Injective tensor norms and open problems in quantum information

Ashley Montanaro

Centre for Quantum Information and Foundations,
Department of Applied Mathematics and Theoretical Physics,
University of Cambridge

January 19, 2012

EPSRC Engineering and Physical Sciences Research Council

Introduction

This talk is about how several interesting open problems in quantum information can be phrased in terms of injective tensor norms:

- Finding the pure quantum state which is most entangled with respect to the geometric measure of entanglement;
- Determining whether multiple-prover quantum Merlin-Arthur games obey a parallel repetition theorem;
- Deciding whether quantum query algorithms can be simulated by classical query algorithms on most inputs.

Injective tensor norms

For me …

- a *n*-index tensor T is a multidimensional $\overbrace{d \times d \times \cdots \times d}^{n}$ array of (usually complex) numbers.

Injective tensor norms

For me …

- a *n*-index tensor T is a multidimensional $\overbrace{d \times d \times \cdots \times d}^{n}$ array of (usually complex) numbers.
- a tensor is identified with a multilinear form $f_T : (\mathbb{C}^d)^n \to \mathbb{C}$ by

$$f_T(e^{x_1}, \ldots, e^{x_n}) = T_{x_1, \ldots, x_n},$$

where $e^{x_1}, \ldots, e^{x_n}$ are vectors in the standard basis.

Injective tensor norms

For me …

- a *n*-index tensor T is a multidimensional $\overbrace{d \times d \times \cdots \times d}^{n}$ array of (usually complex) numbers.
- a tensor is identified with a multilinear form $f_T : (\mathbb{C}^d)^n \to \mathbb{C}$ by

$$f_T(e^{x_1}, \ldots, e^{x_n}) = T_{x_1,\ldots,x_n},$$

  where $e^{x_1}, \ldots, e^{x_n}$ are vectors in the standard basis.
- the injective tensor norm $\|T\|_p^{\text{inj}}$ is defined as

$$\|T\|_p^{\text{inj}} \quad := \quad \max\left\{|f_T(v_1, \ldots, v_n)|, \|v_i\|_p \leqslant 1,\ i = 1, \ldots, n\right\}$$

Injective tensor norms

For me ...

- a *n*-index tensor T is a multidimensional $\overbrace{d \times d \times \cdots \times d}^{n}$ array of (usually complex) numbers.
- a tensor is identified with a multilinear form $f_T : (\mathbb{C}^d)^n \to \mathbb{C}$ by

$$f_T(e^{x_1}, \ldots, e^{x_n}) = T_{x_1,\ldots,x_n},$$

  where $e^{x_1}, \ldots, e^{x_n}$ are vectors in the standard basis.
- the injective tensor norm $\|T\|_p^{\text{inj}}$ is defined as

$$\begin{aligned} \|T\|_p^{\text{inj}} &:= \max\left\{|f_T(v_1, \ldots, v_n)|, \|v_i\|_p \leqslant 1, \ i = 1, \ldots, n\right\} \\ &= \max\left\{\left|\sum_{i_1,\ldots,i_n=1}^{d} T_{i_1,\ldots,i_n} \alpha^1_{i_1} \ldots \alpha^n_{i_n}\right|, \sum_{j=1}^{d} |\alpha^i_j|^p \leqslant 1\right\} \end{aligned}$$

Injective tensor norms

Examples:

- If T is a 0-index tensor (i.e. a scalar), $\|T\|_p^{\text{inj}} = |T|$.

Injective tensor norms

Examples:

- If T is a 0-index tensor (i.e. a scalar), $\|T\|_p^{\text{inj}} = |T|$.
- If T is a 1-index tensor (i.e. a vector),

$$\|T\|_p^{\text{inj}} = \|T\|_{p'},$$

where p' is dual to p, i.e. $1/p + 1/p' = 1$.

Injective tensor norms

Examples:

- If T is a 0-index tensor (i.e. a scalar), $\|T\|_p^{\text{inj}} = |T|$.
- If T is a 1-index tensor (i.e. a vector),

  $$\|T\|_p^{\text{inj}} = \|T\|_{p'},$$

  where p' is dual to p, i.e. $1/p + 1/p' = 1$.
- If T is a 2-index tensor (i.e. a matrix),

  $$\|T\|_p^{\text{inj}} = \|T\|_{p \to p'},$$

  where for any matrix M

  $$\|M\|_{p \to q} := \max_{v, \|v\|_p = 1} \|Mv\|_q.$$

  When $p = 2$ this is the operator norm $\|T\|_{\text{op}}$, i.e. the largest singular value of T.

The geometric measure of entanglement

Let $|\psi\rangle \in B((\mathbb{C}^d)^{\otimes n})$ be a pure quantum state of n d-dimensional systems.

- $|\psi\rangle$ is said to be product if

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle = |\psi_1, \ldots, \psi_n\rangle.$$

The geometric measure of entanglement

Let $|\psi\rangle \in B((\mathbb{C}^d)^{\otimes n})$ be a pure quantum state of n d-dimensional systems.

- $|\psi\rangle$ is said to be product if

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle = |\psi_1, \ldots, \psi_n\rangle.$$

- The geometric measure of entanglement is defined as

$$E_{\text{geom}}(|\psi\rangle) := -\log_2 \max_{|\phi_1\rangle,\ldots,|\phi_n\rangle \in B(\mathbb{C}^d)} |\langle\psi|\phi_1, \ldots, \phi_n\rangle|^2.$$

The geometric measure of entanglement

Let $|\psi\rangle \in B((\mathbb{C}^d)^{\otimes n})$ be a pure quantum state of n d-dimensional systems.

- $|\psi\rangle$ is said to be product if

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle = |\psi_1, \ldots, \psi_n\rangle.$$

- The geometric measure of entanglement is defined as

$$E_{\text{geom}}(|\psi\rangle) := -\log_2 \max_{|\phi_1\rangle,\ldots,|\phi_n\rangle \in B(\mathbb{C}^d)} |\langle\psi|\phi_1, \ldots, \phi_n\rangle|^2.$$

- If we think of $|\psi\rangle$ as an n-index tensor ψ, where $\psi_{i_1,\ldots,i_n} = \langle\psi|i_1, \ldots, i_n\rangle$,

$$E_{\text{geom}}(|\psi\rangle) = -2\log_2 \|\psi\|_2^{\text{inj}}.$$

The geometric measure of entanglement

Let $|\psi\rangle \in B((\mathbb{C}^d)^{\otimes n})$ be a pure quantum state of n d-dimensional systems.

