Information Efficiency of Quantum Data Hiding

Andreas Winter
(ICREA & Universitat Autònoma de Barcelona)

BIID 5, IMS@NUS, 27/7/2017
Outline

1. The discrimination problem
2. Local ("LOCC") data hiding
3. Distinguishability norms
4. Information efficiency of LOCC hiding
5. Discussion
1. Discrimination problem

Assume that well-characterized system (Hilbert space \( \mathcal{H} \)) is equally likely in one of two states (density matrices): \( \rho_0 \) or \( \rho_1 \).
1. Discrimination problem

Assume that well-characterized system (Hilbert space \( \mathcal{H} \)) is equally likely in one of two states (density matrices): \( \rho_0 \) or \( \rho_1 \).

To distinguish, make a measurement and decide based on outcome: \( M_0, M_1 \geq 0 \) s.t. \( M_0 + M_1 = I \) (e.g. orthogonal projectors).
1. Discrimination problem

Assume that well-characterized system (Hilbert space $\mathcal{H}$) is equally likely in one of two states (density matrices): $\rho_0$ or $\rho_1$

To distinguish, make a measurement and decide based on outcome: $M_0$, $M_1 \geq 0$ s.t. $M_0 + M_1 = I$ (e.g. orthogonal projectors).

Want to maximise success probability $\Pr[\text{success}] = \frac{1}{2} \text{Tr} \rho_0 M_0 + \frac{1}{2} \text{Tr} \rho_1 M_1$
1. Discrimination problem

Want to maximise success probability

\[ \Pr\{\text{success}\} = \frac{1}{2} \text{Tr} \, \rho_0 \, M_0 + \frac{1}{2} \text{Tr} \, \rho_1 \, M_1 \]
1. Discrimination problem

\[ x = 0, 1 \]

Want to maximise success probability

\[ \text{Pr\{success\}} = \frac{1}{2} \text{Tr} \rho_0 M_0 + \frac{1}{2} \text{Tr} \rho_1 M_1 \]

\[ = \frac{1}{2} \text{Tr} \rho_0 M_0 + \frac{1}{2} \text{Tr} \rho_1 (I - M_0) \]
1. Discrimination problem

Want to maximise success probability

\[ \Pr[\text{success}] = \frac{1}{2} \text{Tr} \rho_0 M_0 + \frac{1}{2} \text{Tr} \rho_1 M_1 \]

\[ = \frac{1}{2} + \frac{1}{2} \text{Tr} (\rho_0 - \rho_1) M_0 \]
1. Discrimination problem

Want to maximise success probability

\[ \text{Pr\{success\}} = \frac{1}{2} \text{Tr} \rho_0 M_0 + \frac{1}{2} \text{Tr} \rho_1 M_1 \]

\[ = \frac{1}{2} + \frac{1}{4} \text{Tr} (\rho_0 - \rho_1)(M_0 - M_1) \]
1. Discrimination problem

\( x = 0, 1 \)

Want to maximise success probability

\[
\Pr[\text{success}] = \frac{1}{2} \Tr \rho_0 M_0 + \frac{1}{2} \Tr \rho_1 M_1
\]

\[
= \frac{1}{2} + \frac{1}{4} \Tr (\rho_0 - \rho_1)(M_0 - M_1)
\]

\[\max = ||\rho_0 - \rho_1||_1 \quad (\text{trace norm})\]

[Helstrom/Holevo]
1. Discrimination problem

\[ x = 0, 1 \]

\[ \max_{x_0} \Pr \{ \text{success} \} = \frac{1}{2} + \frac{1}{4} \| \rho_0 - p_1 \|_1 \]

\[ \| \rho_0 - p_1 \|_1 = \text{Tr} | \rho_0 - p_1 | \]
1. Discrimination problem

$\max \Pr\xi_{\text{succ}} \geq \frac{1}{2} + \frac{1}{4} \frac{1}{1||\rho_0 - \rho_1||_1}$

