Optimal Hiding of Quantum Information

Francesco Buscemi[1]

18th Asian Quantum Information Conference (AQIS18)
Nagoya University, 12 September 2018

[1]Dept. of Mathematical Informatics, Nagoya University, buscemi@i.nagoya-u.ac.jp

worried about data remanence?

What Quantum Theory Tells Us

- the input (information carrier) is a quantum system Q
- the hiding process is a CPTP map $\mathcal{E} : Q \to Q'$
- the eavesdropper holds the environment E purifying ($\to$ Appendix) the hiding process $\mathcal{E}$

Perfect Hiding

Ideal objective: the initial information, after the erasure process, is neither in Q' nor in E.

Question: is this possible?

No, It's Not Possible

No-Hiding Theorem (Braunstein, Pati, 2007)

- input: an unknown quantum state $|\psi\rangle \in \mathcal{H}_Q$
- assumption: perfect erasure, i.e., the output $\mathcal{E}(|\psi\rangle\langle\psi|)$ does not depend on $|\psi\rangle$
- conclusion: no-hiding, i.e., the initial state $|\psi\rangle$ can be found intact in the environment E

Interpretation. Perfect hiding of quantum information is impossible, that is, quantum information is preserved: it can only be moved to the environment (i.e., handed over to the eavesdropper)

Yes, It Is Possible

- **input**: an unknown state $|\psi^i\rangle$ chosen from a set of orthogonal states
- **hiding process**: measurement on the Fourier transform basis $|\tilde{\psi}^j\rangle$, i.e., $|\langle\tilde{\psi}^j|\psi^i\rangle|^2 = \frac{1}{d}$
- the corresponding **Stinespring-Kraus dilation** is given by

$$|\psi^i_Q\rangle \longmapsto \underbrace{\sum_j |\tilde{\psi}^j_{Q'}\rangle|\tilde{\psi}^j_E\rangle\langle\tilde{\psi}^j_Q|}_{\text{isometry } V_{Q\to Q'E}}\,|\psi^i_Q\rangle = \underbrace{|\mathcal{B}^i_{Q'E}\rangle}_{\text{max. ent.}}\,,$$

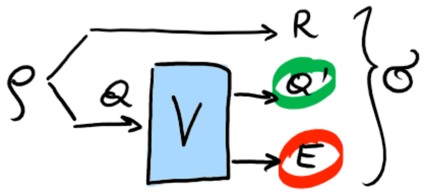
- perfect hiding has been achieved in this case

Motivation of This Talk

- whether perfect hiding can be achieved or not, depends on the "form" of the set of input states used to encode information
- tantalizing idea: quantum information (the first example) cannot be hidden, while classical information (the second example) can; to what extent is this true?
- problem: to find a framework able to **handle general sets of input states**

Private Quantum Decoupling

The Extended Setting



- **input**: instead of a *set* of states of Q, we consider *one* bipartite state ρ_{RQ}, shared with a reference R
- **hiding process**: an isometry V splitting the input system Q into output Q' and junk E
- **ideal goal (perfect hiding)**: $\sigma_{RQ'} = \sigma_R \otimes \sigma_{Q'}$ (perfect decoupling) and $\sigma_{RE} = \sigma_R \otimes \sigma_E$ (perfect privacy)

Relation with The Conventional Setting

- original question is single-partite: are all states ρ_Q in set S hidable?
- but is any set S "reasonable"?
- **preparability assumption**: there must exist an input system X and a CP (maybe not TP) map $\mathcal{S} : X \to Q$ such that S is the image of $\mathcal{S}$
- **fact**: a set is preparable *if and only if* there exists a bipartite state ρ_{RQ} such that S is recovered by steering from R:

$$\forall \rho_Q \in \mathsf{S},\ \exists \pi_R \geq 0 : \rho_Q = \frac{\mathrm{Tr}_R[\rho_{RQ}\ (\pi_R \otimes I_Q)]}{\mathrm{Tr}[\rho_{RQ}\ (\pi_R \otimes I_Q)]}$$

- hence, from now on, instead of considering a set of possible input states, we consider a single bipartite state

The Quantum Mutual Information (QMI)

- define $I(X;Y) \overset{\text{def}}{=} H(X) + H(Y) - H(XY)$
- $0 \leq I(X;Y) \leq 2H(X)$
- $I(X;Y) \geq \frac{1}{2\ln 2} \|\rho_{XY} - \rho_X \otimes \rho_Y\|_1^2$

Ideal Hiding (Reformulation)

Given an input bipartite state ρ_{RQ}, find an isometry V, taking Q into $Q'E$, such that

$$\underbrace{I(R;Q') = 0}_{\text{decoupling}} \quad \text{and} \quad \underbrace{I(R;E) = 0}_{\text{privacy}} .$$

Reformulation of No-Hiding Using QMI

- consider an initial bipartite *pure* state $|\Psi_{RQ}\rangle$
- *any* isometry on Q will output a tripartite pure state $|\tilde{\Psi}_{RQ'E}\rangle$
- in this case, the balance relation identically holds

$$\underbrace{I(R;Q')}_{\text{decoupling}} + \underbrace{I(R;E)}_{\text{privacy}} = 2H(R)$$

No-Hiding (reform.): in the pure state case, all correlations are intrinsic, i.e., decoupling and privacy are mutually incompatible requirements.