- $|\psi\rangle$ is said to be product if

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle = |\psi_1, \dots, \psi_n\rangle.$$

- The geometric measure of entanglement is defined as

$$E_{\text{geom}}(|\psi\rangle) := -\log_2 \max_{|\phi_1\rangle,\dots,|\phi_n\rangle \in B(\mathbb{C}^d)} |\langle\psi|\phi_1, \dots, \phi_n\rangle|^2.$$

- If we think of $|\psi\rangle$ as an n-index tensor ψ, where $\psi_{i_1,\dots,i_n} = \langle\psi|i_1, \dots, i_n\rangle$,

$$E_{\text{geom}}(|\psi\rangle) = -2\log_2 \|\psi\|_2^{\text{inj}}.$$

- Observe that trivially $0 \leqslant E_{\text{geom}}(|\psi\rangle) \leqslant n \log_2 d$, by writing $|\psi\rangle$ in an arbitrary product basis.

The geometric measure of entanglement

Open problem 1

What is
$$\max_{|\psi\rangle \in B((\mathbb{C}^d)^{\otimes n})} E_{\text{geom}}(|\psi\rangle)?$$

The geometric measure of entanglement

Open problem 1

What is

$$\max_{|\psi\rangle \in B((\mathbb{C}^d)^{\otimes n})} E_{\mathrm{geom}}(|\psi\rangle)?$$

- In other words, what is $\min_T \|T\|_2^{\mathrm{inj}}$, given that $\sum_{i_1,\dots,i_n} |T_{i_1,\dots,i_n}|^2 = 1$?

The geometric measure of entanglement

Open problem 1

What is

$$\max_{|\psi\rangle \in B((\mathbb{C}^d)^{\otimes n})} E_{\text{geom}}(|\psi\rangle)?$$

- In other words, what is $\min_T \|T\|_2^{\text{inj}}$, given that $\sum_{i_1,\dots,i_n} |T_{i_1,\dots,i_n}|^2 = 1$?
- As far as I know, still open for $d = 2$ (qubits)!

The geometric measure of entanglement

Open problem 1

What is

$$\max_{|\psi\rangle \in B((\mathbb{C}^d)^{\otimes n})} E_{\text{geom}}(|\psi\rangle)?$$

- In other words, what is $\min_T \|T\|_2^{\text{inj}}$, given that $\sum_{i_1,\dots,i_n} |T_{i_1,\dots,i_n}|^2 = 1$?
- As far as I know, still open for $d = 2$ (qubits)!
- Application: Can be used to replace finding the ground-state energy of a local Hamiltonian (a QMA-hard problem) with an optimisation over product states (in the complexity class NP) [Gharibian and Kempe '11].

The geometric measure of entanglement

Open problem 1

What is

$$\max_{|\psi\rangle \in B((\mathbb{C}^d)^{\otimes n})} E_{\text{geom}}(|\psi\rangle)?$$

- In other words, what is $\min_T \|T\|_2^{\text{inj}}$, given that $\sum_{i_1,\dots,i_n} |T_{i_1,\dots,i_n}|^2 = 1$?
- As far as I know, still open for $d = 2$ (qubits)!
- Application: Can be used to replace finding the ground-state energy of a local Hamiltonian (a QMA-hard problem) with an optimisation over product states (in the complexity class NP) [Gharibian and Kempe '11].
- But a very natural question in its own right! "What is the most entangled quantum state?"

Some (easy and well-known) partial results

Proposition

For any $|\psi\rangle \in B(\mathbb{C}^d \otimes \mathbb{C}^d)$, $E_{\mathrm{geom}}(|\psi\rangle) \leqslant \log_2 d$, which is achieved by

$$|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle|i\rangle.$$

Some (easy and well-known) partial results

Proposition

For any $|\psi\rangle \in B(\mathbb{C}^d \otimes \mathbb{C}^d)$, $E_{\text{geom}}(|\psi\rangle) \leqslant \log_2 d$, which is achieved by

$$|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle|i\rangle.$$

Proof:

$$E_{\text{geom}}(|\psi\rangle) = -2\log_2 \|\psi\|_2^{\text{inj}}$$

Some (easy and well-known) partial results

Proposition

For any $|\psi\rangle \in B(\mathbb{C}^d \otimes \mathbb{C}^d)$, $E_{\text{geom}}(|\psi\rangle) \leqslant \log_2 d$, which is achieved by

$$|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle|i\rangle.$$

Proof:

$$\begin{aligned} E_{\text{geom}}(|\psi\rangle) &= -2\log_2 \|\psi\|_2^{\text{inj}} \\ &= \log_2(1/\|\psi\|_{\text{op}}^2) \end{aligned}$$

Some (easy and well-known) partial results

Proposition

For any $|\psi\rangle \in B(\mathbb{C}^d \otimes \mathbb{C}^d)$, $E_{\text{geom}}(|\psi\rangle) \leqslant \log_2 d$, which is achieved by

$$|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle|i\rangle.$$

Proof:

$$\begin{aligned} E_{\text{geom}}(|\psi\rangle) &= -2\log_2 \|\psi\|_2^{\text{inj}} \\ &= \log_2(1/\|\psi\|_{\text{op}}^2) \\ &\leqslant \log_2(d/\|\psi\|_2^2) \end{aligned}$$

Some (easy and well-known) partial results

Proposition

For any $|\psi\rangle \in B(\mathbb{C}^d \otimes \mathbb{C}^d)$, $E_{\text{geom}}(|\psi\rangle) \leqslant \log_2 d$, which is achieved by

$$|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle|i\rangle.$$

Proof:

$$\begin{aligned} E_{\text{geom}}(|\psi\rangle) &= -2\log_2 \|\psi\|_2^{\text{inj}} \\ &= \log_2(1/\|\psi\|_{\text{op}}^2) \\ &\leqslant \log_2(d/\|\psi\|_2^2) \\ &= \log_2 d. \end{aligned}$$

Some (easy and well-known) partial results

Proposition

For any $|\psi\rangle \in B((\mathbb{C}^d)^{\otimes n})$, $E_{\mathrm{geom}}(|\psi\rangle) \leqslant (n-1)\log_2 d$.
Equivalently, $(\|\psi\|_2^{\mathrm{inj}})^2 \geqslant d^{1-n}$.