$||\rho_0 - \rho_1||_1 = Tr |\rho_0 - \rho_1|$

$= 2\sqrt{1 - |\langle \psi_0 | \psi_1 \rangle|^2}$

(for pure states)
1. Discrimination problem

$X = 0, 1$

$max Pr[\text{succ}] = \frac{1}{2} + \frac{1}{4} ||\rho_0 - \rho_1||_1$

$||\rho_0 - \rho_1||_1 = Tr |\rho_0 - \rho_1|$

$= 2\sqrt{1 - |\langle \psi_0 | \psi_1 \rangle|^2}$

Optimal measurement: $\rho_0 - \rho_1$

for pure states
1. Discrimination problem

\[ x=0,1 \]

\[ \rho_{\text{max}} \text{Pr}\{\text{success}\} = \frac{1}{2} + \frac{1}{4} \|\rho_0 - \rho_1\|_1 \]

\[ \|\rho_0 - \rho_1\|_1 = \text{Tr} \|\rho_0 - \rho_1\| \]

\[ = 2 \sqrt{1 - |<\psi_0|\psi_1>|^2} \]

\[ \text{for pure states} \]

Optimal measurement: \[ \rho_0 - \rho_1 \]

iff \[ \rho_0 \perp \rho_1 \]
1. Discrimination problem

What if we cannot perform the optimal measurement? In particular (here), in a composite system, if we are restricted to local quantum operations ("LOCC")?

\[
\max \Pr[\text{succ}] = \frac{1}{2} + \frac{1}{4} \|\rho - \rho_1\|_1
\]
1. Discrimination problem

$x = 0, 1$

What if we cannot perform the optimal measurement? In particular (here), in a composite system, if we are restricted to local quantum operations ("LOCC")?

$$\max \Pr[\text{success}] \leq \frac{1}{2} + \frac{1}{4} \| \rho - \rho_1 \|_1$$
Let $\rho$ be states on a composite system: $\mathcal{H} = A \otimes B$, and let A (Alice) and B (Bob) be far apart. Without a quantum channel between them, they can only perform local operations and classical communication (LOCC). [Definition/characterization somewhat painful/complex, cf. Chitambar et al., CMP 328:303-326, 2014]
2. Bipartite system - LOCC
2. Bipartite system - LOCC
2. Bipartite system - LOCC
2. Bipartite system - LOCC
2. Bipartite system - LOCC
Two pure states $\psi_0$, $\psi_1$: Distinguishable by LOCC as well as by general measurements, $||\psi_0 - \psi_1||_1$. [Walgate et al., PRL 85:4972-4975, 2000]
General (mixed) states $\rho_0, \rho_1$ in $d \otimes d$:

$\rho_x$

$O, i \rightarrow O', j$

$O, O'$: random observables (eigenbases),

$i, j$: outcomes. Distinguishing guarantee:

$\Pr\{\text{succ}\} \geq \frac{1}{2} + \frac{1}{4} \frac{1}{13} \|\rho_0 - \rho_1\|_2$
General (mixed) states $\rho, \rho'$ in $d \otimes d$:

- $\rho$: random observables (eigenbases), $i,j$: outcomes.
- Distinguishing guarantee:
  $\Pr\{\text{succ}\} \geq 1 - \frac{1}{2} \frac{1}{\sqrt{13}} ||\rho - \rho'||$

Hilbert-Schmidt (2-)norm: $||X|| = \sqrt{\text{Tr} XX^\dagger}$

[Matthews/Wehner/Aw, CMP291:813-843, 2009]
General (mixed) states $\rho_0, \rho_1$ in $d \otimes d$:

$O, i \xrightarrow{\rho_x} O', j$

$O, O'$: random observables (eigenbases),

$i, j$: outcomes. Distinguishing guarantee:

$$\Pr[\text{succ}] \geq \frac{1}{2} + \frac{1}{4.13} \frac{1}{2} \|\rho_0 - \rho_1\|_1$$

$$\geq \frac{1}{2} + \frac{1}{4.13} \frac{1}{2} \frac{1}{2} \|\rho_0 - \rho_1\|_1$$

[Matthews/Wehner/AW, CMP291:813-843, 2009]
General (mixed) states $\rho_0, \rho_1$ in $d \otimes d$:

$\rho_x$

$\lambda, i$

$\lambda$: random variable to approximate max. entangled state. Spock makes teleportation measurement (outcome $i$). Yields:

$$\Pr\{\text{succ}\} \geq \frac{1}{2} + \frac{1}{4} \cdot \frac{1}{2d} \|\rho_0 - \rho_1\|_1$$
(Anti-)Symmetric states $\rho_0, \rho_1$ in $d \otimes d$: (orthogonal!)

