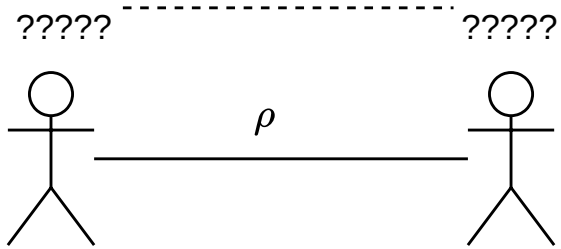
Robustness of quantum data hiding against entangled catalysts and memory

Aby Philip

Institute of Fundemental Technological Research, Polish Academy of Sciences

Based on work with Alexander Streltsov. **arXiv:2511.04408**

Motivation



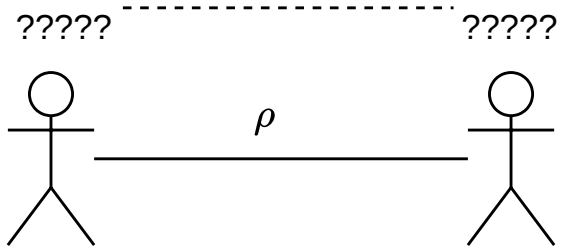
Given a set of states shared between distant parties, Alice and Bob, can they identify which state they hold using only LOCC?

For two orthogonal pure states, the answer is always yes [1].

However, when considering larger and more general sets of states, things are more interesting.

[1] Walgate *et al.*, PRL (2000).

Motivation



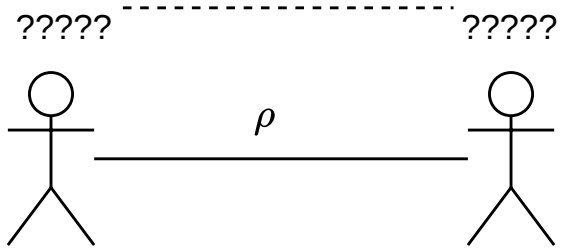
Given a set of states shared between distant parties, Alice and Bob, can they identify which state they hold using only LOCC?

For two orthogonal pure states, the answer is always yes [1].

However, when considering larger and more general sets of states, things are more interesting.

[1] Walgate *et al.*, PRL (2000).

Motivation



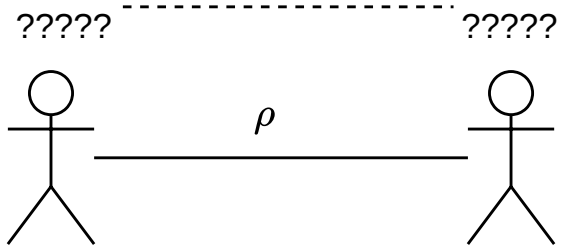
Given a set of states shared between distant parties, Alice and Bob, can they identify which state they hold using only LOCC?

For two orthogonal pure states, the answer is always yes [1].

However, when considering larger and more general sets of states, things are more interesting.

[1] Walgate *et al.*, PRL (2000).

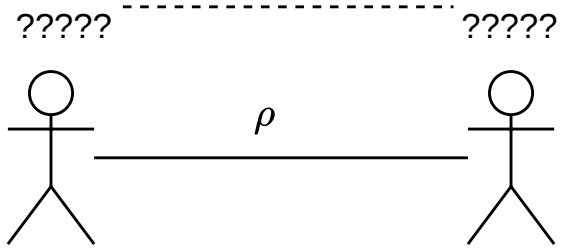
Motivation to hide



- Quantum data hiding [2] is where classical information is encoded into bipartite states
- that are perfectly distinguishable in principle,
- yet almost indistinguishable by any LOCC procedure.

