

Fidelity of recovery, geometric squashed entanglement, and measurement recoverability

Mark M. Wilde

*Hearne Institute for Theoretical Physics
Department of Physics and Astronomy
Center for Computation and Technology
Louisiana State University, Baton Rouge*

Joint work with **Kaushik Seshadreesan**

arXiv:1410.1441



Quantifying Correlation

- Given a bipartite density matrix ρ_{AB} , we can quantify the correlations between Alice and Bob using the quantum mutual information:

$$I(A;B) = H(A) + H(B) - H(AB)$$

where $H(S)$ is the von Neumann entropy of a state on system S (use natural logarithm).

- Advantage: simple to compute and has an operational interpretation as the amount of local noise needed to destroy all correlations, so that

$$\rho_{AB} \rightarrow \rho_A \times \rho_B$$

Quantum mutual information

- Quantum mutual information is about closeness to a product state
- Define fidelity between two states as

$$F(\rho, \sigma) \equiv \left\| \sqrt{\rho} \sqrt{\sigma} \right\|_1^2$$

- F is between 0 and 1. F near 0 means states are nearly orthogonal and F near 1 means they are nearly indistinguishable
- It is known from Pinsker inequality and continuity of entropy that

$$I(A; B) \approx \varepsilon \Leftrightarrow F(\rho_{AB}, \rho_A \otimes \rho_B) \approx 1 - \varepsilon$$

(however, read these theorems carefully for details)

Fidelity to product states

- The surprisal of the fidelity to product states can act as a proxy for mutual information:

$$-\log F(\rho_{AB}, \rho_A \otimes \rho_B)$$

- Can even optimize over the “closest” product state:

$$-\log \sup_{\sigma_A, \tau_B} F(\rho_{AB}, \sigma_A \otimes \tau_B)$$

Quantum mutual information

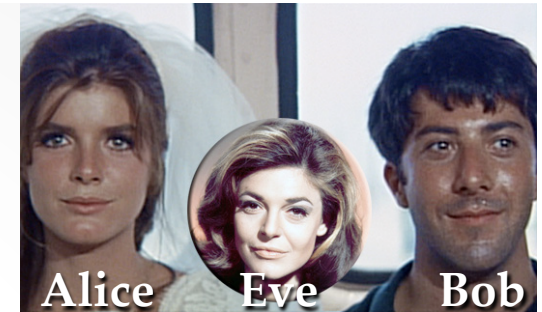
- Disadvantage: neglects third parties, which is particularly relevant for quantum cryptography
- Example:

$$\rho_{AB} = \frac{1}{d} \sum_i |i\rangle\langle i|_A \otimes |i\rangle\langle i|_B$$

- State has $\log(d)$ “nats” of mutual information, but...



What about Eve?



- Alice and Bob's state could be the reduction of a larger state in which Eve has a system:

$$\rho_{ABE} = \frac{1}{d} \sum_i |i\rangle\langle i|_A \otimes |i\rangle\langle i|_B \otimes |i\rangle\langle i|_E$$

- So even though Alice and Bob are maximally correlated, they have no privacy from Eve!
- Situation becomes even more complicated for a fully quantum Eve!



Conditional mutual information

- **Conditional mutual information** quantifies how correlated Alice and Bob are from Eve's perspective:

$$I(A;B | E) = H(A | E) + H(B | E) - H(AB | E) \geq 0 \text{ (SSA)}$$

where $H(F | G) = H(FG) - H(G)$

- Intuition: If $I(A;B | E)$ is high, then it is not possible for Eve to recover either the A or B system by acting on hers alone... conversely, if $I(A;B | E)$ is low, then Eve can recover (see Fawzi-Renner 1410.0664)
- This is the basis for the **squashed entanglement measure**
(if correlations between Alice and Bob are classical, then Eve can recover them)

Back to Alice's concern



Alice says next:

Bob, if you were to lose me, then I fear that Eve would be able to regain with you everything that we shared together...