Best LOCC distinguishability:

$$\text{Pr\{succ\}} = \frac{1}{2} + \frac{1}{2d+2}$$

[Terhal/DiVincenzo/Leung, PRL 86:5807-5810, 2001]
3. Distinguishability norms

Abstract model: Given quantum system, $M$ class of allowed measurements. Then,

$$\sup_{M} \Pr[\text{success}] = \frac{1}{2} + \frac{1}{4} \|\rho_0 - \rho_1\|_M$$

gives rise to a norm on states.

[Matthews/Wehner/AW, CMP 291:813-843, 2009]
Abstract model: Given quantum system, M class of allowed measurements. Then,

\[ \sup_M \text{Pr}\{\text{success}\} = \frac{1}{2} + \frac{1}{4} \|\rho - \rho_1\|_M \]

gives rise to a norm on states.

Helstrom/Holevo: trace norm for \( M = \text{ALL} \)

...in general smaller, sometimes much.

[Matthews/Wehner/AW, CMP 291:813-843, 2009]
Example [Matthews/Wehner/AW, CMP 291:813-843, 2009]:

\[ M \text{ a single measurement } (M_\lambda) \text{ and its post-processings (of } \lambda). \]

\[
\|\rho_0 - \rho_1\|_M = \sum_\lambda \text{Tr} \ M_\lambda (\rho_0 - \rho_1)
\]
Example [Matthews/Wehner/AW, CMP 291:813-843, 2009]:

$M$ a single measurement ($M_{\lambda}$) and its post-processings (of $\lambda$).

$$\|\rho_0 - \rho_1\|_M = \sum_{\lambda} \|\text{TR} M_{\lambda}(\rho_0 - \rho_1)\|$$

For "generic" measurement (e.g. 4-design):

$$\frac{1}{3}\|\rho_0 - \rho_1\|_2 \leq \|\rho_0 - \rho_1\|_M \leq \|\rho_0 - \rho_1\|_2$$

$M$-data hiding: Are there states with

$$\|p_0 - p_1\|_M \ll 1, \text{ but } \|p_0 - p_1\|_1 \approx 2$$

If $M$ corresponds to class of quantum operations, with which the states can be prepared: Irreversibility of preparation and measurement.
\( M \)-data hiding: Are there states with

\[
\|p_0-p_1\|_M \ll 1 \text{, but } \|p_0-p_1\|_1 \approx 2
\]

If \( M \) corresponds to class of quantum operations, with which the states can be prepared: Irreversibility of preparation and measurement.

LOCC data hiding leads to \( \|\cdot\|_{\text{LOCC}} \)
Let $\rho_x$ be states on a composite system $\mathcal{H} = \mathcal{A} \otimes \mathcal{B}$, with the systems of Alice and Bob having dimensions $|\mathcal{A}| = |\mathcal{B}| = d$ ($x = 1 \ldots M$), such that any pair of states is LOCC-hiding, but that there is a global POVM revealing $x$ among all $M$. 

4. LOCC hiding efficiency
Let $\rho_x$ be states on a composite system $\mathcal{H} = \mathcal{A} \otimes \mathcal{B}$, with the systems of Alice and Bob having dimensions $|A| = |B| = d$ ($x = 1 \ldots M$), such that any pair of states is LOCC-hiding, but that there is a global POVM revealing $x$ among all $M$.

> How large can $M$ be in relation to $d$?
4. LOCC hiding efficiency

Known for a while [e.g. Hayden/Leung/Shor/Alw, CMP 250:371-391, 2004]: Random states in $d \otimes d$ of rank $r = d \text{ polylog}(d)$ are hiding states. Can distinguish $M = d/\text{polylog}(d)$ many of them.
4. LOCC hiding efficiency

Known for a while [e.g. Hayden/Leung/Shor/Aw, CMP 250:371-391, 2004]: Random states in $d \otimes d$ of rank $r = d \text{polylog}(d)$ are hiding states. Can distinguish $M = d / \text{polylog}(d)$ many of them.

Information $\log M \sim \log d = \text{local share.}$
Known for a while [e.g. Hayden/Leung/Shor/Aw, CMP 250:371-391, 2004]: Random states in \(d \otimes d\) of rank \(r = d \text{ polylog}(d)\) are hiding states. Can distinguish \(M = d / \text{polylog}(d)\) many of them.