[2] Terhal *et al.*, PRL (2001). DiVincenzo *et al.*, IEEE ToIT (2002)

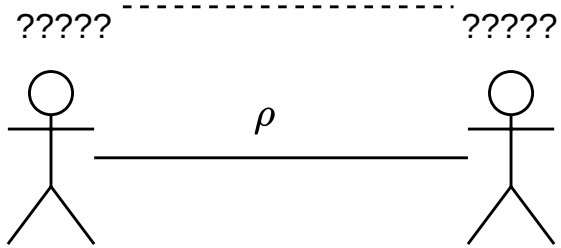
Motivation to hide



- Quantum data hiding [2] is where classical information is encoded into bipartite states
- that are perfectly distinguishable in principle,
- yet almost indistinguishable by any LOCC procedure.

[2] Terhal *et al.*, PRL (2001). DiVincenzo *et al.*, IEEE ToIT (2002)

Motivation to hide



- Quantum data hiding [2] is where classical information is encoded into bipartite states
- that are perfectly distinguishable in principle,
- yet almost indistinguishable by any LOCC procedure.

[2] Terhal *et al.*, PRL (2001). DiVincenzo *et al.*, IEEE ToIT (2002)

Motivation to hide data

Can we "un-hide" data hiding states using quantum catalysts or quantum memory?

What if you had some shared entanglement? Not a supply of shared entanglement but just a finite initial amount.

Motivation to hide data

Can we "un-hide" data hiding states using quantum catalysts or quantum memory?

What if you had some shared entanglement? Not a supply of shared entanglement but just a finite initial amount.

Previously...

With access to all possible quantum operation, you could distinguish $\{\rho_0, \rho_1\}$ with probability

$$P_{\text{opt}}(\rho_0, \rho_1) = \frac{1}{2} + \frac{1}{4}\left\|\rho_0 - \rho_1\right\|_1, \tag{1}$$

where $\|M\|_1 = \text{Tr}\sqrt{M^\dagger M}$ is the trace norm.

Previously...

With access to only LOCC, Alice and Bob could distinguish $\{\rho_0^{AB}, \rho_1^{AB}\}$ with probability

$$P_{\mathrm{LOCC}}(\rho_0^{AB}, \rho_1^{AB}) = \frac{1}{2} + \frac{1}{4}\|\rho_0^{AB} - \rho_1^{AB}\|_{\mathrm{LOCC}}. \tag{2}$$

Here $\|\cdot\|_{\mathrm{LOCC}}$ is the LOCC norm.

Previously...

The *LOCC norm* of an operator X is defined as [3]

$$\|X\|_{\mathrm{LOCC}} = \sup_{\mathcal{M}} \|\mathcal{M}(X)\|_1, \tag{3}$$

where the supremum is taken over all LOCC measurement channels $\mathcal{M}$.

By the data processing inequality for the trace norm, it follows that

$$\|\rho_0^{AB} - \rho_1^{AB}\|_{\mathrm{LOCC}} \leq \|\rho_0^{AB} - \rho_1^{AB}\|_1, \tag{4}$$

for any pair of quantum states ρ_0 and ρ_1.

[3] Matthews *et al.*, CMP (2009)

Previously...

The *LOCC norm* of an operator X is defined as [3]

$$\|X\|_{\mathrm{LOCC}} = \sup_{\mathcal{M}} \|\mathcal{M}(X)\|_1, \tag{3}$$

where the supremum is taken over all LOCC measurement channels $\mathcal{M}$.

By the data processing inequality for the trace norm, it follows that

$$\|\rho_0^{AB} - \rho_1^{AB}\|_{\mathrm{LOCC}} \leq \|\rho_0^{AB} - \rho_1^{AB}\|_1, \tag{4}$$

for any pair of quantum states ρ_0 and ρ_1.

