Optimising quantum data hiding

Joint work with Ludovico Lami

NEST

SCUOLA NORMALE SUPERIORE

Mele and Lami, *Optimising quantum data hiding,* arXiv:2510.03538

Quantum data hiding

Definition (informal)

ρ_{AB} and σ_{AB} form a pair of **quantum data hiding** states if:

- They are perfectly distinguishable via global operations;
- They are nearly indistinguishable via LOCC.

Terhal, DiVincenzo, Leung, *PRL* (2001)
DiVincenzo, Leung, Terhal, *IEEE ToIT* (2002)

Quantum data hiding

Definition (informal)

ρ_{AB} and σ_{AB} form a pair of **quantum data hiding** states if:

- They are perfectly distinguishable via global operations;
- They are nearly indistinguishable via LOCC.

Terhal, DiVincenzo, Leung, *PRL* (2001)
DiVincenzo, Leung, Terhal, *IEEE ToIT* (2002)

ρ_{AB} **or** σ_{AB}

Distinguishable globally

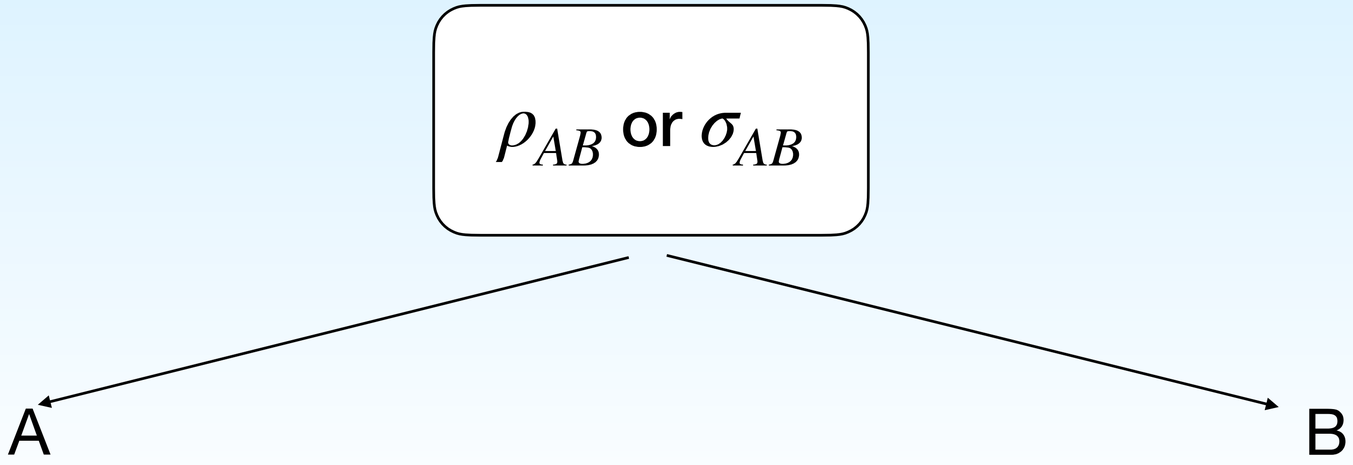
Quantum data hiding

Definition (informal)

ρ_{AB} and σ_{AB} form a pair of **quantum data hiding** states if:

- They are perfectly distinguishable via global operations;
- They are nearly indistinguishable via LOCC.

Terhal, DiVincenzo, Leung, *PRL* (2001)
DiVincenzo, Leung, Terhal, *IEEE ToIT* (2002)



Distinguishable globally

Quantum data hiding

Definition (informal)

ρ_{AB} and σ_{AB} form a pair of **quantum data hiding** states if:

- They are perfectly distinguishable via global operations;
- They are nearly indistinguishable via LOCC.

Terhal, DiVincenzo, Leung, *PRL* (2001)
DiVincenzo, Leung, Terhal, *IEEE ToIT* (2002)

ρ_{AB} **or** σ_{AB}

A ..... B Indistinguishable via LOCC

Quantum data hiding

Definition (informal)

ρ_{AB} and σ_{AB} form a pair of **quantum data hiding** states if:

- They are perfectly distinguishable via global operations;
- They are nearly indistinguishable via LOCC.

Terhal, DiVincenzo, Leung, *PRL* (2001)
DiVincenzo, Leung, Terhal, *IEEE ToIT* (2002)

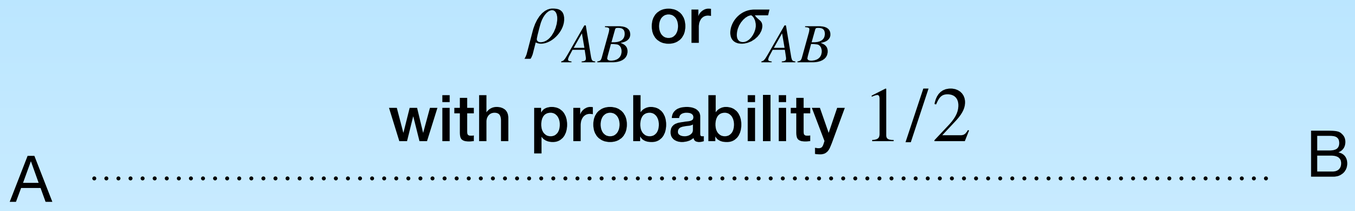
Motivations:

- Cryptography
- Bound entanglement

Horodecki$^{\otimes 3}$, Oppenheim, *PRL* (2005)
Christandl and Ferrara, *PRL* (2017)

LOCC norm

Matthews, Wehner, and Winter; *CMP* (2009)

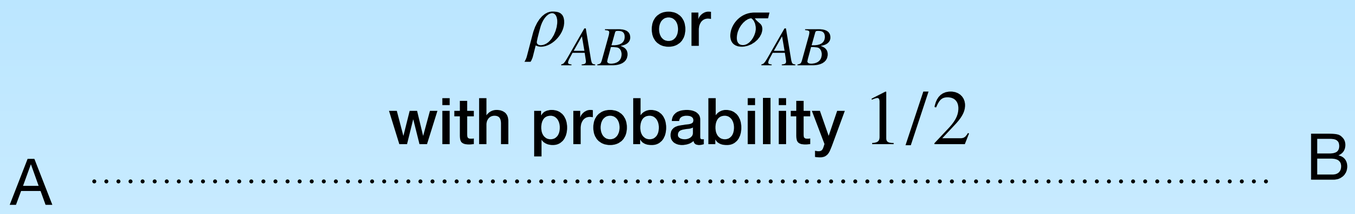


- What is the best probability of successfully discriminating via **global operations**?

$$P_{\text{succ}}(\rho_{AB}, \sigma_{AB}) = \frac{1}{2}\left(1 + \frac{1}{2}\|\rho_{AB} - \sigma_{AB}\|_1\right)$$

LOCC norm

Matthews, Wehner, and Winter; *CMP* (2009)



- What is the best probability of successfully discriminating via **global operations**?

$$P_{\text{succ}}(\rho_{AB}, \sigma_{AB}) = \frac{1}{2}\left(1 + \frac{1}{2}\|\rho_{AB} - \sigma_{AB}\|_1\right)$$

- What is the best probability of successfully discriminating via **LOCC**?

$$P_{\text{succ}}^{(\text{LOCC})}(\rho_{AB}, \sigma_{AB}) = \frac{1}{2}\left(1 + \frac{1}{2}\|\rho_{AB} - \sigma_{AB}\|_{\text{LOCC}}\right)$$