Some (easy and well-known) partial results

Proposition

For any $|\psi\rangle \in B((\mathbb{C}^d)^{\otimes n})$, $E_{\text{geom}}(|\psi\rangle) \leqslant (n-1)\log_2 d$.
Equivalently, $(\|\psi\|_2^{\text{inj}})^2 \geqslant d^{1-n}$.

Comments on this result:

- Has been rediscovered independently several times in the quantum information literature, e.g. [Jung et al '08], [Gharibian and Kempe '11], ...

Some (easy and well-known) partial results

Proposition

For any $|\psi\rangle \in B((\mathbb{C}^d)^{\otimes n})$, $E_{\text{geom}}(|\psi\rangle) \leqslant (n-1)\log_2 d$.
Equivalently, $(\|\psi\|_2^{\text{inj}})^2 \geqslant d^{1-n}$.

Comments on this result:

- Has been rediscovered independently several times in the quantum information literature, e.g. [Jung et al '08], [Gharibian and Kempe '11], ...
- [Jung et al '08] show that this cannot be tight for $n > 2$.

Some (easy and well-known) partial results

Proposition

For any $|\psi\rangle \in B((\mathbb{C}^d)^{\otimes n})$, $E_{\text{geom}}(|\psi\rangle) \leqslant (n-1)\log_2 d$.
Equivalently, $(\|\psi\|_2^{\text{inj}})^2 \geqslant d^{1-n}$.

Comments on this result:

- Has been rediscovered independently several times in the quantum information literature, e.g. [Jung et al '08], [Gharibian and Kempe '11], ...
- [Jung et al '08] show that this cannot be tight for $n > 2$.
- For any symmetric state $|\psi\rangle$, the (often much tighter) bound

$$E_{\text{geom}}(|\psi\rangle) \leqslant \log_2 \binom{n+d-1}{d-1} = O(d(\log n + \log d))$$

holds (e.g. see [Aulbach '11]).

Some (easy and well-known) partial results

Proposition

For any $|\psi\rangle \in B((\mathbb{C}^d)^{\otimes n})$, $E_{\text{geom}}(|\psi\rangle) \leqslant (n-1)\log_2 d$.
Equivalently, $(\|\psi\|_2^{\text{inj}})^2 \geqslant d^{1-n}$.

Some (easy and well-known) partial results

Proposition

For any $|\psi\rangle \in B((\mathbb{C}^d)^{\otimes n})$, $E_{\mathrm{geom}}(|\psi\rangle) \leqslant (n-1)\log_2 d$.
Equivalently, $(\|\psi\|_2^{\mathrm{inj}})^2 \geqslant d^{1-n}$.

$$(\|\psi\|_2^{\mathrm{inj}})^2 = \max_{\phi^1,\ldots,\phi^n} \left| \sum_{i_1,\ldots,i_n=1}^{d} \psi_{i_1,\ldots,i_n} \phi^1_{i_1} \ldots \phi^n_{i_n} \right|^2$$

Some (easy and well-known) partial results

Proposition

For any $|\psi\rangle \in B((\mathbb{C}^d)^{\otimes n})$, $E_{\text{geom}}(|\psi\rangle) \leqslant (n-1)\log_2 d$.
Equivalently, $(\|\psi\|_2^{\text{inj}})^2 \geqslant d^{1-n}$.

$$
\begin{aligned}
(\|\psi\|_2^{\text{inj}})^2 &= \max_{\phi^1,\ldots,\phi^n} \left| \sum_{i_1,\ldots,i_n=1}^{d} \psi_{i_1,\ldots,i_n} \phi^1_{i_1} \ldots \phi^n_{i_n} \right|^2 \\
&= \max_{\phi^2,\ldots,\phi^n} \sum_{i_1=1}^{d} \left| \sum_{i_2,\ldots,i_n=1}^{d} \psi_{i_1,\ldots,i_n} \phi^2_{i_2} \ldots \phi^n_{i_n} \right|^2
\end{aligned}
$$

Some (easy and well-known) partial results

Proposition

For any $|\psi\rangle \in B((\mathbb{C}^d)^{\otimes n})$, $E_{\mathrm{geom}}(|\psi\rangle) \leqslant (n-1)\log_2 d$.
Equivalently, $(\|\psi\|_2^{\mathrm{inj}})^2 \geqslant d^{1-n}$.

$$\begin{aligned}
(\|\psi\|_2^{\mathrm{inj}})^2 &= \max_{\phi^1,\ldots,\phi^n} \left| \sum_{i_1,\ldots,i_n=1}^{d} \psi_{i_1,\ldots,i_n} \phi^1_{i_1} \ldots \phi^n_{i_n} \right|^2 \\
&= \max_{\phi^2,\ldots,\phi^n} \sum_{i_1=1}^{d} \left| \sum_{i_2,\ldots,i_n=1}^{d} \psi_{i_1,\ldots,i_n} \phi^2_{i_2} \ldots \phi^n_{i_n} \right|^2 \\
&\geqslant \sum_{i_1=1}^{d} \mathbb{E}_{\phi^2,\ldots,\phi^n} \left| \sum_{i_2,\ldots,i_n=1}^{d} \psi_{i_1,\ldots,i_n} \phi^2_{i_2} \ldots \phi^n_{i_n} \right|^2
\end{aligned}$$

Some (easy and well-known) partial results

Proposition

For any $|\psi\rangle \in B((\mathbb{C}^d)^{\otimes n})$, $E_{\text{geom}}(|\psi\rangle) \leqslant (n-1)\log_2 d$.
Equivalently, $(\|\psi\|_2^{\text{inj}})^2 \geqslant d^{1-n}$.