[3] Matthews *et al.*, CMP (2009)

Quantum Data Hiding

States that are perfectly distinguished by a global measurement but, they remain almost indistinguishable when restricted to LOCC

For any $\varepsilon > 0$, there exist bipartite quantum states ρ_0^{AB} and ρ_1^{AB} such that [4]

$$P_{\text{opt}}(\rho_0, \rho_1) = 1, \tag{5}$$

$$P_{\text{LOCC}}(\rho_0, \rho_1) < \frac{1}{2} + \varepsilon. \tag{6}$$

[4] Eggling & Werner, PRL (2001). Hayden *et al.* CMP (2004). Aubrun & Lancien, QIC (2015). Ha & Kim, PRA (2025). Anna Mele & Lami (2025)

Quantum Data Hiding

States that are perfectly distinguished by a global measurement but, they remain almost indistinguishable when restricted to LOCC

For any $\varepsilon > 0$, there exist bipartite quantum states ρ_0^{AB} and ρ_1^{AB} such that [4]

$$P_{\text{opt}}(\rho_0, \rho_1) = 1, \tag{5}$$

$$P_{\text{LOCC}}(\rho_0, \rho_1) < \frac{1}{2} + \varepsilon. \tag{6}$$

[4] Eggling & Werner, PRL (2001). Hayden *et al.* CMP (2004). Aubrun & Lancien, QIC (2015). Ha & Kim, PRA (2025). Anna Mele & Lami (2025)

Quantum Data Hiding

Can we "un-hide" data hiding states using quantum catalysts or quantum memory?

Quantum Catalyst

A quantum state of the catalyst $\tau^{A'B'}$ and an LOCC protocol Λ_{LOCC} such that

$$\Lambda_{\mathrm{LOCC}}\left(\rho_i^{AB} \otimes \tau^{A'B'}\right) = \sigma_i^{AB} \otimes \tau^{A'B'}, \tag{7}$$

$$P_{\mathrm{LOCC}}\left(\sigma_0^{AB}, \sigma_1^{AB}\right) > P_{\mathrm{LOCC}}\left(\rho_0^{AB}, \rho_1^{AB}\right). \tag{8}$$

Quantum Memory

- A fixed finite-dimensional auxiliary bipartite system
- LOCC operations in each round
- Reuse of the updated auxiliary state in later rounds, with no requirement that the memory be restored to its initial state.