(This can be regarded as the definition of LOCC norm)

Definition

ρ_{AB} and σ_{AB} form a pair of ε-**quantum data hiding** states if:

- $\frac{1}{2}\|\rho_{AB} - \sigma_{AB}\|_{\mathrm{LOCC}} \leq \varepsilon$ (i.e., nearly indistinguishable under LOCC)
- $\frac{1}{2}\|\rho_{AB} - \sigma_{AB}\|_{1} = 1$ (i.e., perfectly distinguishable globally)

Definition

ρ_{AB} and σ_{AB} form a pair of ε-**quantum data hiding** states if:

- $\frac{1}{2}\|\rho_{AB} - \sigma_{AB}\|_{\mathrm{LOCC}} \leq \varepsilon$ (i.e., nearly indistinguishable under LOCC)
- $\frac{1}{2}\|\rho_{AB} - \sigma_{AB}\|_{1} = 1$ (i.e., perfectly distinguishable globally)

Theorem Terhal, DiVincenzo, Leung, *PRL* (2001); DiVincenzo, Leung, Terhal, *IoIT* (2002); Aubrun and Lancien; *QIC* (2015)

There exist ε-**quantum data hiding** states for all $\varepsilon \in (0,1)$

Definition

ρ_{AB} and σ_{AB} form a pair of ε-**quantum data hiding** states if:

- $\frac{1}{2}\|\rho_{AB} - \sigma_{AB}\|_{\mathrm{LOCC}} \leq \varepsilon$ (i.e., nearly indistinguishable under LOCC)
- $\frac{1}{2}\|\rho_{AB} - \sigma_{AB}\|_{1} = 1$ (i.e., perfectly distinguishable globally)

Theorem Terhal, DiVincenzo, Leung, *PRL* (2001)
DiVincenzo, Leung, Terhal, *IoIT* (2002)
Aubrun and Lancien; *QIC* (2015)

There exist ε-**quantum data hiding** states for all $\varepsilon \in (0,1)$

However, for ε sufficiently small, all the known constructions are **entangled** (Werner states, random states)

Definition

ρ_{AB} and σ_{AB} form a pair of ε-**quantum data hiding** states if:

- $\frac{1}{2}\|\rho_{AB} - \sigma_{AB}\|_{\mathrm{LOCC}} \leq \varepsilon$ (i.e., nearly indistinguishable under LOCC)
- $\frac{1}{2}\|\rho_{AB} - \sigma_{AB}\|_{1} = 1$ (i.e., perfectly distinguishable globally)

Theorem Terhal, DiVincenzo, Leung, *PRL* (2001); DiVincenzo, Leung, Terhal, *IoIT* (2002); Aubrun and Lancien; *QIC* (2015)

There exist ε-**quantum data hiding** states for all $\varepsilon \in (0,1)$

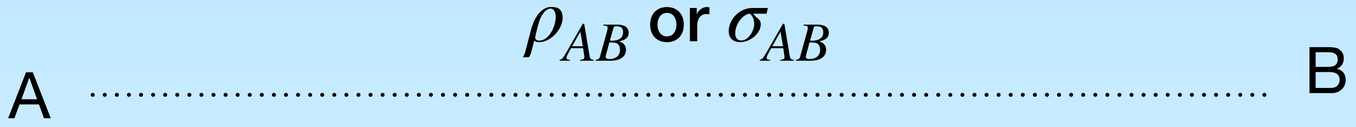
However, for ε sufficiently small, all the known constructions are **entangled** (Werner states, random states)

[Eggeling and Werner; PRL (2002)] exhibit **separable** states ρ_{AB} and σ_{AB} such that:

$\frac{1}{2}\|\rho_{AB} - \sigma_{AB}\|_{\mathrm{LOCC}} \leq \varepsilon$ but $\frac{1}{2}\|\rho_{AB} - \sigma_{AB}\|_{1} \neq 1$ (i.e., they are not *perfectly* orthogonal)

Does there exist a pair of **separable** ε-quantum data hiding states?

(i.e. a pair of states that are separable, orthogonal, and ε-close in LOCC-norm)



Does there exist a pair of **separable** ε-quantum data hiding states?

(i.e. a pair of states that are separable, orthogonal, and ε-close in LOCC-norm)

A ρ_{AB} **or** σ_{AB} B

Equivalently, can ε-quantum data hiding states be produced via LOCC?

Does there exist a pair of **separable** ε-quantum data hiding states?

(i.e. a pair of states that are separable, orthogonal, and ε-close in LOCC-norm)

A ρ_{AB} **or** σ_{AB} B

Equivalently, can ε-quantum data hiding states be produced via LOCC?

Yes! (Our main result)

Does there exist a pair of **separable** ε-quantum data hiding states?

(i.e. a pair of states that are separable, orthogonal, and ε-close in LOCC-norm)

A ρ_{AB} **or** σ_{AB} B

Equivalently, can ε-quantum data hiding states be produced via LOCC?

Yes! (Our main result)

See also the independent work [Ha and Kim, *PRA*, (2025)]

Does there exist a pair of **separable** ε-quantum data hiding states?

(i.e. a pair of states that are separable, orthogonal, and ε-close in LOCC-norm)

A ..... ρ_{AB} **or** σ_{AB} ..... B

Equivalently, can ε-quantum data hiding states be produced via LOCC?

Yes! (Our main result)

See also the independent work [Ha and Kim, *PRA*, (2025)]

A secret can be hidden using no entanglement,
while remaining nearly unrecoverable unless entanglement is available.

Does there exist a pair of **separable** ε-quantum data hiding states?

(i.e. a pair of states that are separable, orthogonal, and ε-close in LOCC-norm)

A ..... ρ_{AB} **or** σ_{AB} ..... B

Equivalently, can ε-quantum data hiding states be produced via LOCC?

Yes! (Our main result)

See also the independent work [Ha and Kim, *PRA*, (2025)]

A secret can be hidden using no entanglement,
while remaining nearly unrecoverable unless entanglement is available.

→ Irreversibility of hiding secrets into quantum states via LOCC

Theorem 1 (Existence of separable ε-quantum data hiding states)

For all $\varepsilon \in (0,1)$ there exist **separable** states ρ_{AB} and σ_{AB} on $\mathbb{C}^D \otimes \mathbb{C}^D$ such that:

Theorem 1 (Existence of separable ε-quantum data hiding states)

For all $\varepsilon \in (0,1)$ there exist **separable** states ρ_{AB} and σ_{AB} on $\mathbb{C}^D \otimes \mathbb{C}^D$ such that:

- $\frac{1}{2}\|\rho_{AB} - \sigma_{AB}\|_{\mathrm{LOCC}} \leq \varepsilon$ (i.e., ε-indistinguishable via LOCC)
- $\frac{1}{2}\|\rho_{AB} - \sigma_{AB}\|_1 = 1$ (i.e., perfectly distinguishable globally)

Theorem 1 (Existence of separable ε-quantum data hiding states)

For all $\varepsilon \in (0,1)$ there exist **separable** states ρ_{AB} and σ_{AB} on $\mathbb{C}^D \otimes \mathbb{C}^D$ such that:

- $\frac{1}{2}\|\rho_{AB} - \sigma_{AB}\|_{\mathrm{LOCC}} \leq \varepsilon$ (i.e., ε-indistinguishable via LOCC)
- $\frac{1}{2}\|\rho_{AB} - \sigma_{AB}\|_1 = 1$ (i.e., perfectly distinguishable globally)

- Our construction has local dimension $D = O\left(1/\varepsilon^{10}\right)$.