$$\begin{aligned}
(\|\psi\|_2^{\text{inj}})^2 &= \max_{\phi^1,\dots,\phi^n} \left| \sum_{i_1,\dots,i_n=1}^{d} \psi_{i_1,\dots,i_n} \phi^1_{i_1} \dots \phi^n_{i_n} \right|^2 \\
&= \max_{\phi^2,\dots,\phi^n} \sum_{i_1=1}^{d} \left| \sum_{i_2,\dots,i_n=1}^{d} \psi_{i_1,\dots,i_n} \phi^2_{i_2} \dots \phi^n_{i_n} \right|^2 \\
&\geqslant \sum_{i_1=1}^{d} \mathbb{E}_{\phi^2,\dots,\phi^n} \left| \sum_{i_2,\dots,i_n=1}^{d} \psi_{i_1,\dots,i_n} \phi^2_{i_2} \dots \phi^n_{i_n} \right|^2 \\
&= \frac{1}{d^{n-1}} \sum_{i_1=1}^{d} \sum_{i_2,\dots,i_n=1}^{d} |\psi_{i_1,\dots,i_n}|^2 = \frac{1}{d^{n-1}}.
\end{aligned}$$

Some (easy and well-known) partial results

Proposition

Pick $|\psi\rangle \in B((\mathbb{C}^d)^{\otimes n})$ at random (according to Haar measure). Then with high probability

$$E_{\text{geom}}(|\psi\rangle) \geqslant (n - \log_2 n)\log_2 d - \log_2(9/2).$$

Some (easy and well-known) partial results

Proposition

Pick $|\psi\rangle \in B((\mathbb{C}^d)^{\otimes n})$ at random (according to Haar measure). Then with high probability

$$E_{\text{geom}}(|\psi\rangle) \geqslant (n - \log_2 n)\log_2 d - \log_2(9/2).$$

- So random quantum states have geometric measure which is close to maximal.

Some (easy and well-known) partial results

Proposition

Pick $|\psi\rangle \in B((\mathbb{C}^d)^{\otimes n})$ at random (according to Haar measure). Then with high probability

$$E_{\text{geom}}(|\psi\rangle) \geqslant (n - \log_2 n) \log_2 d - \log_2(9/2).$$

- So random quantum states have geometric measure which is close to maximal.
- In the quantum information literature, originally proven for $d = 2$ by [Gross, Flammia, Eisert '08], and extended to general d by [Zhu, Chen, Hayashi '10].

Some (easy and well-known) partial results

Proposition

Pick $|\psi\rangle \in B((\mathbb{C}^d)^{\otimes n})$ at random (according to Haar measure). Then with high probability

$$E_{\text{geom}}(|\psi\rangle) \geqslant (n - \log_2 n) \log_2 d - \log_2(9/2).$$

- So random quantum states have geometric measure which is close to maximal.
- In the quantum information literature, originally proven for $d = 2$ by [Gross, Flammia, Eisert '08], and extended to general d by [Zhu, Chen, Hayashi '10].
- No known candidate for an explicit quantum state which beats this bound!

From injective tensor norms to quantum Merlin-Arthur games

- A separable state $\rho \in \mathrm{SEP} \subset \mathcal{B}(\mathbb{C}^d \otimes \mathbb{C}^d)$ is a state of the form
$$\rho = \sum_i p_i \rho_i \otimes \sigma_i,$$
where ρ_i, σ_i are quantum states (density matrices).

From injective tensor norms to quantum Merlin-Arthur games

- A separable state $\rho \in \mathrm{SEP} \subset \mathcal{B}(\mathbb{C}^d \otimes \mathbb{C}^d)$ is a state of the form
$$\rho = \sum_i p_i \rho_i \otimes \sigma_i,$$
where ρ_i, σ_i are quantum states (density matrices).
- Define the support function of the separable states,

$$\begin{aligned} h_{\mathrm{SEP}}(M) &:= \max_{\rho \in \mathrm{SEP}} \operatorname{tr} M\rho \\ &= \max_{|\phi_1\rangle, |\phi_2\rangle \in B(\mathbb{C}^d)} \langle \phi_1 | \langle \phi_2 | M | \phi_1 \rangle | \phi_2 \rangle \end{aligned}$$

From injective tensor norms to quantum Merlin-Arthur games

- A separable state $\rho \in \mathrm{SEP} \subset \mathcal{B}(\mathbb{C}^d \otimes \mathbb{C}^d)$ is a state of the form
$$\rho = \sum_i p_i \rho_i \otimes \sigma_i,$$
where ρ_i, σ_i are quantum states (density matrices).
- Define the support function of the separable states,
$$\begin{aligned} h_{\mathrm{SEP}}(M) &:= \max_{\rho \in \mathrm{SEP}} \operatorname{tr} M\rho \\ &= \max_{|\phi_1\rangle, |\phi_2\rangle \in B(\mathbb{C}^d)} \langle\phi_1|\langle\phi_2|M|\phi_1\rangle|\phi_2\rangle \end{aligned}$$
- It turns out that h_{SEP} can be expressed in terms of injective tensor norms.

h_{SEP} and injective tensor norms

Let $T_{i,j,k}$ be an arbitrary 3-index tensor. Then

$$(\|T\|_2^{\text{inj}})^2 = \max_{x,y,z \in B(\mathbb{C}^d)} \left| \sum_{i,j,k=1}^{d} T_{i,j,k} x_i y_j z_k \right|^2$$

h_{SEP} and injective tensor norms

Let $T_{i,j,k}$ be an arbitrary 3-index tensor. Then

$$
\begin{aligned}
(\|T\|_2^{\text{inj}})^2 &= \max_{x,y,z \in B(\mathbb{C}^d)} \left| \sum_{i,j,k=1}^{d} T_{i,j,k} x_i y_j z_k \right|^2 \\
&= \max_{x,y \in B(\mathbb{C}^d)} \left\| \sum_{i,j,k=1}^{d} T_{i,j,k} x_i y_j |k\rangle \right\|_2^2
\end{aligned}
$$

h_{SEP} and injective tensor norms

Let $T_{i,j,k}$ be an arbitrary 3-index tensor. Then

$$
\begin{aligned}
(\|T\|_2^{\text{inj}})^2 &= \max_{x,y,z\in B(\mathbb{C}^d)} \left| \sum_{i,j,k=1}^{d} T_{i,j,k} x_i y_j z_k \right|^2 \\
&= \max_{x,y\in B(\mathbb{C}^d)} \left\| \sum_{i,j,k=1}^{d} T_{i,j,k} x_i y_j |k\rangle \right\|_2^2 \\
&= \max_{x,y\in B(\mathbb{C}^d)} \sum_{i,j,i',j',k=1}^{d} T_{i,j,k} T^*_{i',j',k} x_i y_j x^*_{i'} y^*_{j'}
\end{aligned}
$$