Setup

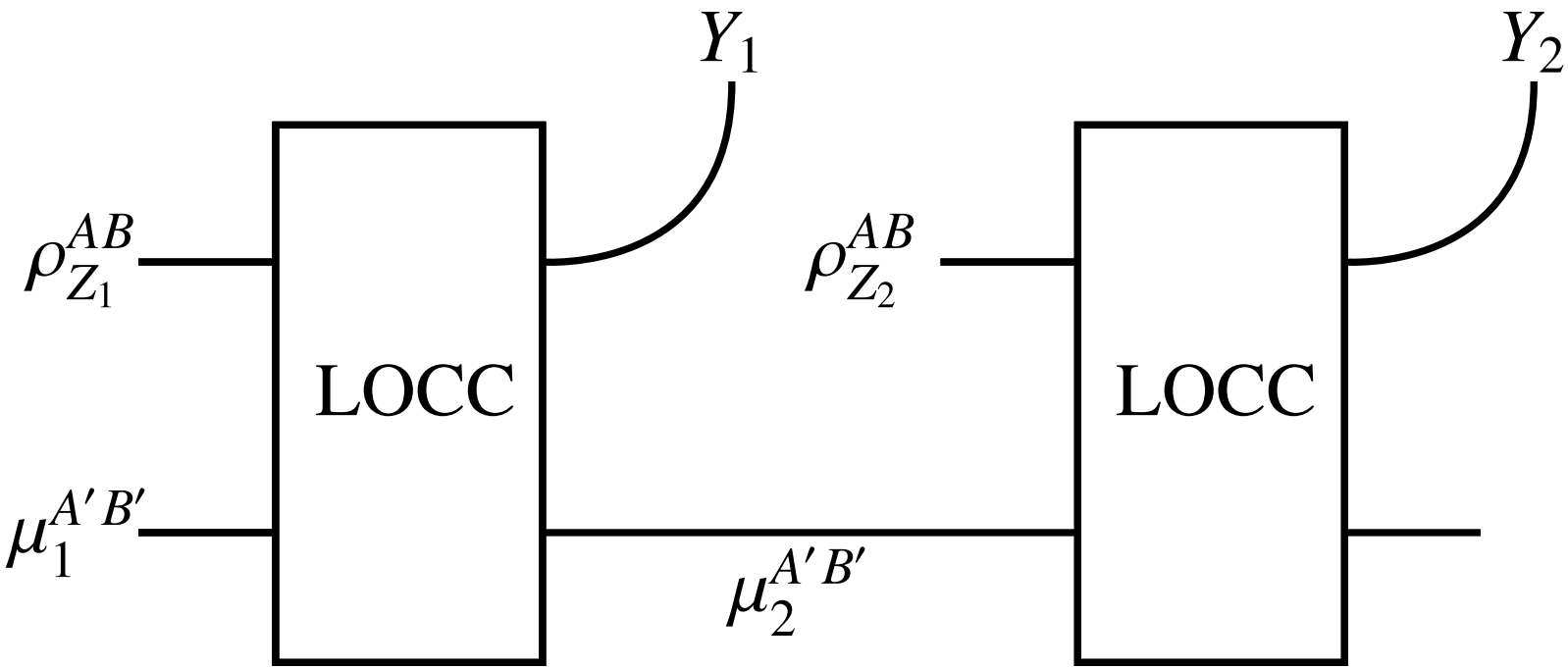


Figure: Z_j is an i.i.d. random variable taking values in $\{0,1\}$ uniformly at random. $Y_j \in \{0,1\}$ denote the outcome of Alice and Bob's guess in the j-th round.

Further define X_j to represent whether the guess in round j is correct:

$$X_j = \begin{cases} 1, & \text{if } Y_j = Z_j, \\ 0, & \text{otherwise.} \end{cases} \tag{9}$$

The total number of correct guesses after n rounds is then given by

$$S_n = \sum_{j=1}^{n} X_j. \tag{10}$$

Setup

We say that the rate $r \in [0, 1]$ is achievable if, for every $\varepsilon > 0$ and $n' > 0$, there exists $n \geq n'$ such that

$$\Pr(S_n \geq n \cdot r) \geq 1 - \varepsilon. \tag{11}$$

The *optimal success rate* R is then obtained by taking supremum over all achievable rates r.