Theorem 1 (Existence of separable ε-quantum data hiding states)

For all $\varepsilon \in (0,1)$ there exist **separable** states ρ_{AB} and σ_{AB} on $\mathbb{C}^D \otimes \mathbb{C}^D$ such that:

- $\frac{1}{2}\|\rho_{AB} - \sigma_{AB}\|_{\mathrm{LOCC}} \leq \varepsilon$ (i.e., ε-indistinguishable via LOCC)
- $\frac{1}{2}\|\rho_{AB} - \sigma_{AB}\|_1 = 1$ (i.e., perfectly distinguishable globally)

- Our construction has local dimension $D = O\left(1/\varepsilon^{10}\right)$.

$D \xrightarrow{\varepsilon \to 0} \infty$, but this is unavoidable

Theorem 1 (Existence of separable ε-quantum data hiding states)

For all $\varepsilon \in (0,1)$ there exist **separable** states ρ_{AB} and σ_{AB} on $\mathbb{C}^D \otimes \mathbb{C}^D$ such that:

- $\frac{1}{2}\|\rho_{AB} - \sigma_{AB}\|_{\mathrm{LOCC}} \leq \varepsilon$ (i.e., ε-indistinguishable via LOCC)
- $\frac{1}{2}\|\rho_{AB} - \sigma_{AB}\|_1 = 1$ (i.e., perfectly distinguishable globally)

- Our construction has local dimension $D = O\left(1/\varepsilon^{10}\right)$.

$$\mathrm{D} \xrightarrow{\varepsilon \to 0} \infty, \text{ but this is unavoidable}$$

- All ε-quantum data hiding states on $\mathbb{C}^D \otimes \mathbb{C}^D$ must satisfy $D = \Omega(1/\varepsilon)$.

Matthews, Wehner, and Winter; *CMP* (2009)
Lami, Palazuelos, and Winter; *CMP* (2018)

How to boost the indistinguishability between two states σ_0 and σ_1?

How to boost the indistinguishability between two states σ_0 and σ_1?

Parity trick

Terhal, DiVincenzo, Leung, *PRL* (2001)
DiVincenzo, Leung, Terhal, *IEEE ToIT* (2002)

How to boost the indistinguishability between two states σ_0 and σ_1?

Parity trick

Terhal, DiVincenzo, Leung, *PRL* (2001)
DiVincenzo, Leung, Terhal, *IEEE ToIT* (2002)

- **Even state:** $\rho_0^{(k)} := \frac{1}{2^{k-1}} \sum_{\substack{x_1,\ldots,x_k \in \{0,1\} \\ x_1+\cdots+x_k \equiv 0 \pmod 2}} \sigma_{x_1} \otimes \cdots \otimes \sigma_{x_k}$

  The number of states σ_1 is even

How to boost the indistinguishability between two states σ_0 and σ_1?

Parity trick

Terhal, DiVincenzo, Leung, *PRL* (2001)
DiVincenzo, Leung, Terhal, *IEEE ToIT* (2002)

- **Even state:** $\rho_0^{(k)} := \frac{1}{2^{k-1}} \sum_{\substack{x_1,\ldots,x_k \in \{0,1\} \\ x_1+\cdots+x_k \equiv 0 \pmod 2}} \sigma_{x_1} \otimes \cdots \otimes \sigma_{x_k}$

The number of states σ_1 is even

Example for $k = 2$: $\rho_0^{(2)} = \frac{\sigma_0 \otimes \sigma_0 + \sigma_1 \otimes \sigma_1}{2}$

How to boost the indistinguishability between two states σ_0 and σ_1?

Parity trick

Terhal, DiVincenzo, Leung, *PRL* (2001)
DiVincenzo, Leung, Terhal, *IEEE ToIT* (2002)

- **Even state:** $\rho_0^{(k)} := \frac{1}{2^{k-1}} \sum_{\substack{x_1,\ldots,x_k \in \{0,1\} \\ x_1+\cdots+x_k \equiv 0 \pmod 2}} \sigma_{x_1} \otimes \cdots \otimes \sigma_{x_k}$

  The number of states σ_1 is even

  Example for $k = 2$: $\rho_0^{(2)} = \frac{\sigma_0 \otimes \sigma_0 + \sigma_1 \otimes \sigma_1}{2}$

- **Odd state:** $\rho_1^{(k)} := \frac{1}{2^{k-1}} \sum_{\substack{x_1,\ldots,x_k \in \{0,1\} \\ x_1+\cdots+x_k \equiv 1 \pmod 2}} \sigma_{x_1} \otimes \cdots \otimes \sigma_{x_k}$

  The number of states σ_1 is odd

How to boost the indistinguishability between two states σ_0 and σ_1?

Parity trick

Terhal, DiVincenzo, Leung, *PRL* (2001)
DiVincenzo, Leung, Terhal, *IEEE ToIT* (2002)

- **Even state:** $\rho_0^{(k)} := \frac{1}{2^{k-1}} \sum_{\substack{x_1,\ldots,x_k \in \{0,1\} \\ x_1+\cdots+x_k \equiv 0 \pmod 2}} \sigma_{x_1} \otimes \cdots \otimes \sigma_{x_k}$

  The number of states σ_1 is even

  Example for $k=2$: $\rho_0^{(2)} = \frac{\sigma_0 \otimes \sigma_0 + \sigma_1 \otimes \sigma_1}{2}$

- **Odd state:** $\rho_1^{(k)} := \frac{1}{2^{k-1}} \sum_{\substack{x_1,\ldots,x_k \in \{0,1\} \\ x_1+\cdots+x_k \equiv 1 \pmod 2}} \sigma_{x_1} \otimes \cdots \otimes \sigma_{x_k}$

  The number of states σ_1 is odd

  Example for $k=2$: $\rho_1^{(2)} = \frac{\sigma_0 \otimes \sigma_1 + \sigma_1 \otimes \sigma_0}{2}$

How to boost the indistinguishability between two states σ_0 and σ_1?

Parity trick

Terhal, DiVincenzo, Leung, *PRL* (2001)
DiVincenzo, Leung, Terhal, *IEEE ToIT* (2002)

- **Even state:** $\rho_0^{(k)} := \frac{1}{2^{k-1}} \sum_{\substack{x_1,\ldots,x_k \in \{0,1\} \\ x_1+\cdots+x_k \equiv 0 \pmod 2}} \sigma_{x_1} \otimes \cdots \otimes \sigma_{x_k}$ The number of states σ_1 is even

- **Odd state:** $\rho_1^{(k)} := \frac{1}{2^{k-1}} \sum_{\substack{x_1,\ldots,x_k \in \{0,1\} \\ x_1+\cdots+x_k \equiv 1 \pmod 2}} \sigma_{x_1} \otimes \cdots \otimes \sigma_{x_k}$ The number of states σ_1 is odd

$$\frac{\rho_1^{(k)} - \rho_0^{(k)}}{2} = \left(\frac{\sigma_1 - \sigma_0}{2} \right)^{\otimes k}$$

How to boost the indistinguishability between two states σ_0 and σ_1?