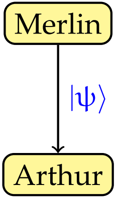
h_{SEP} and injective tensor norms

Let $T_{i,j,k}$ be an arbitrary 3-index tensor. Then

$$
\begin{aligned}
(\|T\|_2^{\mathrm{inj}})^2 &= \max_{x,y,z \in B(\mathbb{C}^d)} \left| \sum_{i,j,k=1}^{d} T_{i,j,k} x_i y_j z_k \right|^2 \\
&= \max_{x,y \in B(\mathbb{C}^d)} \left\| \sum_{i,j,k=1}^{d} T_{i,j,k} x_i y_j |k\rangle \right\|_2^2 \\
&= \max_{x,y \in B(\mathbb{C}^d)} \sum_{i,j,i',j',k=1}^{d} T_{i,j,k} T^*_{i',j',k} x_i y_j x^*_{i'} y^*_{j'} \\
&= h_{\mathrm{SEP}} \left(\sum_{i,j,i',j',k=1}^{d} T_{i,j,k} T^*_{i',j',k} |i\rangle\langle i'| \otimes |j\rangle\langle j'| \right).
\end{aligned}
$$

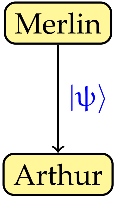
Quantum Merlin-Arthur games

The complexity class QMA is the quantum analogue of NP.



Quantum Merlin-Arthur games

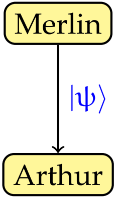
The complexity class QMA is the quantum analogue of NP.



- Arthur has some decision problem of size n to solve, and Merlin wants to convince him that the answer is “yes”.

Quantum Merlin-Arthur games

The complexity class QMA is the quantum analogue of NP.



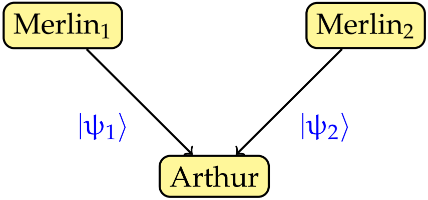
- Arthur has some decision problem of size n to solve, and Merlin wants to convince him that the answer is “yes”.
- Merlin sends him a quantum state $|\psi\rangle$ of poly(n) qubits. Arthur runs some polynomial-time quantum algorithm $\mathcal{A}$ on $|\psi\rangle$ and his input and outputs “yes” if the algorithm says “accept”.

Quantum Merlin-Arthur games

QMA(2) is a variant where Arthur has access to two unentangled Merlins.

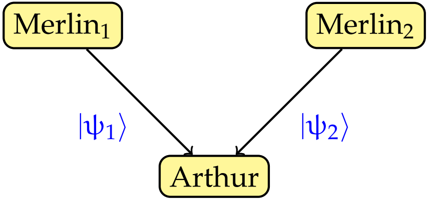
Quantum Merlin-Arthur games

QMA(2) is a variant where Arthur has access to two unentangled Merlins.



Quantum Merlin-Arthur games

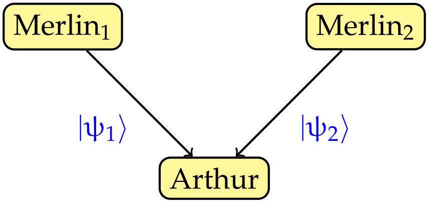
QMA(2) is a variant where Arthur has access to two unentangled Merlins.



- This might be more powerful than QMA because the lack of entanglement helps Arthur tell when the Merlins are cheating.

Quantum Merlin-Arthur games

QMA(2) is a variant where Arthur has access to two unentangled Merlins.



- This might be more powerful than QMA because the lack of entanglement helps Arthur tell when the Merlins are cheating.
- For example, 3-SAT on n clauses can be solved by a QMA(2) protocol with constant probability of error using proofs of length $O(\sqrt{n}\,\mathrm{polylog}(n))$ qubits [Harrow and AM '10].

QMA(2) and h_{SEP}

Fact

For a given "no" problem instance, let Arthur's measurement operator corresponding to a "yes" outcome be M. Then the maximal probability with which the Merlins can force Arthur to incorrectly output "yes" is precisely $h_{\mathrm{SEP}}(M)$.

QMA(2) and h_{SEP}

Fact

For a given "no" problem instance, let Arthur's measurement operator corresponding to a "yes" outcome be M. Then the maximal probability with which the Merlins can force Arthur to incorrectly output "yes" is precisely $h_{\mathrm{SEP}}(M)$.

- Via the connection to 3-SAT, implies computational hardness of approximating $h_{\mathrm{SEP}}(M)$.
- Unless there exists a subexponential-time algorithm for 3-SAT, there is no polynomial-time algorithm for estimating $h_{\mathrm{SEP}}(M)$ up to an additive constant.

Multiplicativity of h_{SEP}

Open problem 2

Is h_{SEP} weakly multiplicative? i.e. does it hold that, for all M,

$$h_{\text{SEP}}(M^{\otimes n}) \leqslant h_{\text{SEP}}(M)^{\alpha n}$$

for some $0 < \alpha < 1$?

Multiplicativity of h_{SEP}

Open problem 2

Is h_{SEP} weakly multiplicative? i.e. does it hold that, for all M,

$$h_{\text{SEP}}(M^{\otimes n}) \leqslant h_{\text{SEP}}(M)^{\alpha n}$$

for some $0 < \alpha < 1$?

- If true, this would imply that QMA(2) protocols obey a form of parallel repetition: to achieve exponentially small failure probability, Arthur can simply repeat the protocol n times in parallel.

Multiplicativity of h_{SEP}

Open problem 2

Is h_{SEP} weakly multiplicative? i.e. does it hold that, for all M,

$$h_{\mathrm{SEP}}(M^{\otimes n}) \leqslant h_{\mathrm{SEP}}(M)^{\alpha n}$$

for some $0 < \alpha < 1$?

- If true, this would imply that QMA(2) protocols obey a form of parallel repetition: to achieve exponentially small failure probability, Arthur can simply repeat the protocol n times in parallel.
- There are also connections to many other open additivity/multiplicativity problems in quantum information theory via a link to maximum output p-norms of quantum channels.

