\rangle$ pass test with prob $1 - \varepsilon$. Then $\exists$ local isometry V s.t.

$$M_X(a)|\psi\rangle \approx V^\dagger X(a) V|\psi\rangle \quad M_Z(b)|\psi\rangle \approx V^\dagger Z(b) V|\psi\rangle$$

for $a, b \in S$.

Open problems

- Can we prove the games PCP conjecture?

Open problems

- Can we prove the games PCP conjecture?
  - Need self-tests for a richer class of Hamiltonians, or QMA-hardness for those we can test.

Open problems

- Can we prove the games PCP conjecture?
  - Need self-tests for a richer class of Hamiltonians, or QMA-hardness for those we can test.
- Efficient delegated computation?

Open problems

- Can we prove the games PCP conjecture?
  - Need self-tests for a richer class of Hamiltonians, or QMA-hardness for those we can test.
- Efficient delegated computation?
  - Using post-hoc framework of [FH15], or verifier-on-a-leash framework of [CGJV17]

Open problems

- Can we prove the games PCP conjecture?
  - Need self-tests for a richer class of Hamiltonians, or QMA-hardness for those we can test.
- Efficient delegated computation?
  - Using post-hoc framework of [FH15], or verifier-on-a-leash framework of [CGJV17]
- Noise-tolerant entanglement tests?

Open problems

- Can we prove the games PCP conjecture?
  - Need self-tests for a richer class of Hamiltonians, or QMA-hardness for those we can test.
- Efficient delegated computation?
  - Using post-hoc framework of [FH15], or verifier-on-a-leash framework of [CGJV17]
- Noise-tolerant entanglement tests?
  - Need guarantees even when success probability is far from optimal, as in [AFY17]

Thank You!

arXiv: 1710.03062 & 1801.03821