Parity trick

Terhal, DiVincenzo, Leung, *PRL* (2001)
DiVincenzo, Leung, Terhal, *IEEE ToIT* (2002)

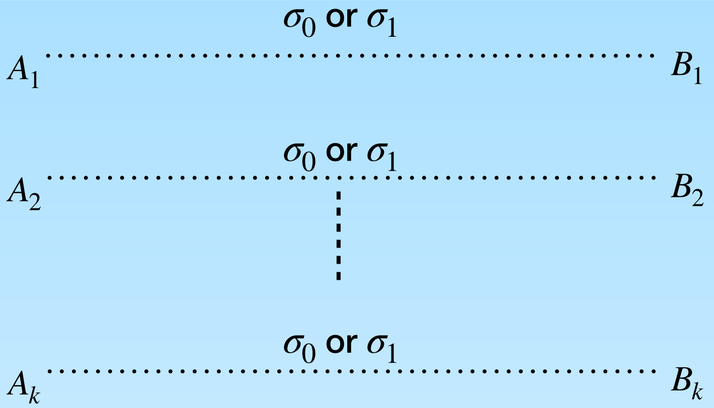
- **Even state:** $\rho_0^{(k)} := \frac{1}{2^{k-1}} \sum_{\substack{x_1,\ldots,x_k \in \{0,1\} \\ x_1+\cdots+x_k \equiv 0 \pmod 2}} \sigma_{x_1} \otimes \cdots \otimes \sigma_{x_k}$ The number of states σ_1 is even

- **Odd state:** $\rho_1^{(k)} := \frac{1}{2^{k-1}} \sum_{\substack{x_1,\ldots,x_k \in \{0,1\} \\ x_1+\cdots+x_k \equiv 1 \pmod 2}} \sigma_{x_1} \otimes \cdots \otimes \sigma_{x_k}$ The number of states σ_1 is odd

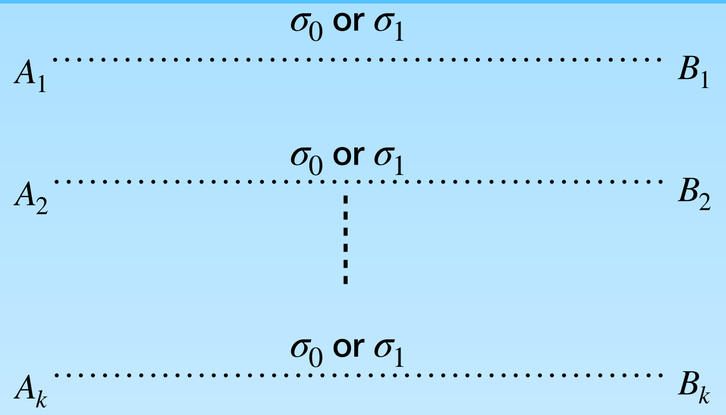
$$\frac{\rho_1^{(k)} - \rho_0^{(k)}}{2} = \left(\frac{\sigma_1 - \sigma_0}{2}\right)^{\otimes k}$$

$$\frac{1}{2}\|\rho_1^{(k)} - \rho_0^{(k)}\|_1 = \left(\frac{1}{2}\|\sigma_1 - \sigma_0\|_1\right)^k \xrightarrow{k\to\infty} \begin{cases} 0 & \text{if } \frac{1}{2}\|\sigma_1 - \sigma_0\|_1 < 1 \\ 1 & \text{otherwise} \end{cases}$$

$$\frac{\rho_1^{(k)} - \rho_0^{(k)}}{2} = \left(\frac{\sigma_1 - \sigma_0}{2}\right)^{\otimes k} \longrightarrow \frac{1}{2}\|\rho_1^{(k)} - \rho_0^{(k)}\|_{\mathrm{LOCC}} = \frac{1}{2^k}\|(\sigma_1 - \sigma_0)^{\otimes k}\|_{\mathrm{LOCC}}$$



$$\frac{\rho_1^{(k)} - \rho_0^{(k)}}{2} = \left(\frac{\sigma_1 - \sigma_0}{2}\right)^{\otimes k} \longrightarrow \frac{1}{2}\|\rho_1^{(k)} - \rho_0^{(k)}\|_{\mathrm{LOCC}} = \frac{1}{2^k}\|(\sigma_1 - \sigma_0)^{\otimes k}\|_{\mathrm{LOCC}}$$

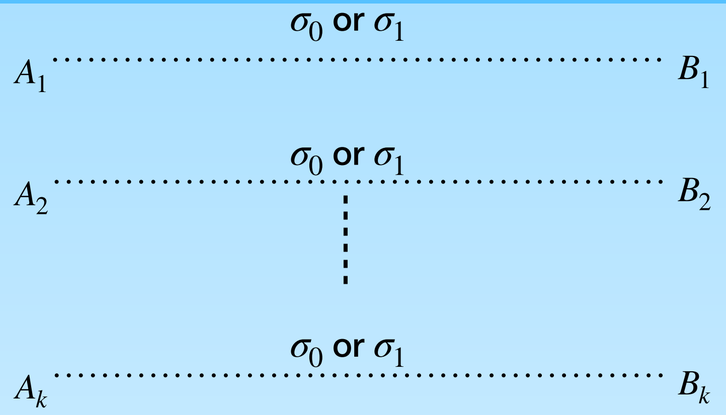


Open problem (Sub-multiplicativity of LOCC-norm)

$$\|(\rho_1 - \sigma_1) \otimes (\rho_2 - \sigma_2)\|_{\mathrm{LOCC}} \overset{?}{\leq} \|\rho_1 - \sigma_1\|_{\mathrm{LOCC}} \|\rho_2 - \sigma_2\|_{\mathrm{LOCC}}$$

$$\|X_{A_1B_1} \otimes Y_{A_2B_2}\|_{\mathrm{LOCC(A_1A_2:B_1B_2)}} \overset{?}{\leq} \|X\|_{\mathrm{LOCC(A_1:B_1)}} \|Y\|_{\mathrm{LOCC(A_2:B_2)}}$$

$$\frac{\rho_1^{(k)} - \rho_0^{(k)}}{2} = \left(\frac{\sigma_1 - \sigma_0}{2}\right)^{\otimes k} \longrightarrow \frac{1}{2}\|\rho_1^{(k)} - \rho_0^{(k)}\|_{\mathrm{LOCC}} = \frac{1}{2^k}\|(\sigma_1 - \sigma_0)^{\otimes k}\|_{\mathrm{LOCC}}$$