Quantum Memory/Catalyst

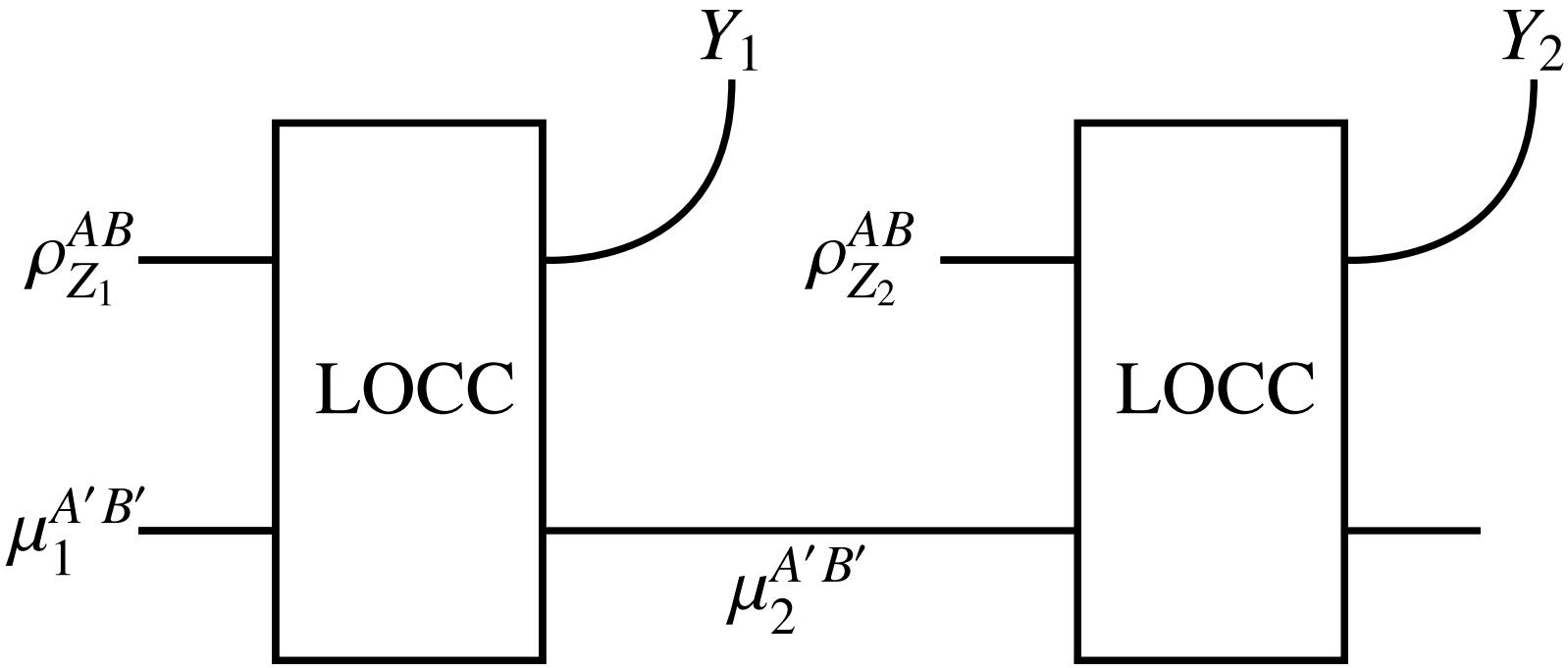


Figure: For a quantum catalyst, $\mu_1 = \mu_2$. This needn't be true for quantum memory.

Can't beat separable states

Theorem

For separable data hiding states $\rho_{0,1}$ neither quantum catalysis nor quantum memory can increase the optimal success probability:

$$R_{\mathrm{m}}(\rho_0, \rho_1) = R_{\mathrm{c}}(\rho_0, \rho_1) = P_{\mathrm{LOCC}}(\rho_0, \rho_1). \tag{12}$$

Toward a contradiction

Assume that quantum memory does provide an advantage such that $R_{\mathrm{m}}(\rho_0, \rho_1) > P_{\mathrm{LOCC}}(\rho_0, \rho_1)$.

Let $\mu^{A'B'}$ be an initial state of the quantum memory, and $\{\mathcal{M}_j\}$ a sequence of LOCC protocols achieving the rate $R_{\mathrm{m}}(\rho_0, \rho_1)$.

Let $r_{\mathrm{m}} = R_{\mathrm{m}}(\rho_0, \rho_1)$ and $p_{\mathrm{LOCC}} = P_{\mathrm{LOCC}}(\rho_0, \rho_1)$, and

Fix $\delta > 0$ such that $r_{\mathrm{m}} > p_{\mathrm{LOCC}} + \delta$.

Toward a contradiction

Assume that quantum memory does provide an advantage such that $R_{\mathrm{m}}(\rho_0, \rho_1) > P_{\mathrm{LOCC}}(\rho_0, \rho_1)$.

Let $\mu^{A'B'}$ be an initial state of the quantum memory, and $\{\mathcal{M}_j\}$ a sequence of LOCC protocols achieving the rate $R_{\mathrm{m}}(\rho_0, \rho_1)$.