Information \(\log M \sim \log d = \text{local share.}\)

Essentially optimal! [Aw, in preparation]
4. LOCC hiding efficiency

Compare secret sharing [A. Shamir, 1979; G.R. Blakley, 1979]:

Uniformly distributed message ("secret") $X \in [M]$ is associated with encryption $R_1$, $R_2$, $\ldots$, $R_n$ ("shares") of $n$ random parts.
Compare secret sharing [A. Shamir, 1979; G.R. Blakley, 1979]:

Uniformly distributed message ("secret") $X \in [M]$ is associated with encryption $R_1, R_2, ..., R_n$ ("shares") of $n$ random parts. Certain subsets $A \subseteq [n]$ of users are authorized, meaning $H(X|R_A) \approx 0$ (i.e., $X$ can be recovered as a function of the tuple $R_A = (R_i : i \in A)$).

Others are adversarial, i.e. $I(X;R_A) \approx 0$ ($X$ independent of $R_A$).
4. LOCC hiding efficiency

Compare secret sharing [A. Shamir, 1979; G.R. Blakley, 1979]: In any tight secret sharing scheme (i.e. where all subsets are either authorized or adversarial), each relevant share must be at least as large as the secret.
4. LOCC hiding efficiency

Compare secret sharing [A. Shamir, 1979; G.R. Blakley, 1979]: In any tight secret sharing scheme (i.e. where all subsets are either authorized or adversarial), each relevant share must be at least as large as the secret.

Attained for \((n,t)\) threshold schemes of \(t\) out of \(n\) parties – i.e. any set of \(t\) or more parties is authorized, all others are adversarial.
4. LOCC hiding efficiency

Compare secret sharing [A. Shamir, 1979; G.R. Blakley, 1979]: In any tight secret sharing scheme (i.e. where all subsets are either authorized or adversarial), each relevant share must be at least as large as the secret.

Attained for \((n,t)\) threshold schemes of \(t\) out of \(n\) parties — i.e. any set of \(t\) or more parties is authorized, all others are adversarial. \((2,2)\): Shannon cipher :-)

(2,2): Shannon cipher :-(
4. LOCC hiding efficiency

Compare secret sharing [A. Shamir, 1979; G.R. Blakley, 1979]: In any tight secret sharing scheme (i.e. where all subsets are either authorized or adversarial), each relevant share must be at least as large as the secret. Attained for $(n,t)$ threshold schemes of $t$ out of $n$ parties - i.e. any set of $t$ or more parties is authorized, all others are adversarial. (2,2): Shannon cipher :-)

Our LOCC hiding case also "(2,2)"...
Theorem. Assume that $\epsilon, \delta > 0$ are small enough, s.t. $\|\rho_x - \rho_y\|_{\text{LOCC}} \leq \delta$ for all $x,y,$ and $\text{Tr} \rho_x D_x \geq 1 - \epsilon$ for a POVM $(D_x)$. 
Theorem. Assume that $\epsilon, \delta > 0$ are small enough, s.t. $\|\rho_x - \rho_y\|_{\text{LOCC}} \leq \delta$ for all $x, y,$ and $\text{Tr} \rho_x D_x \geq 1 - \epsilon$ for a POVM $(D_x)$. Then, exist $\mu, C > 0$ (dep. only on $\epsilon, \delta$) with

$$\log(M-1) \leq H_{\max}(A|B)_\Omega + C \leq \log d + O(1),$$

w.r.t. average state $\Omega$ of the $\rho_x$. 
Theorem. Assume that $\varepsilon, \delta > 0$ are small enough, s.t. $\|\rho_x - \rho_y\|_{\text{LOCC}} \leq \delta$ for all $x, y$, and $\text{Tr} \rho_x D_x \geq 1 - \varepsilon$ for a POVM $(D_x)$.

Then, exist $\mu, C > 0$ (dep. only on $\varepsilon, \delta$) with

$$\log(M-1) \leq \log_{\text{max}}(A|B)_\Omega + C \leq \log d + O(1),$$

w.r.t. average state $\Omega$ of the $\rho_x$.

(Smooth) max-entropy

[cf. Renner, PhD 2005; Tomamichel, PhD 2012]
Theorem. Assume that $\varepsilon, \delta > 0$ are small enough, s.t. $\|\rho_x - \rho_y\|_{\text{LOCC}} \leq \delta$ for all $x, y$, and $\text{Tr}_x D_x \geq 1 - \varepsilon$ for a POVM $(D_x)$. Then, exist $\mu, C > 0$ (dep. only on $\varepsilon, \delta$) with

$$\log(M-1) \leq H^\mu_{\text{max}}(A|B)_\Omega + C \leq \log d + O(1),$$

w.r.t. average state $\Omega$ of the $\rho_x$.