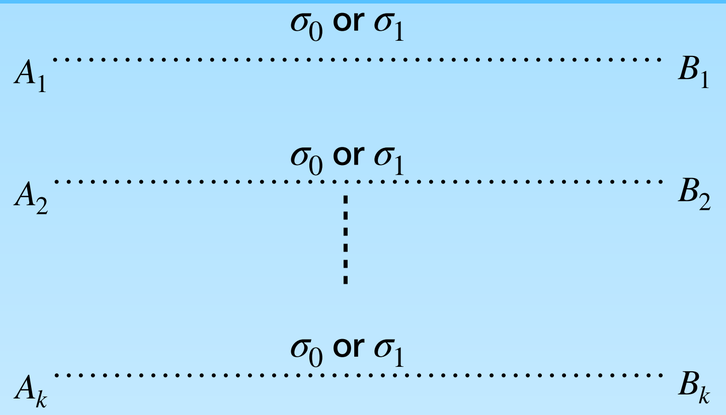
Open problem (Sub-multiplicativity of LOCC-norm)

$$\|(\rho_1 - \sigma_1) \otimes (\rho_2 - \sigma_2)\|_{\mathrm{LOCC}} \overset{?}{\leq} \|\rho_1 - \sigma_1\|_{\mathrm{LOCC}} \|\rho_2 - \sigma_2\|_{\mathrm{LOCC}}$$

$$\|X_{A_1B_1} \otimes Y_{A_2B_2}\|_{\mathrm{LOCC(A_1A_2:B_1B_2)}} \overset{?}{\leq} \|X\|_{\mathrm{LOCC(A_1:B_1)}} \|Y\|_{\mathrm{LOCC(A_2:B_2)}}$$

$$\longrightarrow \frac{1}{2}\|\rho_1^{(k)} - \rho_0^{(k)}\|_{\mathrm{LOCC}} \overset{?}{\leq} \left(\frac{1}{2}\|\sigma_1 - \sigma_0\|_{\mathrm{LOCC}}\right)^k \overset{k\to\infty}{\longrightarrow} 0 \quad \text{if} \quad \frac{1}{2}\|\sigma_1 - \sigma_0\|_{\mathrm{LOCC}} < 1$$

$$\frac{\rho_1^{(k)} - \rho_0^{(k)}}{2} = \left(\frac{\sigma_1 - \sigma_0}{2}\right)^{\otimes k} \longrightarrow \frac{1}{2}\|\rho_1^{(k)} - \rho_0^{(k)}\|_{\mathrm{LOCC}} = \frac{1}{2^k}\|(\sigma_1 - \sigma_0)^{\otimes k}\|_{\mathrm{LOCC}}$$



Open problem (Sub-multiplicativity of LOCC-norm)

$$\|(\rho_1 - \sigma_1) \otimes (\rho_2 - \sigma_2)\|_{\mathrm{LOCC}} \overset{?}{\leq} \|\rho_1 - \sigma_1\|_{\mathrm{LOCC}} \|\rho_2 - \sigma_2\|_{\mathrm{LOCC}}$$

$$\|X_{A_1B_1} \otimes Y_{A_2B_2}\|_{\mathrm{LOCC(A_1A_2:B_1B_2)}} \overset{?}{\leq} \|X\|_{\mathrm{LOCC(A_1:B_1)}} \|Y\|_{\mathrm{LOCC(A_2:B_2)}}$$

$$\longrightarrow \frac{1}{2}\|\rho_1^{(k)} - \rho_0^{(k)}\|_{\mathrm{LOCC}} \overset{?}{\leq} \left(\frac{1}{2}\|\sigma_1 - \sigma_0\|_{\mathrm{LOCC}}\right)^k \overset{k\to\infty}{\longrightarrow} 0 \quad \text{if } \frac{1}{2}\|\sigma_1 - \sigma_0\|_{\mathrm{LOCC}} < 1$$

Proof idea of Theorem 1 (Existence of separable ε-quantum data hiding states):

Pick σ_0, σ_1 separable-orthogonal states satisfying $\frac{1}{2}\|\sigma_1 - \sigma_0\|_{\mathrm{LOCC}} < 1$. Then, use *parity trick*.

How to upper bound the LOCC norm? → **PPT norm** [Matthews, Wehner, and Winter; *CMP* (2009)]

How to upper bound the LOCC norm? ⟶ **PPT norm** [Matthews, Wehner, and Winter; *CMP* (2009)]

- $\|\cdot\|_{\mathrm{LOCC}} \leq \|\cdot\|_{\mathrm{PPT}}$

How to upper bound the LOCC norm? ⟶ **PPT norm** [Matthews, Wehner, and Winter; *CMP* (2009)]

- $\|\cdot\|_{\mathrm{LOCC}} \leq \|\cdot\|_{\mathrm{PPT}}$
- $\frac{1}{2}\|\rho_0 - \rho_1\|_{\mathrm{PPT}} = \max_{\substack{0 \leq E \leq \mathbb{I} \\ 0 \leq E^{t_B} \leq \mathbb{I}}} \mathrm{Tr}[E(\rho_0 - \rho_1)]$ = semidefinite program

How to upper bound the LOCC norm? ⟶ **PPT norm** [Matthews, Wehner, and Winter; *CMP* (2009)]

- $\|\cdot\|_{\mathrm{LOCC}} \leq \|\cdot\|_{\mathrm{PPT}}$
- $\frac{1}{2}\|\rho_0 - \rho_1\|_{\mathrm{PPT}} = \max_{\substack{0 \leq E \leq \mathbb{I} \\ 0 \leq E^{t_B} \leq \mathbb{I}}} \mathrm{Tr}[E(\rho_0 - \rho_1)]$ = semidefinite program
- If ρ_0 and ρ_1 satisfy a *symmetry*, then $\frac{1}{2}\|\rho_0 - \rho_1\|_{\mathrm{PPT}}$ = linear program (Simple to analyse!)

How to upper bound the LOCC norm? ⟶ **PPT norm** [Matthews, Wehner, and Winter; *CMP* (2009)]

- $\|\cdot\|_{\mathrm{LOCC}} \leq \|\cdot\|_{\mathrm{PPT}}$
- $\frac{1}{2}\|\rho_0 - \rho_1\|_{\mathrm{PPT}} = \max_{\substack{0 \leq E \leq \mathbb{I} \\ 0 \leq E^{t_B} \leq \mathbb{I}}} \mathrm{Tr}[E(\rho_0 - \rho_1)]$ = semidefinite program
- If ρ_0 and ρ_1 satisfy a *symmetry*, then $\frac{1}{2}\|\rho_0 - \rho_1\|_{\mathrm{PPT}}$ = linear program (Simple to analyse!)

Which symmetry to choose?

How to upper bound the LOCC norm? ⟶ **PPT norm** [Matthews, Wehner, and Winter; *CMP* (2009)]

- $\|\cdot\|_{\mathrm{LOCC}} \leq \|\cdot\|_{\mathrm{PPT}}$
- $\frac{1}{2}\|\rho_0 - \rho_1\|_{\mathrm{PPT}} = \max_{\substack{0 \leq E \leq \mathbb{I} \\ 0 \leq E^{t_B} \leq \mathbb{I}}} \mathrm{Tr}[E(\rho_0 - \rho_1)]$ = semidefinite program
- If ρ_0 and ρ_1 satisfy a *symmetry*, then $\frac{1}{2}\|\rho_0 - \rho_1\|_{\mathrm{PPT}}$ = linear program (Simple to analyse!)

Which symmetry to choose?

- 1st attempt: $(U \otimes U)\,\rho\,(U \otimes U)^\dagger = \rho \quad \forall U$ ⟶ No examples of separable orthogonal states

How to upper bound the LOCC norm? → **PPT norm** [Matthews, Wehner, and Winter; *CMP* (2009)]

- $\|\cdot\|_{\mathrm{LOCC}} \leq \|\cdot\|_{\mathrm{PPT}}$
- $\frac{1}{2}\|\rho_0 - \rho_1\|_{\mathrm{PPT}} = \max_{\substack{0 \leq E \leq \mathbb{I} \\ 0 \leq E^{t_B} \leq \mathbb{I}}} \mathrm{Tr}[E(\rho_0 - \rho_1)]$ = semidefinite program
- If ρ_0 and ρ_1 satisfy a *symmetry*, then $\frac{1}{2}\|\rho_0 - \rho_1\|_{\mathrm{PPT}}$ = linear program (Simple to analyse!)