Remark. In particular, the original Braunstein-Pati theorem is recovered for $|\Psi_{RQ}\rangle$ maximally entangled.

Optimal Hiding

Since ideal hiding is in general impossible, we consider a relaxation of the problem:

Definition (Symmetric Case)

Given an input bipartite state ρ_{RQ}, its **intrinsic** (or "non-hidable") correlations are defined by

$$\xi(\rho_{RQ}) \stackrel{\text{def}}{=} \inf_{V:Q\to Q'E} \left\{ \frac{I(R;Q') + I(R;E)}{2} \right\}$$

Remark. Perfect hiding for ρ_{RQ} is possible if and only if $\xi(\rho_{RQ}) = 0$.

Remark. One can also consider $\xi^{\epsilon}(\rho_{RQ}) \stackrel{\text{def}}{=} \inf_{V:Q\to Q'E} \{I(R;Q') : I(R;E) \leq \epsilon\}$ or $\xi'(\rho_{RQ}) \stackrel{\text{def}}{=} \inf_{V:Q\to Q'E} \{I(R;Q') : I(R;E) \leq I(R;Q')\}$.

General Bound

Theorem

For any ρ_{RQ}, we have

$$I_c(Q\rangle R) \leq \xi(\rho_{RQ}) \leq \frac{1}{2} I(R;Q) \; ,$$

where $I_c(Q\rangle R) \stackrel{\text{def}}{=} H(R) - H(RQ)$ is the *coherent information*.

- for pure states, $\xi(\rho_{RQ})$ equals the **entropy of entanglement** $H(R)$; in general, however, *it is not an entanglement measure*
- it is nonetheless a good **entanglement parameter**, in the sense that

$$\xi(\rho_{RQ}) \to H(Q) \iff I_c(Q\rangle R) \to H(Q)$$

- it satisfies **monogamy**, that is, for any tripartite pure state $|\Psi_{SRQ}\rangle$, $\xi(\rho_{SR}) + \xi(\rho_{RQ}) \leq H(R)$

More About Monogamy

- given a tripartite density matrix σ_{xyz}, its **quantum conditional mutual information (QCMI)** is defined as $I(x;y|z) = H(x|z) + H(y|z) - H(xy|z) = H(x|z) - H(x|yz)$
- let w be the purifying system for xyz; then $-H(x|yz) = H(x|w)$
- this implies that $2H(x) - I(x;y|z) = I(x;z) + I(x;w)$
- **in our case**: $\rho_{RQ} \xrightarrow{\text{purify}} |\Psi_{SRQ}\rangle \xrightarrow{V:Q\to Q'E} |\tilde{\Psi}_{SRQ'E}\rangle$
- by substituting $(w,x,y,z) \to (E,R,S,Q')$ we obtain

$$H(R) - \frac{1}{2}I(R;S|Q') = \left\{ \frac{I(R;Q') + I(R;E)}{2} \right\} ,$$

which holds for any bipartite splitting.

Relations with Entanglement

From the identity $\left\{\frac{I(R;Q')+I(R;E)}{2}\right\} = H(R) - \frac{1}{2}I(R;S|Q')$, we have that

- $$\underbrace{\inf_{V:Q\to Q'E}\left\{\frac{I(R;Q')+I(R;E)}{2}\right\}}_{\text{intrinsic correlations } \xi(\rho_{RQ})} = H(R) - \underbrace{\sup_{V:Q\to Q'E}\frac{1}{2}I(R;S|Q')}_{\text{``puffed'' entanglement } \overline{E_{\mathrm{sq}}}(\rho_{RS})}\ ;$$
- $$\underbrace{\sup_{V:Q\to Q'E}\left\{\frac{I(R;Q')+I(R;E)}{2}\right\}}_{\text{``extrinsic'' correlations } \overline{\xi}(\rho_{RQ})} = H(R) - \underbrace{\inf_{V:Q\to Q'E}\frac{1}{2}I(R;S|Q')}_{\text{squashed entanglement } E_{\mathrm{sq}}(\rho_{RS})}\ .$$

Theorem. For any tripartite pure state $|\Psi_{SRQ}\rangle$ the following hold:

- $\xi(\rho_{RQ}) + \overline{E_{\mathrm{sq}}}(\rho_{RS}) = H(R)$ and
- $\overline{\xi}(\rho_{RQ}) + E_{\mathrm{sq}}(\rho_{RS}) = H(R)$.