(Smooth) max-entropy

[cf. Renner, PhD 2005; Tomamichel, PhD 2012]

...Proof uses the full power of the min-1 max-entropy calculus
Proof uses the full power of the min-/max-entropy calculus.

Recall definitions: For a state $\rho^{AB}$ with purification $\psi^{ABC}$, let

$$H_{\text{min}}(A|B)_\rho := -\log \min \text{ Tr } \sigma \text{ s.t. } \rho \leq I \otimes \sigma,$$

$$H_{\text{max}}(A|B)_\rho := -H_{\text{min}}(A|C)_\rho$$

$$= \log \max F(\rho, I \otimes \sigma) \text{ s.t. } \sigma \text{ state}$$

[Tomamichel, PhD thesis; arXiv:1203.2142]
Proof uses the full power of the min-/max-entropy calculus.

Recall definitions: For a state $\rho^{AB}$ with purification $\psi^{ABC}$, let

$$H_{\text{min}}(A|B) : = -\text{log} \min Tr \sigma \text{ s.t. } \rho \leq I \otimes \sigma,$$

$$H_{\text{max}}(A|B) : = -H_{\text{min}}(A|C),$$

$$= \text{log} \max F(\rho, I \otimes \sigma)^2 \text{ s.t. } \sigma \text{ state}$$

Smoothed versions $H^{\epsilon}_{\text{min/max}}(A|B)$ by optimizing over states $\rho'$ $\epsilon$-close to $\rho$...

[Tomamichel, PhD thesis; arXiv:1203.2142]
Proof uses the full power of the min-/max-entropy calculus: chain rules!

Recall entropy chain rule identity

$$S(ABIC) = S(AIC) + S(BIAC).$$
Proof uses the full power of the min-/max-entropy calculus: chain rules!

Recall entropy chain rule identity
\[ S(ABIC) = S(AIC) + S(BIAC). \] Turns into inequalities for min-/max-entropies:

\[
\begin{align*}
H_{\min}^{\varepsilon+2\varepsilon'+\varepsilon''}(AB|C)_\rho &\geq H_{\min}^{\varepsilon'}(AB|C)_\rho + H_{\min}^{\varepsilon''}(B|C)_\rho - \log \frac{2}{\varepsilon^2}, \\
H_{\max}^{\varepsilon+\varepsilon'+2\varepsilon''}(AB|C)_\rho &\leq H_{\max}^{\varepsilon'}(A|BC)_\rho + H_{\max}^{\varepsilon''}(B|C)_\rho + \log \frac{2}{\varepsilon^2}, \\
H_{\min}^{\varepsilon+3\varepsilon'+2\varepsilon''}(A|BC)_\rho &\geq H_{\min}^{\varepsilon'}(AB|C)_\rho - H_{\max}^{\varepsilon''}(B|C)_\rho - 2 \log \frac{2}{\varepsilon^2}, \\
H_{\max}^{\varepsilon+\varepsilon'+2\varepsilon''}(A|BC)_\rho &\leq H_{\max}^{\varepsilon'}(A|BC)_\rho - H_{\min}^{\varepsilon''}(B|C)_\rho + 3 \log \frac{2}{\varepsilon^2}, \\
H_{\min}^{2\varepsilon+\varepsilon'+2\varepsilon''}(B|C)_\rho &\geq H_{\min}^{\varepsilon'}(AB|C)_\rho - H_{\max}^{\varepsilon''}(A|BC)_\rho - 3 \log \frac{2}{\varepsilon^2}, \\
H_{\max}^{\varepsilon+3\varepsilon'+2\varepsilon''}(B|C)_\rho &\leq H_{\max}^{\varepsilon'}(A|BC)_\rho - H_{\min}^{\varepsilon''}(A|BC)_\rho + 2 \log \frac{2}{\varepsilon^2}.
\end{align*}
\]

[A. Vitanov, MSc thesis 2011, cf. 1203.21442]
Proof (sketch):

Define $\Omega^{XAB} = \frac{1}{M} \sum_x |x><x| \otimes \rho^{AB}_x$. Then:

$$\log(M-1) \leq \min \sqrt{\delta}(X|IB)$$

Local shares give little information?
Proof (sketch):

Define $\Omega^{XAB} = \frac{1}{M} \sum_{x} |x><x|^X \otimes \rho_{X}^{AB}$. Then:

$$\log(M-1) \leq H_{\text{min}}^{\sqrt{\delta}}(XIB)$$

$$\leq H_{\text{min}}^{\sqrt{\delta}}(XIB) + H_{\text{max}}^{Y}(AIBX) + O(1)$$

Local shares give little information.