To which Bob replies:

If you're so concerned about that, then you should have entangled me...

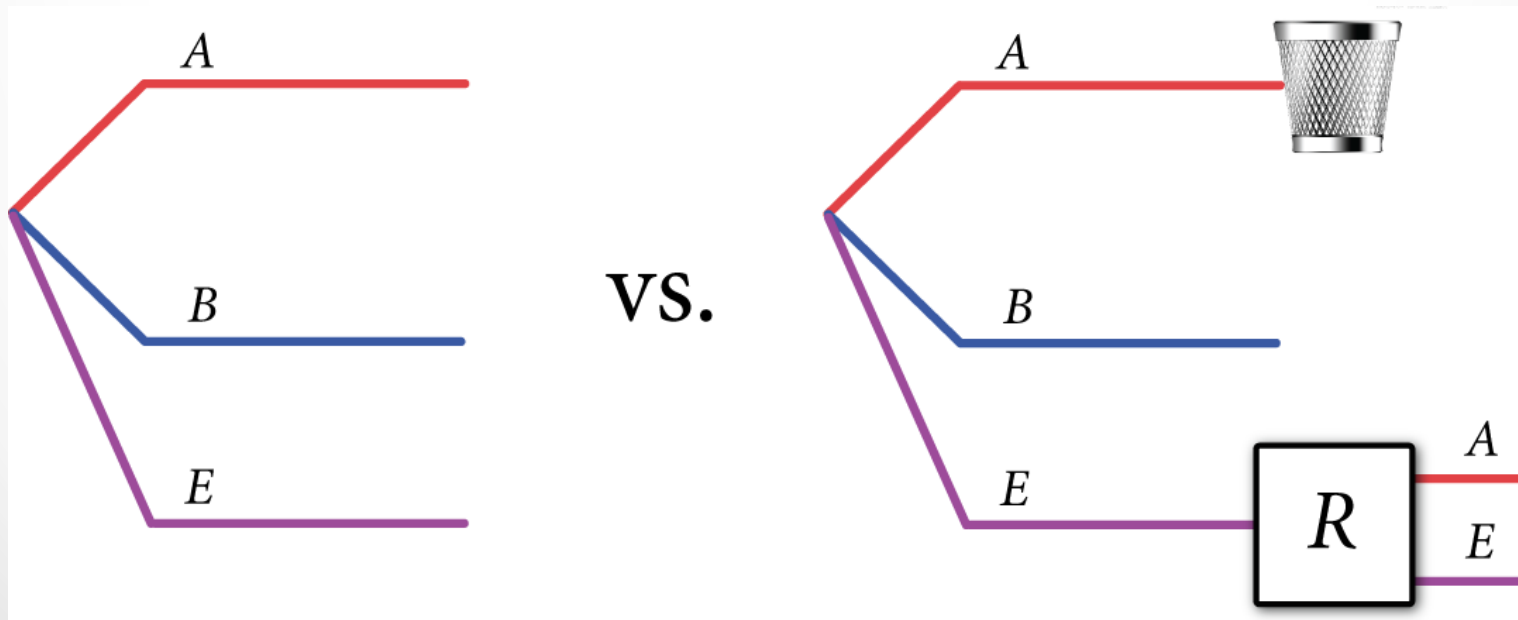
Furthermore, I actually have the same concern about you and Eve...

Fidelity of recovery

- Quantify how well Eve can recover a “lost Alice” with the fidelity of recovery:

$$F(A; B|E) \equiv \sup_{\mathcal{R}_{E \rightarrow AE}} F(\rho_{ABE}, \mathcal{R}_{E \rightarrow AE}(\rho_{BE}))$$

- In a picture,



Surprisal of FoR

- Negative logarithm of a probability is called the “surprisal”. So we get the surprisal of the FoR:

$$I_F(A; B|E) \equiv -\log F(A; B|E)$$

- One of our main contributions is to show that I_F “follows” the conditional mutual information, in the sense that it obeys many of the same properties...