Some known partial results

Theorem [Werner and Holevo '02], [Grudka et al '09]

There exists M such that

$$h_{\mathrm{SEP}}(M^{\otimes 2}) = h_{\mathrm{SEP}}(M)(1 - o(1)).$$

Some known partial results

Theorem [Werner and Holevo '02], [Grudka et al '09]

There exists M such that

$$h_{\mathrm{SEP}}(M^{\otimes 2}) = h_{\mathrm{SEP}}(M)(1 - o(1)).$$

- One can take M to be the projector onto the antisymmetric subspace of $\mathbb{C}^d \otimes \mathbb{C}^d$, or alternatively a random subspace of $\mathbb{R}^d \otimes \mathbb{R}^d$.

Some known partial results

Theorem [Werner and Holevo '02], [Grudka et al '09]

There exists M such that

$$h_{\text{SEP}}(M^{\otimes 2}) = h_{\text{SEP}}(M)(1 - o(1)).$$

- One can take M to be the projector onto the antisymmetric subspace of $\mathbb{C}^d \otimes \mathbb{C}^d$, or alternatively a random subspace of $\mathbb{R}^d \otimes \mathbb{R}^d$.
- This result implies that strict parallel repetition does not hold for QMA(2) protocols.

Some known partial results

Theorem **[Werner and Holevo '02], [Grudka et al '09]**

There exists M such that

$$h_{\mathrm{SEP}}(M^{\otimes 2}) = h_{\mathrm{SEP}}(M)(1 - o(1)).$$

- One can take M to be the projector onto the antisymmetric subspace of $\mathbb{C}^d \otimes \mathbb{C}^d$, or alternatively a random subspace of $\mathbb{R}^d \otimes \mathbb{R}^d$.
- This result implies that strict parallel repetition does not hold for QMA(2) protocols.
- Connected to the failure of the famous additivity conjecture for Holevo capacity of quantum channels [Hastings '09].

Some known partial results

Theorem [AM '11]

Pick the subspace onto which M projects at random (according to Haar measure) from the set of all dimension r subspaces of $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$. Then the probability that $h_{\text{SEP}}(M)$ is *not* weakly multiplicative with exponent $1/2 - o(1)$ is exponentially small in $\min\{r, d_A, d_B\}$.

Some known partial results

Theorem [AM '11]

Pick the subspace onto which M projects at random (according to Haar measure) from the set of all dimension r subspaces of $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$. Then the probability that $h_{\mathrm{SEP}}(M)$ is *not* weakly multiplicative with exponent $1/2 - o(1)$ is exponentially small in $\min\{r, d_A, d_B\}$.

Note: The above result holds with the following (fairly weak) restrictions on r, d_A, d_B:

- $r = o(d_A d_B)$.
- $\min\{r, d_A, d_B\} \geqslant 2(\log_2 \max\{d_A, d_B\})^{3/2}$.

Some known partial results

Theorem [AM '11]

Pick the subspace onto which M projects at random (according to Haar measure) from the set of all dimension r subspaces of $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$. Then the probability that $h_{\text{SEP}}(M)$ is *not* weakly multiplicative with exponent $1/2 - o(1)$ is exponentially small in $\min\{r, d_A, d_B\}$.

Note: The above result holds with the following (fairly weak) restrictions on r, d_A, d_B:

- $r = o(d_A d_B)$.
- $\min\{r, d_A, d_B\} \geqslant 2(\log_2 \max\{d_A, d_B\})^{3/2}$.

The proof uses ideas from random matrix theory.

Simulation of quantum query algorithms

- In the model of quantum query complexity, we want to compute some function $f : \{0,1\}^n \to \{0,1\}$ using the minimum number of queries to the input.

Simulation of quantum query algorithms

- In the model of quantum query complexity, we want to compute some function $f : \{0,1\}^n \to \{0,1\}$ using the minimum number of queries to the input.
- Let $x \in \{0,1\}^n$ be an n-bit string and imagine we can query bits of x at unit cost. We want to compute $f(x)$.

Simulation of quantum query algorithms

- In the model of quantum query complexity, we want to compute some function $f : \{0, 1\}^n \to \{0, 1\}$ using the minimum number of queries to the input.
- Let $x \in \{0, 1\}^n$ be an n-bit string and imagine we can query bits of x at unit cost. We want to compute $f(x)$.
- It is known (e.g. [Simon '94]) that some partial functions f (i.e. functions where is a promise on the input) can be computed using exponentially fewer quantum queries than would be required for any classical algorithm.

Simulation of quantum query algorithms

- In the model of quantum query complexity, we want to compute some function $f : \{0,1\}^n \to \{0,1\}$ using the minimum number of queries to the input.
- Let $x \in \{0,1\}^n$ be an n-bit string and imagine we can query bits of x at unit cost. We want to compute $f(x)$.
- It is known (e.g. [Simon '94]) that some partial functions f (i.e. functions where is a promise on the input) can be computed using exponentially fewer quantum queries than would be required for any classical algorithm.
- On the other hand, for any total function f, there can be at most a polynomial separation between quantum and classical query complexity [Beals et al '01].

Simulation of quantum query algorithms

- In the model of quantum query complexity, we want to compute some function $f : \{0,1\}^n \rightarrow \{0,1\}$ using the minimum number of queries to the input.
- Let $x \in \{0,1\}^n$ be an n-bit string and imagine we can query bits of x at unit cost. We want to compute $f(x)$.
- It is known (e.g. [Simon '94]) that some partial functions f (i.e. functions where is a promise on the input) can be computed using exponentially fewer quantum queries than would be required for any classical algorithm.
- On the other hand, for any total function f, there can be at most a polynomial separation between quantum and classical query complexity [Beals et al '01].
- Raises the natural question: how strict does the promise on the input have to be in order to get an exponential speed-up?

Quantum queries and injective tensor norms

Conjecture A [Aaronson and Ambainis '09]

Let Q be a quantum algorithm which makes T queries to x. Then, for any $\epsilon > 0$, there is a classical algorithm which makes $\text{poly}(T, 1/\epsilon, 1/\delta)$ queries to x, and approximates Q's success probability to within $\pm\epsilon$ on a $1 - \delta$ fraction of inputs.

Quantum queries and injective tensor norms

Conjecture A [Aaronson and Ambainis '09]

Let Q be a quantum algorithm which makes T queries to x. Then, for any $\epsilon > 0$, there is a classical algorithm which makes $\mathrm{poly}(T, 1/\epsilon, 1/\delta)$ queries to x, and approximates Q's success probability to within $\pm\epsilon$ on a $1 - \delta$ fraction of inputs.