Otherwise "merging attack" breaks scheme.
Proof (sketch):

Define $\Omega_{XAB} = \frac{1}{M} \sum_x |x><x|^X \otimes \rho_{X}^{AB}$. Then:

$$\log(M-1) \leq H_{\min}^{\sqrt{\delta}}(X|B)$$

$$\leq H_{\min}^{\sqrt{\delta}}(X|B) + H_{\max}^{\gamma}(A|BX) + O(1)$$

$$\leq H_{\max}^{\eta}(AX|B) + O(1)$$

Local shares give little information.

Otherwise "merging attack" breaks scheme.

Local shares give little information.

One of the chain rules.
Proof (sketch):

Define $\Omega^{XAB} = \frac{1}{M} \sum_{x} |x><x| \otimes \rho_{X}^{AB}$. Then:

$$\log(M-1) \leq H_{\min}^{\sqrt{\delta}}(X|B)$$

$$\leq H_{\min}^{\sqrt{\delta}}(X|B) + H_{\max}^{\gamma}(A|BX) + O(1)$$

$$\leq H_{\max}^{\eta}(AX|B) + O(1)$$

$$\leq H_{\max}^{\mu}(A|B) + H_{\max}^{\lambda}(X|AB) + O(1)$$

- Local shares give little information.
- Otherwise “merging attack” breaks scheme.
- One of the chain rules.
- Another chain rule.
Proof (sketch):

Define \( \Omega_{XAB}^{X} = \frac{1}{M} \sum_{x} |x><x|^{X} \otimes \rho_{XAB}^{AB} \). Then:

\[
\log(M-1) \leq H_{min}^{\sqrt{\delta}}(X|B) \\
\leq H_{\min}^{\sqrt{\delta}}(X|B) + H_{\max}^{\gamma}(A|BX) + O(1) \\
\leq H_{\max}^{\eta}(AX|B) + O(1) \\
\leq H_{\max}^{\mu}(A|B) + H_{\max}^{\lambda}(X|AB) + O(1) \\
\leq H_{\max}^{\mu}(A|B) + O(1)
\]

\( \{ \text{Local shares give little information}\} \)
\( \{ \text{Otherwise "merging attack" breaks scheme}\} \)
\( \{ \text{One of the chain rules}\} \)
\( \{ \text{Another chain rule}\} \)
\( \{ \text{Decodability}\} \)

Q.E.D.
Compare secret sharing [A. Shamir, 1979; G.R. Blakley, 1979]: In any tight secret sharing scheme (i.e. where all subsets are either authorized or adversarial), each relevant share must be at least as large as the secret.

Corollary 1: In any tight LOCC data hiding scheme, each relevant share must be at least as large as the secret (plus a constant). Attained for "(n,t)" scheme.

[AW, in prep.; Hayden/Leung/Smith, PRA 71:062339, 2005]
LOCC data hiding scheme: Authorized/adversarial is a property of partitions of $[n]$, where within each segment the parties can exchange quantum messages, but between segments only classical information is allowed.

Corollary 1: In any tight LOCC data hiding scheme, each relevant share must be at least as large as the secret (plus a constant). Attained for "$(n,t)$" scheme.

[AW, in prep.; Hayden/Leung/Smith, PRA 71:062339, 2005]
A quantum channel $N:D \rightarrow A \otimes B$ models the states $N(\rho)$ that a dealer $D$ (Dr Zarkov) can distribute between $A$ (Spock) and $B$ (Strangelove). Data hiding capacity [Lupo/Wilde/Lloyd, 1507.06038]:

$$\kappa(N) := \text{largest rate of hiding information via } N \otimes^n (n \rightarrow \infty).$$

Corollary 2: For every channel $N$,

$$\kappa(N) \leq \max_{\rho} \min_{\omega} \{S(A|B)_\omega, S(B|A)_\omega\},$$

where the entropies are w.r.t. $\omega = N(\rho)$.

[AW, in preparation]
5. Discussion: questions

- Can also do multi-party LOCC hiding
  Hayden/Leung/Smith, PRA 71:062339, 2005].
- Open however: optimal performance for all LOCC access structures (=which partitions can/cannot retrieve secret)?
  Bounds in [Lancien/AW, CMP 323(2): 555-573, 2013], but rather incomplete...
- Other bounds on data hiding capacity?