Comparison – $I(A;B|E)$ vs. $I_F(A;B|E)$

- Both are **non-negative** and equal to zero if and only if the state is a **short quantum Markov chain**
- $I(A;B|E) \geq I_F(A;B|E)$ (Fawzi-Renner)
- Both are **monotone non-increasing** under quantum operations acting on A or B alone
- Both obey **dimension bound** $\leq 2 \log |A|$ for quantum A and $\leq \log |A|$ for classical A
- **Additive** on tensor-product states (Berta & Tomamichel)
- Chain rule?
- Both obey **duality**: for four-party pure state on ABEF,
 $I(A;B|E) = I(A;B|F)$



Eve

Frideborg

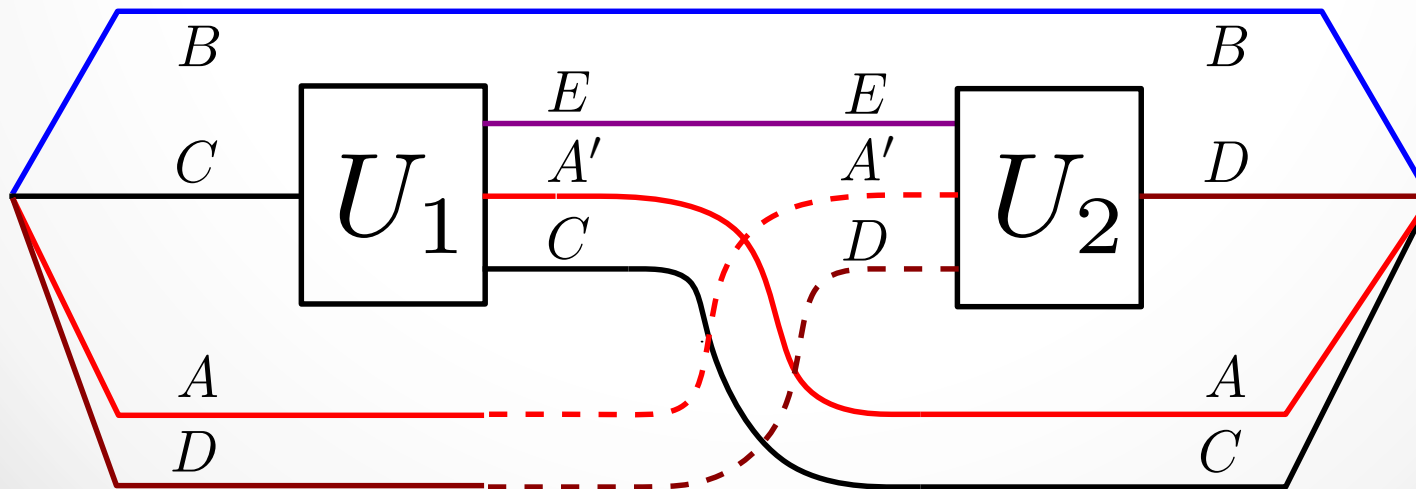


Proof of duality

- Uhlmann's theorem is a powerful tool in quantum information theory:

$$F(\rho_S, \sigma_S) = \sup_{U_R} |\langle \psi_{RS}^\rho | U_R \otimes I_S | \psi_{RS}^\sigma \rangle|^2$$

- Duality of fidelity of recovery $I_F(A;B | C) = I_F(A;B | D)$



Squashed entanglement

- Squashed entanglement of bipartite state ρ_{AB} defined as

$$E_{\text{sq}}(A; B)_{\rho} \equiv \frac{1}{2} \inf_{\rho_{ABE}} \{I(A; B|E)_{\rho} : \text{Tr}_E\{\rho_{ABE}\} = \rho_{AB}\}$$