Let $r_{\mathrm{m}} = R_{\mathrm{m}}(\rho_0, \rho_1)$ and $p_{\mathrm{LOCC}} = P_{\mathrm{LOCC}}(\rho_0, \rho_1)$, and

Fix $\delta > 0$ such that $r_{\mathrm{m}} > p_{\mathrm{LOCC}} + \delta$.

Toward a contradiction

Assume that quantum memory does provide an advantage such that $R_{\mathrm{m}}(\rho_0, \rho_1) > P_{\mathrm{LOCC}}(\rho_0, \rho_1)$.

Let $\mu^{A'B'}$ be an initial state of the quantum memory, and $\{\mathcal{M}_j\}$ a sequence of LOCC protocols achieving the rate $R_{\mathrm{m}}(\rho_0, \rho_1)$.

Let $r_{\mathrm{m}} = R_{\mathrm{m}}(\rho_0, \rho_1)$ and $p_{\mathrm{LOCC}} = P_{\mathrm{LOCC}}(\rho_0, \rho_1)$, and

Fix $\delta > 0$ such that $r_{\mathrm{m}} > p_{\mathrm{LOCC}} + \delta$.

If there were an advantage

An important consequence is that Alice and Bob could exploit such an advantage to probe the initial state of the memory itself.

In the following protocol, $\eta_j^{A'B'}$ is either $\gamma^{A'B'} \in \mathrm{SEP}$ or $\mu^{A'B'} \notin \mathrm{SEP}$ such that $\|\tau^{A'B'} - \gamma^{A'B'}\|_1 \neq 2$.

If there were an advantage

An important consequence is that Alice and Bob could exploit such an advantage to probe the initial state of the memory itself.

In the following protocol, $\eta_j^{A'B'}$ is either $\gamma^{A'B'} \in \text{SEP}$ or $\mu^{A'B'} \notin \text{SEP}$ such that $\|\tau^{A'B'} - \gamma^{A'B'}\|_1 \neq 2$.

Then

- Alice and Bob choose $Z_j \in \{0, 1\}$ uniformly at random.
- They set $X_j = \perp$.
- If $Z_j = 0$, prepare the state ρ_0^{AB} using LOCC, else ρ_1^{AB}.
- They apply the LOCC protocol $\mathcal{M}_j$ on $\rho_{Z_j}^{AB} \otimes \eta_j^{A'B'}$.
- Measure the system registers in the computational basis.
- Obtain Y_j. If $Y_j = Z_j$, then set $X_j = 1$, else $X_j = 0$.
- Update j to $j + 1$.

P.S. $\mathcal{M}_j$ can depend on the outcomes of the previous rounds.

Then

- Alice and Bob choose $Z_j \in \{0, 1\}$ uniformly at random.
- They set $X_j = \perp$.
- If $Z_j = 0$, prepare the state ρ_0^{AB} using LOCC, else ρ_1^{AB}.
- They apply the LOCC protocol $\mathcal{M}_j$ on $\rho_{Z_j}^{AB} \otimes \eta_j^{A'B'}$.
- Measure the system registers in the computational basis.
- Obtain Y_j. If $Y_j = Z_j$, then set $X_j = 1$, else $X_j = 0$.
- Update j to $j + 1$.

P.S. $\mathcal{M}_j$ can depend on the outcomes of the previous rounds.

Then

After n rounds, Alice and Bob compute $S_n = \sum_{i=1}^{n} X_j$. If

$$\frac{S_n}{n} - p_{\mathrm{LOCC}} \geq \delta, \tag{13}$$

then Alice and Bob guess that the initial state of the memory register was $\mu^{A'B'} \notin \mathrm{SEP}$, else $\gamma^{A'B'} \in \mathrm{SEP}$.