The Asymptotic Scenario

As it is customary in information theory, we consider the regularized quantity:

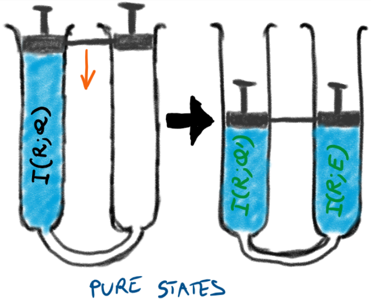
$$\begin{aligned}\xi^{\infty}(\rho_{RQ}) &\stackrel{\text{def}}{=} \lim_{n\to\infty} \frac{1}{n}\xi(\rho_{RQ}^{\otimes n}) \\ &= \lim_{n\to\infty} \frac{1}{n} \inf_{V:Q^{\otimes n}\to Q'_n E_n} \left\{ \frac{I(R^{\otimes n};Q'_n) + I(R^{\otimes n};E_n)}{2} \right\}\end{aligned}$$

Remark. The splitting isometry is in general entangled, that is, $Q^{\otimes n} \to Q'_n E_n \neq (Q'E)^{\otimes n}$.

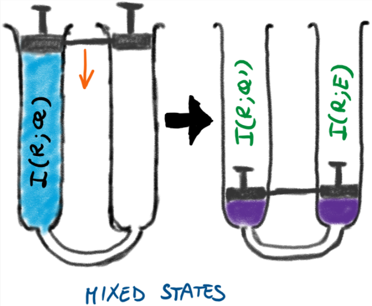
Theorem (Asymptotic Hiding)

For any initial state ρ_{RQ}, $\xi^{\infty}(\rho_{RQ}) = 2I_c(Q\rangle R)$.

An Attempt at Visualizing



$$I(R;Q') + I(R;E) = I(R;Q)$$



$$I(R;Q') + I(R;E) = 2I_c(Q\rangle R)$$

Hence:

- **intrinsic (non-hidable) correlations**: $2I_c(Q\rangle R) \ll I(R;Q)$
- **pure-state correlations are all intrinsic**: $2I_c(Q\rangle R) = I(R;Q)$
- **separable-state correlations are all perfectly hidable**: $2I_c(Q\rangle R) = 0$

Side Remark: The Role of Randomness

With free private randomness, private quantum decoupling becomes trivial.

- **private randomness**: a max. mixed state $\omega_P = \frac{1}{d_P} I_P$ that we can trust to be independent of Eve
- **hiding process**: an isometry $V : QP \to Q'E$
- **output state**: $\sigma_{RQ'E} = (I_R \otimes V_{QP})(\rho_{RQ} \otimes \omega_P)(I_R \otimes V_{QP}^{\dagger})$

Example

Since $\frac{1}{4}\sum_i \sigma_i \rho \sigma_i = \frac{1}{2} I_2$ for any initial qubit state ρ, the state $\omega_P = \frac{1}{4} I_4$ and the isometry $V : QP \to Q'E$, given by $V = \sum_i \sigma_i^{Q \to Q'} \otimes |i_E\rangle\langle i_P|$, are enough to perfectly hide any two-qubit correlation.

Summary

- pure-state correlations cannot be hidden: $I(R;Q')+I(R;E)=I(R;Q)$
- however, in general: $\xi(\rho_{RQ})\stackrel{\text{def}}{=}\inf_{Q\to Q'E}\frac{1}{2}\{I(R;Q')+I(R;E)\}\ll I(R;Q)$
- monogamy 1: intrinsic correlations are dual to “puffed” entanglement, i.e., $\xi(\rho_{RQ})+\overline{E_{\text{sq}}}(\rho_{RS})=H(R)$, for all pure $|\Psi_{SRQ}\rangle$
- monogamy 2: squashed entanglement is dual to “extrinsic” correlations, i.e., $\overline{\xi}(\rho_{RQ})+E_{\text{sq}}(\rho_{RS})=H(R)$, for all pure $|\Psi_{SRQ}\rangle$
- private randomness enables perfect hiding
- connections with other protocols in QIT? e.g., randomness extraction, private key distribution, etc.
- connections with foundations? e.g., Landauer’s principle, uncertainty relations, quantumness of correlations, black holes information, etc.

Thank you

Appendix: The Stinespring-Kraus Dilation

- consider an input/output quantum process (CPTP map) $\mathcal{E}$, mapping density matrices on $\mathcal{H}_Q$ to density matrices on $\mathcal{H}_{Q'}$
- **Kraus operator-sum representation**: $\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$
- **Kraus-Stinespring dilation**: each CPTP map $\mathcal{E}$ can be written as $\mathcal{E}(\rho) = \mathrm{Tr}_E[V \rho V^\dagger]$ (Stinespring) or $\mathcal{E}(\rho) = \mathrm{Tr}_E[U(\rho_Q \otimes |0\rangle\langle 0|_{E_0})U^\dagger]$ (Kraus)
- in quantum crypto-analyses, the subsystem E is the eavesdropper's