- Eve makes her best attempt to “squash down” the correlations between Alice and Bob
- Relevant to QKD by giving upper bounds on key distillation rates

Geometric squashed entanglement

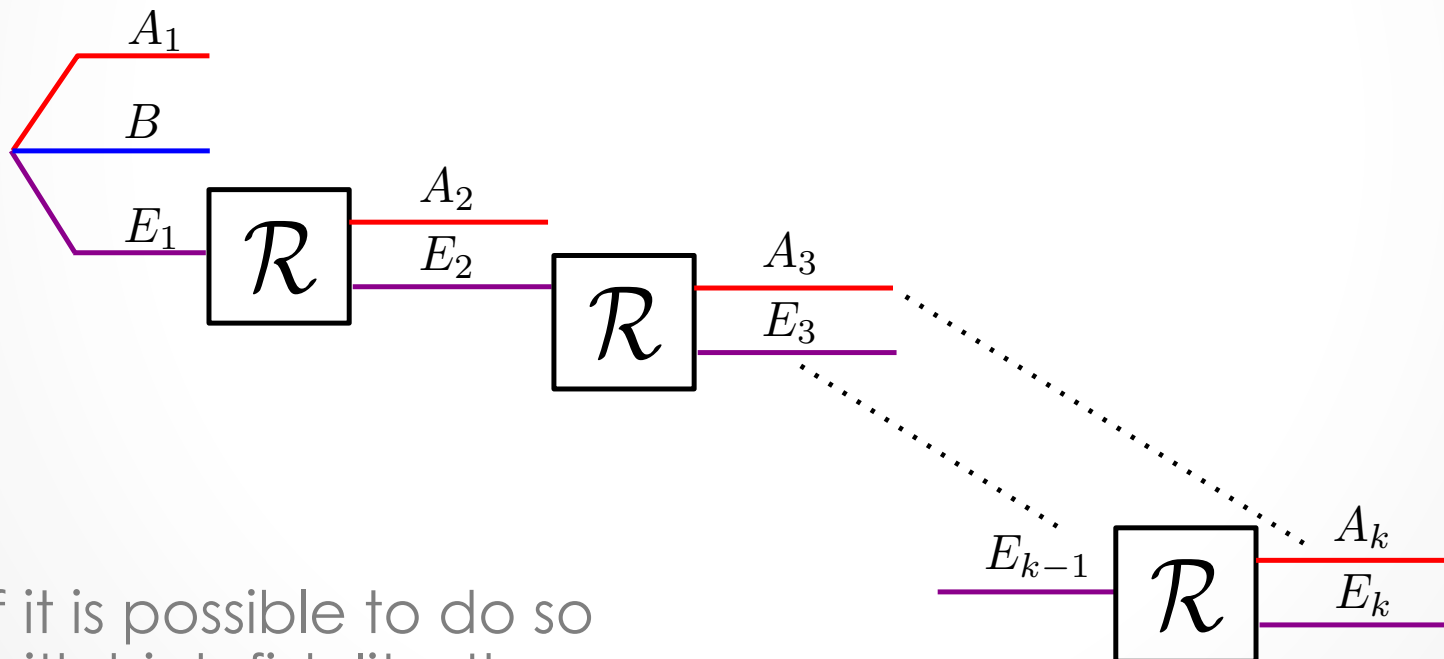
- Define by using surprisal of fidelity of recovery:

$$E_{\text{sq}}^F(A; B)_\rho \equiv \frac{1}{2} \inf_{\rho_{ABE}} \{I_F(A; B|E)_\rho : \text{Tr}_E\{\rho_{ABE}\} = \rho_{AB}\}$$

- Obeys many of the same properties as squashed entanglement
- Faithful, i.e., non-negative and zero if and only if state is separable
- Monotone under LOCC
- Reduces to geometric(-like) measure for pure states
- Normalized on maximally entangled states
- Subadditive, Continuous
- Additive? Monogamous? Asymptotically continuous?