Simple

Case 1: If the initial state is $\eta_1^{A'B'} = \mu^{A'B'}$,

$$P_{\text{corr}}(\mu) = \Pr(S_n - np_{\text{LOCC}} \geq n\delta)\,. \tag{14}$$

By assumption, for every $\varepsilon > 0$ and $n' > 0$, there exists some $n \geq n'$ such that

$$\Pr(S_n \geq nr_{\text{m}}) \geq 1 - \varepsilon. \tag{15}$$

Recalling that $r_{\text{m}} > p_{\text{LOCC}} + \delta$, we get $P_{\text{corr}}(\mu) \geq 1 - \varepsilon$.

Case 1: If the initial state is $\eta_1^{A'B'} = \mu^{A'B'}$,

$$P_{\mathrm{corr}}(\mu) = \mathrm{Pr}(S_n - np_{\mathrm{LOCC}} \geq n\delta)\,. \tag{14}$$

By assumption, for every $\varepsilon > 0$ and $n' > 0$, there exists some $n \geq n'$ such that

$$\mathrm{Pr}(S_n \geq nr_{\mathrm{m}}) \geq 1 - \varepsilon. \tag{15}$$

Recalling that $r_{\mathrm{m}} > p_{\mathrm{LOCC}} + \delta$, we get $P_{\mathrm{corr}}(\mu) \geq 1 - \varepsilon$.

Not so simple

Case 2: If the initial state of the catalyst is $\eta_1^{A'B'} = \gamma^{A'B'} \in \text{SEP}$,

We cannot assume that each round of the process will be independent and identically distributed.

Since the register $A'B'$ was initially in a separable state $\gamma^{A'B'}$, it will remain in a separable state throughout the protocol.

Not so simple

Case 2: If the initial state of the catalyst is $\eta_1^{A'B'} = \gamma^{A'B'} \in \mathrm{SEP}$,

We cannot assume that each round of the process will be independent and identically distributed.

Since the register $A'B'$ was initially in a separable state $\gamma^{A'B'}$, it will remain in a separable state throughout the protocol.

A key point

Note that the addition of a separable state cannot increase the probability of distinguishing between ρ_0^{AB} and ρ_1^{AB}.

Hence, for the $j+1$-th round, the probability for Alice and Bob to make a correct guess can be bounded as

$$\Pr(X_{j+1} = 1 | X_1 \dots X_j) \leq \frac{1}{2} + \frac{1}{4} \|\rho_0^{AB} - \rho_1^{AB}\|_{\mathrm{LOCC}} = p_{\mathrm{LOCC}}. \quad (16)$$

A key point

Note that the addition of a separable state cannot increase the probability of distinguishing between ρ_0^{AB} and ρ_1^{AB}.

Hence, for the $j+1$-th round, the probability for Alice and Bob to make a correct guess can be bounded as

$$\Pr(X_{j+1} = 1 | X_1 \dots X_j) \leq \frac{1}{2} + \frac{1}{4} \|\rho_0^{AB} - \rho_1^{AB}\|_{\mathrm{LOCC}} = p_{\mathrm{LOCC}}. \quad (16)$$

Supermartingales

Let us now consider the random variable $C_j := S_j - j \cdot p_{\mathrm{LOCC}}$ for $1 \leq j \leq n$ and $C_0 = 0$. Then, we show that

$$\mathbb{E}[C_{j+1}|C_j, \ldots, C_1] \leq C_j \tag{17}$$

$$|C_{j+1} - C_j| \leq 1 \tag{18}$$

Hence, C_j is a supermartingale.

Supermartingales

Using Azuma's inequality [5] for supermartingales, we get

$$P_{\mathrm{corr}}(\gamma) = \Pr\left(\frac{S_n}{n} - p_{\mathsf{LOCC}} < \delta\right)$$
$$\geq 1 - \exp\left(\frac{-n\delta^2}{2}\right). \tag{19}$$

[5] Azuma, Tohoku Mathematical Journal (1967)

Reductio ad absurdum?