Which symmetry to choose?

- 1st attempt: $(U \otimes U)\,\rho\,(U \otimes U)^\dagger = \rho \quad \forall U$ → No examples of separable orthogonal states
- 2nd attempt: $(U \otimes U^*)\,\rho\,(U \otimes U^*)^\dagger = \rho \quad \forall U$ → Still no examples

How to upper bound the LOCC norm? → **PPT norm** [Matthews, Wehner, and Winter; *CMP* (2009)]

- $\|\cdot\|_{\mathrm{LOCC}} \leq \|\cdot\|_{\mathrm{PPT}}$
- $\frac{1}{2}\|\rho_0 - \rho_1\|_{\mathrm{PPT}} = \max_{\substack{0 \leq E \leq \mathbb{I} \\ 0 \leq E^{t_B} \leq \mathbb{I}}} \mathrm{Tr}[E(\rho_0 - \rho_1)]$ = semidefinite program
- If ρ_0 and ρ_1 satisfy a *symmetry*, then $\frac{1}{2}\|\rho_0 - \rho_1\|_{\mathrm{PPT}}$ = linear program (Simple to analyse!)

Which symmetry to choose?

- 1st attempt: $(U \otimes U)\,\rho\,(U \otimes U)^\dagger = \rho \quad \forall U$ → No examples of separable orthogonal states
- 2nd attempt: $(U \otimes U^*)\,\rho\,(U \otimes U^*)^\dagger = \rho \quad \forall U$ → Still no examples
- 3rd attempt: $(U \otimes U)\,\rho\,(U \otimes U)^\dagger = \rho \quad \forall U \in$ *hyperoctahedral* group → It works!

Twirling w.r.t. hyperoctahedral group (permutations+signs)

$$\frac{1}{|G|}\sum_{U\in G}(U\otimes U)\,X\,(U\otimes U)^\dagger=\sum_{i=0}^{3}\mathrm{Tr}[X\Theta_i]\,\frac{\Theta_i}{\mathrm{Tr}[\Theta_i]}$$

$$G:=\left\{\sum_{j=0}^{d-1}(-1)^{x_j}|\pi(j)\rangle\langle j|:\ \ \pi\in S_d,\ x\in\{0,1\}^d\right\}$$

Twirling w.r.t. hyperoctahedral group (permutations+signs)

$$\frac{1}{|G|}\sum_{U\in G}(U\otimes U)X(U\otimes U)^\dagger = \sum_{i=0}^{3}\mathrm{Tr}[X\Theta_i]\frac{\Theta_i}{\mathrm{Tr}[\Theta_i]}$$

$$G := \left\{ \sum_{j=0}^{d-1}(-1)^{x_j}|\pi(j)\rangle\langle j| : \ \pi\in S_d,\ x\in\{0,1\}^d \right\}$$

$$\Theta_0 := \Phi,$$

(Max. ent. state)

$$\Phi := \frac{1}{d}\sum_{i,j=0}^{d-1}|i\rangle\langle j|\otimes|i\rangle\langle j|$$ (Max. ent. state)

Twirling w.r.t. hyperoctahedral group (permutations+signs)

$$\frac{1}{|G|}\sum_{U\in G}(U\otimes U)X(U\otimes U)^\dagger = \sum_{i=0}^{3}\mathrm{Tr}[X\Theta_i]\frac{\Theta_i}{\mathrm{Tr}[\Theta_i]}$$

$$G := \left\{ \sum_{j=0}^{d-1}(-1)^{x_j}|\pi(j)\rangle\langle j| : \ \pi\in S_d,\ x\in\{0,1\}^d \right\}$$

$$\Theta_0 := \Phi, \qquad \Theta_1 := P - \Phi,$$

(Max. ent. state)

$$\Phi := \frac{1}{d}\sum_{i,j=0}^{d-1}|i\rangle\langle j|\otimes|i\rangle\langle j|$$ (Max. ent. state)

$$P := \sum_{i=0}^{d-1}|i\rangle\langle i|\otimes|i\rangle\langle i|$$ (Projector on max. correlated subspace)

Twirling w.r.t. hyperoctahedral group (permutations+signs)

$$\frac{1}{|G|}\sum_{U\in G}(U\otimes U)X(U\otimes U)^\dagger=\sum_{i=0}^{3}\mathrm{Tr}[X\Theta_i]\frac{\Theta_i}{\mathrm{Tr}[\Theta_i]}$$

$$G:=\left\{\sum_{j=0}^{d-1}(-1)^{x_j}|\pi(j)\rangle\langle j|:\ \pi\in S_d,\ x\in\{0,1\}^d\right\}$$

$$\Theta_0:=\Phi,\qquad \Theta_1:=P-\Phi,\qquad \Theta_2:=\frac{\mathbb{I}+F-2P}{2},\qquad \Theta_3:=\frac{\mathbb{I}-F}{2},$$

(Max. ent. state)

(Projector on the antisymmetric subspace)

$\Phi:=\frac{1}{d}\sum_{i,j=0}^{d-1}|i\rangle\langle j|\otimes|i\rangle\langle j|$ (Max. ent. state)

$P:=\sum_{i=0}^{d-1}|i\rangle\langle i|\otimes|i\rangle\langle i|$ (Projector on max. correlated subspace)

$F:=\sum_{i,j=0}^{d-1}|i\rangle\langle j|\otimes|j\rangle\langle i|$ (Flip operator)

Twirling w.r.t. hyperoctahedral group (permutations+signs)

$$\frac{1}{|G|}\sum_{U\in G}(U\otimes U)X(U\otimes U)^\dagger = \sum_{i=0}^{3}\mathrm{Tr}[X\Theta_i]\frac{\Theta_i}{\mathrm{Tr}[\Theta_i]}$$

$$G := \left\{ \sum_{j=0}^{d-1}(-1)^{x_j}|\pi(j)\rangle\langle j| : \ \pi\in S_d,\ x\in\{0,1\}^d \right\}$$

$$\Theta_0 := \Phi, \qquad \Theta_1 := P-\Phi, \qquad \Theta_2 := \frac{\mathbb{I}+F-2P}{2}, \qquad \Theta_3 := \frac{\mathbb{I}-F}{2},$$

(Max. ent. state)

(Projector on the antisymmetric subspace)

$$\Phi := \frac{1}{d}\sum_{i,j=0}^{d-1}|i\rangle\langle j|\otimes|i\rangle\langle j|$$ (Max. ent. state)

$$P := \sum_{i=0}^{d-1}|i\rangle\langle i|\otimes|i\rangle\langle i|$$ (Projector on max. correlated subspace)

$$F := \sum_{i,j=0}^{d-1}|i\rangle\langle j|\otimes|j\rangle\langle i|$$ (Flip operator)

$\Theta_0, \Theta_1, \Theta_2, \Theta_3$ are mutually orthogonal projectors, and satisfy

$$\sum_{i=0}^{3}\Theta_i = \mathbb{I}$$

$$\sigma_1 := \frac{1}{2}\left(\frac{\Theta_1}{\mathrm{Tr}\Theta_1} + \frac{\Theta_3}{\mathrm{Tr}\Theta_3}\right)$$ “Biblical state”

$$\Theta_1 := P - \Phi,$$

$$\Theta_3 := \frac{\mathbb{I} - F}{2},$$

(Projector on the antisymmetric subspace)