- Given known results, essentially the strongest conjecture one could make about classical simulation of quantum query algorithms.

Quantum queries and injective tensor norms

Conjecture A [Aaronson and Ambainis '09]

Let Q be a quantum algorithm which makes T queries to x. Then, for any $\epsilon > 0$, there is a classical algorithm which makes $\text{poly}(T, 1/\epsilon, 1/\delta)$ queries to x, and approximates Q's success probability to within $\pm\epsilon$ on a $1-\delta$ fraction of inputs.

- Given known results, essentially the strongest conjecture one could make about classical simulation of quantum query algorithms.
- Aaronson and Ambainis show that Conjecture A follows from the following, more mathematical conjecture...

Quantum queries and injective tensor norms

Conjecture B [Aaronson and Ambainis '09, slightly modified]

Let $f : \mathbb{R}^n \to \mathbb{R}$ be a degree d multivariate polynomial such that $|f(x)| \leqslant 1$ for all $x \in \{\pm 1\}^n$ and $\mathrm{Var}(f) \geqslant \epsilon$. Then there exists $j \in \{1, \ldots, n\}$ such that

$$\mathrm{Inf}_j(f) \geqslant \mathrm{poly}(\epsilon/d).$$

Quantum queries and injective tensor norms

Conjecture B [Aaronson and Ambainis '09, slightly modified]

Let $f : \mathbb{R}^n \to \mathbb{R}$ be a degree d multivariate polynomial such that $|f(x)| \leqslant 1$ for all $x \in \{\pm 1\}^n$ and $\mathrm{Var}(f) \geqslant \epsilon$. Then there exists $j \in \{1, \ldots, n\}$ such that

$$\mathrm{Inf}_j(f) \geqslant \mathrm{poly}(\epsilon/d).$$

In this conjecture:

$$\begin{aligned}
\mathrm{Var}(f) &= \mathbb{E}_x[(f(x) - \mathbb{E}[f])^2] = \frac{1}{2^n} \sum_{x \in \{\pm 1\}^n} \left(f(x) - \frac{1}{2^n} \sum_{y \in \{\pm 1\}^n} f(x) \right)^2 \\
\mathrm{Inf}_j(f) &= \frac{1}{2^{n+2}} \sum_{x \in \{\pm 1\}^n} (f(x) - f(x^j))^2
\end{aligned}$$

A very special case of this conjecture

- Let $f : (\mathbb{R}^s)^t \to \mathbb{R}$ be the multilinear form corresponding to a tensor $T \in (\mathbb{R}^s)^t$.

A very special case of this conjecture

- Let $f : (\mathbb{R}^s)^t \to \mathbb{R}$ be the multilinear form corresponding to a tensor $T \in (\mathbb{R}^s)^t$.
- Observe that f depends on ts variables $x_{(j,k)}$, where $1 \leqslant j \leqslant t$ and $1 \leqslant k \leqslant s$, and has degree t.

A very special case of this conjecture

- Let $f : (\mathbb{R}^s)^t \to \mathbb{R}$ be the multilinear form corresponding to a tensor $T \in (\mathbb{R}^s)^t$.
- Observe that f depends on ts variables $x_{(j,k)}$, where $1 \leqslant j \leqslant t$ and $1 \leqslant k \leqslant s$, and has degree t.
- The influence of variable (j,k) on f is

$$\mathrm{Inf}_{(j,k)}(f) = \sum_{i_1,\ldots,i_{j-1},i_{j+1},\ldots,i_t} T^2_{i_1,\ldots,i_{j-1},k,i_{j+1},\ldots,i_t}.$$

A very special case of this conjecture

- Let $f : (\mathbb{R}^s)^t \to \mathbb{R}$ be the multilinear form corresponding to a tensor $T \in (\mathbb{R}^s)^t$.
- Observe that f depends on ts variables $x_{(j,k)}$, where $1 \leqslant j \leqslant t$ and $1 \leqslant k \leqslant s$, and has degree t.
- The influence of variable (j,k) on f is

$$\mathrm{Inf}_{(j,k)}(f) = \sum_{i_1,\ldots,i_{j-1},i_{j+1},\ldots,i_t} T^2_{i_1,\ldots,i_{j-1},k,i_{j+1},\ldots,i_t}.$$

Open problem 3

Assume that $\|T\|_\infty^{\mathrm{inj}} \leqslant 1$. Show that, for all $1 \leqslant j \leqslant t$,

$$\sum_{k=1}^{s} \mathrm{Inf}_{(j,k)}(f)^{1/2} \leqslant \mathrm{poly}(t).$$

A very special case of this conjecture

- Let $f : (\mathbb{R}^s)^t \to \mathbb{R}$ be the multilinear form corresponding to a tensor $T \in (\mathbb{R}^s)^t$.
- Observe that f depends on ts variables $x_{(j,k)}$, where $1 \leqslant j \leqslant t$ and $1 \leqslant k \leqslant s$, and has degree t.
- The influence of variable (j,k) on f is

$$\mathrm{Inf}_{(j,k)}(f) = \sum_{i_1,\ldots,i_{j-1},i_{j+1},\ldots,i_t} T^2_{i_1,\ldots,i_{j-1},k,i_{j+1},\ldots,i_t}.$$

Open problem 3

Assume that $\|T\|_\infty^{\mathrm{inj}} \leqslant 1$. Show that, for all $1 \leqslant j \leqslant t$,

$$\sum_{k=1}^{s} \mathrm{Inf}_{(j,k)}(f)^{1/2} \leqslant \mathrm{poly}(t).$$

This would imply Conjecture B of Aaronson and Ambainis for the special case where f is a multilinear form.

Open problem 3 implies a special case of Conjecture B

- First observe that $\|T\|_{\infty}^{\text{inj}} \leqslant 1$ is equivalent to $|f(x)| \leqslant 1$ for $x \in \{\pm 1\}^{st}$.

Open problem 3 implies a special case of Conjecture B

- First observe that $\|T\|_\infty^{\text{inj}} \leqslant 1$ is equivalent to $|f(x)| \leqslant 1$ for $x \in \{\pm 1\}^{st}$.