Then, we get that the protocol succeeds in distinguishing $\gamma^{A'B'} \in \text{SEP}$ and $\mu^{A'B'} \notin \text{SEP}$ with probability

$$\begin{aligned} P_{\text{corr}} &= \frac{1}{2}\left[P_{\text{corr}}(\mu) + P_{\text{corr}}(\gamma)\right] \\ &\geq \frac{1}{2}\left(1-\varepsilon\right) + \frac{1}{2}\left(1 - \exp\left(-n\delta^2/2\right)\right). \end{aligned} \tag{20}$$

Picking an arbitrarily small $\varepsilon > 0$ and an arbitrarily large n,

$$P_{\text{corr}} \;>\; \frac{1}{2} + \frac{\|\mu^{A'B'} - \gamma^{A'B'}\|_1}{4}, \tag{21}$$

Reductio ad absurdum

Hence, it would appear that Alice and Bob can distinguish

between two non-orthogonal states $\gamma^{A'B'}$ and $\mu^{A'B'}$

using the above-mentioned LOCC protocol with probability greater than the maximum of P_{opt}.

This is a contradiction. Hence, proved.

Reductio ad absurdum

Hence, it would appear that Alice and Bob can distinguish

between two non-orthogonal states $\gamma^{A'B'}$ and $\mu^{A'B'}$

using the above-mentioned LOCC protocol with probability greater than the maximum of P_{opt}.

This is a contradiction. Hence, proved.

Reductio ad absurdum

Hence, it would appear that Alice and Bob can distinguish

between two non-orthogonal states $\gamma^{A'B'}$ and $\mu^{A'B'}$

using the above-mentioned LOCC protocol with probability greater than the maximum of P_{opt}.

This is a contradiction. Hence, proved.

Remember Quantum Memory

Theorem

For every $\varepsilon, \delta > 0$ there exist data hiding states ρ_0, ρ_1 such that

$$P_{\mathrm{LOCC}}(\rho_0, \rho_1) < \frac{1}{2} + \varepsilon, \tag{22}$$

$$R_{\mathrm{m}}(\rho_0, \rho_1) > 1 - \delta. \tag{23}$$

Proof Outline

Let $\sigma_0^{A_1B_1}$ and $\sigma_0^{A_1B_1}$ be data hiding states.

$$\rho_0^{AB} = \sigma_0^{A_1B_1} \otimes |\psi\rangle\langle\psi|^{A_2B_2}, \tag{24}$$

$$\rho_1^{AB} = \sigma_1^{A_1B_1} \otimes |\psi\rangle\langle\psi|^{A_2B_2}. \tag{25}$$

where $|\psi\rangle^{A_2B_2}$ be an entangled state, for some $\varepsilon' > 0$ satisfying

$$\left\| |\psi\rangle\langle\psi|^{A_2B_2} - |00\rangle\langle 00| \right\|_1 < \varepsilon', \tag{26}$$

$$S(\psi^{A_2}) > \log_2 d_{A_1} \tag{27}$$

Alice and Bob can store sufficiently many copies of the pure state $|\psi\rangle$ in the quantum memory and subsequently distill them into Bell states in later rounds.

So, TL DR

- when the hiding states are separable, neither borrowing an entangled catalyst nor employing a reusable quantum memory can improve the optimal success probability

- for entangled data hiding states, access to a reusable quantum memory offers a significant advantage

So, TL DR

- when the hiding states are separable, neither borrowing an entangled catalyst nor employing a reusable quantum memory can improve the optimal success probability

- for entangled data hiding states, access to a reusable quantum memory offers a significant advantage

Acknowledgments

This work was supported by the National Science Centre Poland (Grant No. 2022/46/E/ST2/00115 and 2024/55/B/ST2/01590).

- when the hiding states are separable, neither borrowing an entangled catalyst nor employing a reusable quantum memory can improve the optimal success probability

- for entangled data hiding states, access to a reusable quantum memory offers a significant advantage

Thank you for your attention