$\Phi := \frac{1}{d}\sum_{i,j=0}^{d-1} |i\rangle\langle j| \otimes |i\rangle\langle j|$ (Max. ent. state)

$P := \sum_{i=0}^{d-1} |i\rangle\langle i| \otimes |i\rangle\langle i|$ (Projector on max. correlated subspace)

$F := \sum_{i,j=0}^{d-1} |i\rangle\langle j| \otimes |j\rangle\langle i|$ (Flip operator)

$$\sigma_0 := \frac{1}{d}\Theta_0 + \frac{2}{d^2}\Theta_2$$

$$\sigma_1 := \frac{1}{2(d-1)}\Theta_1 + \frac{1}{d(d-1)}\Theta_3$$

"Biblical state"

$$\Theta_0 := \Phi, \qquad \Theta_1 := P - \Phi, \qquad \Theta_2 := \frac{\mathbb{I} + F - 2P}{2}, \qquad \Theta_3 := \frac{\mathbb{I} - F}{2},$$

(Max. ent. state)

(Projector on the antisymmetric subspace)

$$\Phi := \frac{1}{d}\sum_{i,j=0}^{d-1} |i\rangle\langle j| \otimes |i\rangle\langle j|$$ (Max. ent. state)

$$P := \sum_{i=0}^{d-1} |i\rangle\langle i| \otimes |i\rangle\langle i|$$ (Projector on max. correlated subspace)

$$F := \sum_{i,j=0}^{d-1} |i\rangle\langle j| \otimes |j\rangle\langle i|$$ (Flip operator)

$\Theta_0, \Theta_1, \Theta_2, \Theta_3$ are mutually orthogonal projectors, and satisfy

$$\sum_{i=0}^{3} \Theta_i = \mathbb{I}$$

$$\sigma_0 := \frac{1}{d}\Theta_0 + \frac{2}{d^2}\Theta_2$$

$$\sigma_1 := \frac{1}{2(d-1)}\Theta_1 + \frac{1}{d(d-1)}\Theta_3$$

“Biblical state”

σ_0 and σ_1 are separable and orthogonal

Even state: $\rho_0^{(k)} := \frac{1}{2^{k-1}} \sum_{\substack{x_1,\ldots,x_k \in \{0,1\} \\ x_1+\cdots+x_k \equiv 0 \pmod 2}} \sigma_{x_1} \otimes \cdots \otimes \sigma_{x_k}$

Odd state: $\rho_1^{(k)} := \frac{1}{2^{k-1}} \sum_{\substack{x_1,\ldots,x_k \in \{0,1\} \\ x_1+\cdots+x_k \equiv 1 \pmod 2}} \sigma_{x_1} \otimes \cdots \otimes \sigma_{x_k}$

$$\frac{1}{2}\|\rho_0^{(k)} - \rho_1^{(k)}\|_{\mathrm{PPT}} \overset{\text{Symmetry}}{=} \text{linear program}$$

PPT norm between the even and odd states

$$\frac{1}{2}\|\rho_0^{(k)} - \rho_1^{(k)}\|_{\mathrm{PPT}} = \inf_{\mathbf{x}\in\mathbb{R}^{4^k}} \left[\|\mathbf{x}\|_1 + \|W^{\otimes k}\mathbf{x} - \mathbf{r}^{\otimes k}\|_1\right]$$

where $W \in \mathbb{R}^{4\times 4}$ and $\mathbf{r} \in \mathbb{R}^4$.

$$\mathbf{r} := \begin{pmatrix} \frac{1}{2d} \\ -\frac{1}{4} \\ \frac{d-1}{2d} \\ -\frac{1}{4} \end{pmatrix} \qquad W := \begin{pmatrix} \frac{1}{d} & \frac{1}{d} & \frac{1}{d} & -\frac{1}{d} \\ 1-\frac{1}{d} & 1-\frac{1}{d} & -\frac{1}{d} & \frac{1}{d} \\ \frac{d-1}{2} & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ -\frac{d-1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

- $$\frac{1}{2}\|\rho_0^{(k)} - \rho_1^{(k)}\|_{\mathrm{PPT}} = \inf_{\mathbf{x}\in\mathbb{R}^{4^k}} \left[\|W^{\otimes k}\mathbf{x} - \mathbf{r}^{\otimes k}\|_1 + \|\mathbf{x}\|_1\right]$$

- $$\frac{1}{2}\|\rho_0^{(k)} - \rho_1^{(k)}\|_{\mathrm{PPT}} = \inf_{\mathbf{x}\in\mathbb{R}^{4^k}} \left[\|W^{\otimes k}\mathbf{x} - \mathbf{r}^{\otimes k}\|_1 + \|\mathbf{x}\|_1\right]$$

$$\leq 2^{k+\frac{1}{2}} \inf_{\mathbf{x}\in\mathbb{R}^{4^k}} \sqrt{\|W^{\otimes k}\mathbf{x} - \mathbf{r}^{\otimes k}\|_2^2 + \|\mathbf{x}\|_2^2}$$

- $$\frac{1}{2}\|\rho_0^{(k)} - \rho_1^{(k)}\|_{\mathrm{PPT}} = \inf_{\mathbf{x}\in\mathbb{R}^{4^k}} \left[\|W^{\otimes k}\mathbf{x} - \mathbf{r}^{\otimes k}\|_1 + \|\mathbf{x}\|_1\right]$$

$$\leq 2^{k+\frac{1}{2}} \inf_{\mathbf{x}\in\mathbb{R}^{4^k}} \sqrt{\|W^{\otimes k}\mathbf{x} - \mathbf{r}^{\otimes k}\|_2^2 + \|\mathbf{x}\|_2^2}$$

Tikhonov-regularised least squares

$$\inf_{\mathbf{x}} \left[\|A\mathbf{x} - \mathbf{b}\|_2^2 + \|\mathbf{x}\|_2^2\right] = \sum_i \frac{(\mathbf{u}_i^\intercal \mathbf{b})^2}{1+\sigma_i^2}$$

where $A = \sum_i \sigma_i \mathbf{u}_i \mathbf{v}_i^\intercal$ is a singular value decomposition for A

- $$\frac{1}{2}\|\rho_0^{(k)} - \rho_1^{(k)}\|_{\mathrm{PPT}} = \inf_{\mathbf{x}\in\mathbb{R}^{4^k}} \left[\|W^{\otimes k}\mathbf{x} - \mathbf{r}^{\otimes k}\|_1 + \|\mathbf{x}\|_1\right]$$

$$\leq 2^{k+\frac{1}{2}} \inf_{\mathbf{x}\in\mathbb{R}^{4^k}} \sqrt{\|W^{\otimes k}\mathbf{x} - \mathbf{r}^{\otimes k}\|_2^2 + \|\mathbf{x}\|_2^2}$$

Tikhonov-regularised least squares

$$\inf_{\mathbf{x}} \left[\|A\mathbf{x} - \mathbf{b}\|_2^2 + \|\mathbf{x}\|_2^2\right] = \sum_i \frac{(\mathbf{u}_i^\intercal \mathbf{b})^2}{1+\sigma_i^2}$$

where $A = \sum_i \sigma_i \mathbf{u}_i \mathbf{v}_i^\intercal$ is a singular value decomposition for A