- Now we have

$$\mathrm{Var}(f) \leqslant \sum_{j,k} \mathrm{Inf}_{(j,k)}(f)$$

Open problem 3 implies a special case of Conjecture B

- First observe that $\|T\|_\infty^{\text{inj}} \leqslant 1$ is equivalent to $|f(x)| \leqslant 1$ for $x \in \{\pm 1\}^{st}$.

- Now we have

$$\mathrm{Var}(f) \quad \leqslant \quad \sum_{j,k} \mathrm{Inf}_{(j,k)}(f) \leqslant \max_{j,k} \mathrm{Inf}_{(j,k)}(f)^{1/2} \sum_{j,k} \mathrm{Inf}_{(j,k)}(f)^{1/2}$$

Open problem 3 implies a special case of Conjecture B

- First observe that $\|T\|_\infty^{\text{inj}} \leqslant 1$ is equivalent to $|f(x)| \leqslant 1$ for $x \in \{\pm 1\}^{st}$.

- Now we have

$$\begin{aligned}\mathrm{Var}(f) &\leqslant \sum_{j,k} \mathrm{Inf}_{(j,k)}(f) \leqslant \max_{j,k} \mathrm{Inf}_{(j,k)}(f)^{1/2} \sum_{j,k} \mathrm{Inf}_{(j,k)}(f)^{1/2} \\ &\leqslant \mathrm{poly}(t) \max_{j,k} \mathrm{Inf}_{(j,k)}(f)^{1/2},\end{aligned}$$

so

$$\max_{j,k} \mathrm{Inf}_{(j,k)}(f) \geqslant \mathrm{poly}(\mathrm{Var}(f)/t).$$

Partial results

Theorem [Bohnenblust and Hille '31]

Assume that $\|T\|_\infty^{\text{inj}} \leqslant 1$. Then there is a universal constant $C > 1$ such that, for all $1 \leqslant j \leqslant t$,

$$\sum_{k=1}^{s} \text{Inf}_{(j,k)}(f)^{1/2} \leqslant C^t.$$

Partial results

Theorem [Bohnenblust and Hille '31]

Assume that $\|T\|_\infty^{\text{inj}} \leqslant 1$. Then there is a universal constant $C > 1$ such that, for all $1 \leqslant j \leqslant t$,

$$\sum_{k=1}^{s} \mathrm{Inf}_{(j,k)}(f)^{1/2} \leqslant C^t.$$

- This is a generalisation of Littlewood's 4/3 inequality [Littlewood '30].
- The constant C has gradually been improved over the years...

Partial results

Theorem [AM '11, folklore?]

Let $f : \mathbb{R}^n \to \mathbb{R}$ be a symmetric degree d multivariate polynomial such that $|f(x)| \leqslant 1$ for all $x \in \{\pm 1\}^n$ and $\mathrm{Var}(f) \geqslant \epsilon$. Then, for all $j \in \{1, \ldots, n\}$,

$$\mathrm{Inf}_j(f) \geqslant \mathrm{poly}(\epsilon/d).$$

Partial results

Theorem [AM '11, folklore?]

Let $f : \mathbb{R}^n \to \mathbb{R}$ be a symmetric degree d multivariate polynomial such that $|f(x)| \leqslant 1$ for all $x \in \{\pm 1\}^n$ and $\mathrm{Var}(f) \geqslant \epsilon$. Then, for all $j \in \{1, \ldots, n\}$,

$$\mathrm{Inf}_j(f) \geqslant \mathrm{poly}(\epsilon/d).$$

- A symmetric polynomial $f(x)$ depends only on the Hamming weight of $x \in \{\pm 1\}^n$, i.e. the number of 1s in x.
- For such polynomials, all influences are equal.

Conclusions

- Injective tensor norms are a powerful general framework in which to attack many open problems in quantum information theory.
- Many of these problems are accessible and can be stated purely mathematically, with no reference to quantum information.
- This doesn’t stop them from probably being very hard!

Thanks!

Further reading:

- "Classification of Entanglement in Symmetric States" [Aulbach '11] – an entire PhD thesis on the geometric measure of entanglement (!)
- "An efficient test for product states, with applications to quantum Merlin-Arthur games" [Harrow and AM '10] (arXiv:1001.0017) – stay tuned for a new version giving many other interpretations of $h_{\mathrm{SEP}}(M)$
- "Weak multiplicativity for random quantum channels" [AM '11] (arXiv:1112.5271) – includes references to many other papers on multiplicativity questions
- "The role of structure in quantum speed-ups" [Aaronson and Ambainis '09].

Conjecture B implies Conjecture A (sketch)

Consider the following algorithm:

1. If $\mathrm{Var}(f) \leqslant (\delta\epsilon)^2$, stop and return $\mathbb{E}_x[f(x)]$.
2. Query the variable j such that $\mathrm{Inf}_j(f)$ is maximal and set f to be the resulting function.
3. Go to step 1.

Theorem [Aaronson and Ambainis '09]

Assuming Conjecture B, this algorithm terminates in expected time $\mathrm{poly}(d, 1/\epsilon, 1/\delta)$, where the expectation is taken over x, and computes $f(x)$ to within ϵ on at least a $1-\delta$ fraction of inputs x.

Conjecture B implies Conjecture A (sketch)

- Let $\tilde{f}$ be the function computed by the algorithm (observe that it always terminates).
- We have

$$\Pr_x[|f(x) - \tilde{f}(x)| \geqslant \epsilon] \leqslant \frac{\mathbb{E}_x[|f(x) - \tilde{f}(x)|]}{\epsilon} \leqslant \frac{\mathrm{Var}(f)^{1/2}}{\epsilon} \leqslant \delta.$$

- The algorithm terminates when $\mathrm{Var}(f) \leqslant (\delta\epsilon)^2$, and at the beginning of the algorithm $\mathrm{Var}(f) \leqslant \sum_j \mathrm{Inf}_j(f) \leqslant d$.
- The expected decrease in the total influence with each query is $\max_j \mathrm{Inf}_j(f)$.
- Assuming Conjecture B, this is lower bounded by $\mathrm{poly}(\mathrm{Var}(f)/d) \geqslant \mathrm{poly}(\delta\epsilon/d)$.
- Thus the expected number of queries until the algorithm terminates is at most $\mathrm{poly}(d, 1/\epsilon, 1/\delta)$.