- The last step of the proof uses the Sanov's theorem

(Sanov's theorem quantifies how unlikely it is that an empirical distribution of k i.i.d. samples deviates from the true distribution)

Proposition (Upper bound on the LOCC-norm between the even and odd states)

The even and odd states satisfies

$$\frac{1}{4}\|\rho_0^{(k)} - \rho_1^{(k)}\|_{\mathrm{LOCC}} \leq \mu^k$$

where $\mu \in (0,1)$.

$$\mu = \sqrt{1 - \frac{\frac{5}{8} + \frac{1}{d}\left(\frac{1}{4} + \frac{2}{d} + \frac{9}{d^2} - \frac{6}{d^3} - \sqrt{2}\left(\frac{9}{4} + \frac{3}{d} + \frac{1}{d^2}\right)\sqrt{1 - \frac{2}{d + \frac{4}{d}}}\right)}{1 + \frac{2}{d} + \frac{4}{d^2}}}$$

Proposition (Upper bound on the LOCC-norm between the even and odd states)

The even and odd states satisfies

$$\frac{1}{4}\|\rho_0^{(k)} - \rho_1^{(k)}\|_{\mathrm{LOCC}} \leq \mu^k$$

where $\mu \in (0,1)$.

$$\mu = \sqrt{1 - \frac{\frac{5}{8} + \frac{1}{d}\left(\frac{1}{4} + \frac{2}{d} + \frac{9}{d^2} - \frac{6}{d^3} - \sqrt{2}\left(\frac{9}{4} + \frac{3}{d} + \frac{1}{d^2}\right)\sqrt{1 - \frac{2}{d + \frac{4}{d}}}\right)}{1 + \frac{2}{d} + \frac{4}{d^2}}}$$

→

For k sufficiently large, it holds $\frac{1}{2}\|\rho_0^{(k)} - \rho_1^{(k)}\|_{\mathrm{LOCC}} \leq \varepsilon$, i.e.

$\rho_0^{(k)}$ and $\rho_1^{(k)}$ form a pair of separable ε-quantum data hiding states.

Proposition (Upper bound on the LOCC-norm between the even and odd states)

The even and odd states satisfies

$$\frac{1}{4}\|\rho_0^{(k)} - \rho_1^{(k)}\|_{\mathrm{LOCC}} \leq \mu^k$$

where $\mu \in (0,1)$.

$$\mu = \sqrt{1 - \frac{\frac{5}{8} + \frac{1}{d}\left(\frac{1}{4} + \frac{2}{d} + \frac{9}{d^2} - \frac{6}{d^3} - \sqrt{2}\left(\frac{9}{4} + \frac{3}{d} + \frac{1}{d^2}\right)\sqrt{1 - \frac{2}{d + \frac{4}{d}}}\right)}{1 + \frac{2}{d} + \frac{4}{d^2}}}$$

→ For k sufficiently large, it holds $\frac{1}{2}\|\rho_0^{(k)} - \rho_1^{(k)}\|_{\mathrm{LOCC}} \leq \varepsilon$, i.e.

$\rho_0^{(k)}$ and $\rho_1^{(k)}$ form a pair of separable ε-quantum data hiding states.

Optimising over k, the local dimension is $D = O(1/\varepsilon^{10})$.

Proposition (Upper bound on the LOCC-norm between the even and odd states)

The even and odd states satisfies

$$\frac{1}{4}\|\rho_0^{(k)} - \rho_1^{(k)}\|_{\mathrm{LOCC}} \leq \mu^k$$

where $\mu \in (0,1)$.

$$\mu = \sqrt{1 - \frac{\frac{5}{8} + \frac{1}{d}\left(\frac{1}{4} + \frac{2}{d} + \frac{9}{d^2} - \frac{6}{d^3} - \sqrt{2}\left(\frac{9}{4} + \frac{3}{d} + \frac{1}{d^2}\right)\sqrt{1 - \frac{2}{d + \frac{4}{d}}}\right)}{1 + \frac{2}{d} + \frac{4}{d^2}}}$$

→ For k sufficiently large, it holds $\frac{1}{2}\|\rho_0^{(k)} - \rho_1^{(k)}\|_{\mathrm{LOCC}} \leq \varepsilon$, i.e.

$\rho_0^{(k)}$ and $\rho_1^{(k)}$ form a pair of separable ε-quantum data hiding states.

Optimising over k, the local dimension is $D = O(1/\varepsilon^{10})$.

All ε-quantum data hiding states on $\mathbb{C}^D \otimes \mathbb{C}^D$ must satisfy $D = \Omega(1/\varepsilon)$. Matthews, Wehner, and Winter; *CMP* (2009)
Lami, Palazuelos, and Winter; *CMP* (2018)

Conclusions

- Constructions of **separable** ε-quantum data hiding states for all $\varepsilon > 0$

(i.e. a pair of states that are separable, orthogonal, and ε-close in LOCC-norm)

Conclusions

- Constructions of **separable** ε-quantum data hiding states for all $\varepsilon > 0$

(i.e. a pair of states that are separable, orthogonal, and ε-close in LOCC-norm)

See also the independent work [Ha and Kim, *PRA*, (2025)]

Conclusions

- Constructions of **separable** ε-quantum data hiding states for all $\varepsilon > 0$

  (i.e. a pair of states that are separable, orthogonal, and ε-close in LOCC-norm)

  See also the independent work [Ha and Kim, *PRA*, (2025)]

- The key idea is to exploit the *parity trick* and *symmetries*

Conclusions

- Constructions of **separable** ε-quantum data hiding states for all $\varepsilon > 0$

  (i.e. a pair of states that are separable, orthogonal, and ε-close in LOCC-norm)

  See also the independent work [Ha and Kim, *PRA*, (2025)]

- The key idea is to exploit the *parity trick* and *symmetries*

- **Open problem** (Sub-multiplicativity of LOCC-norm)

$$\|(\rho_1 - \sigma_1) \otimes (\rho_2 - \sigma_2)\|_{\mathrm{LOCC}} \overset{?}{\leq} \|\rho_1 - \sigma_1\|_{\mathrm{LOCC}} \|\rho_2 - \sigma_2\|_{\mathrm{LOCC}}$$

(And similar the PPT norm)

Conclusions

- Constructions of **separable** ε-quantum data hiding states for all $\varepsilon > 0$

  (i.e. a pair of states that are separable, orthogonal, and ε-close in LOCC-norm)

  See also the independent work [Ha and Kim, *PRA*, (2025)]

- The key idea is to exploit the *parity trick* and *symmetries*

- **Open problem** (Sub-multiplicativity of LOCC-norm)

$$\|(\rho_1 - \sigma_1) \otimes (\rho_2 - \sigma_2)\|_{\mathrm{LOCC}} \overset{?}{\leq} \|\rho_1 - \sigma_1\|_{\mathrm{LOCC}} \|\rho_2 - \sigma_2\|_{\mathrm{LOCC}}$$

(And similar the PPT norm)

This would imply:

Conjecture

Let σ_0, σ_1 separable-orthogonal states satisfying $\frac{1}{2}\|\sigma_1 - \sigma_0\|_{\mathrm{LOCC}} < 1$. Then, for k sufficiently large, the associated even and odd states form a pair of **separable** ε-quantum data hiding states.

Thank you!