Proof of faithfulness

- Use recovery idea from Winter and Li, to extract many copies of A from E alone which gives a k -extension of original state:

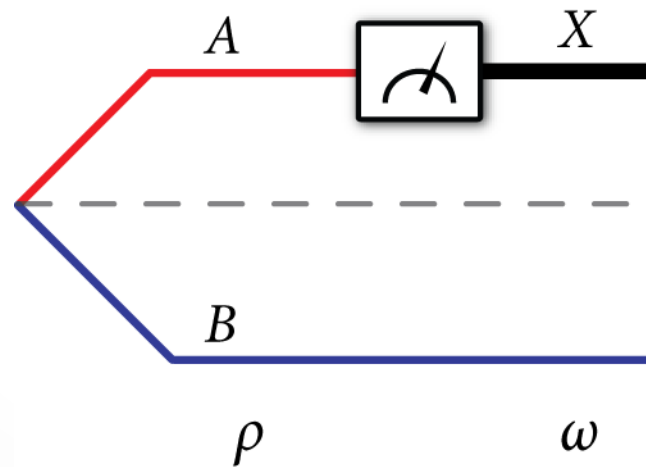


- If it is possible to do so with high fidelity, then Alice-Bob state must not be very entangled

Quantum discord

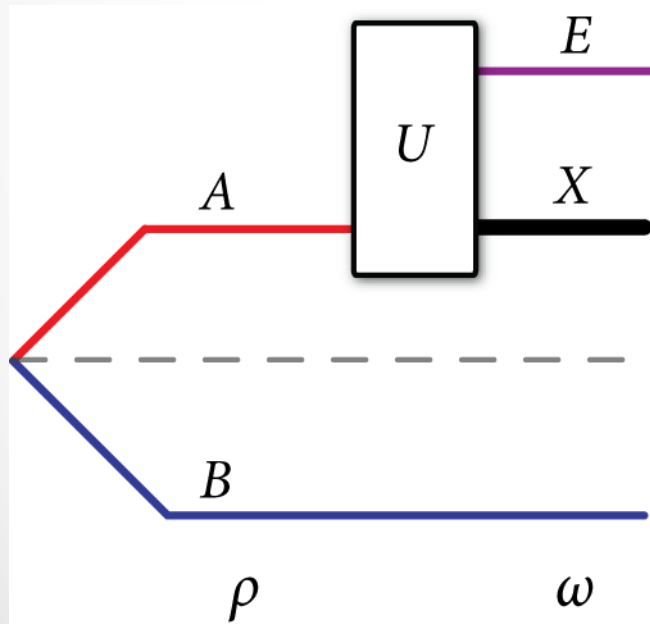
- Quantum discord as the gap between mutual information and “classical correlation” of ρ_{AB} :

$$D(\overline{A}; B)_\rho \equiv I(A; B)_\rho - I(X; B)_\omega$$



Quantum discord as conditional mutual information

- A measurement is a quantum channel, and thus can be represented as a unitary on a larger system including an environment:



$$\begin{aligned} I(A; B)_\rho - I(X; B)_\omega \\ &= I(EX; B)_\omega - I(X; B)_\omega \\ &= I(E; B|X)_\omega \end{aligned}$$

So discord is about recovering a
“lost environment” of a measurement

Surprisal of measurement recoverability

- Define a discord-like quantity by replacing I with I_F :

$$D_F(\bar{A}; B)_\rho = I_F(E; B|X)_\omega$$

- After some steps, we find that this is the same as

$$D_F(\bar{A}; B)_\rho = -\log \sup_{\mathcal{E}_A} F(\rho_{AB}, \mathcal{E}_A(\rho_{AB}))$$

where the optimization is over entanglement breaking channels

- Idea is that if state is not perturbed by some EB channel, then it is not very quantum

Lower bound on discord

- Interesting new lower bound on discord:

$$D(\overline{A}; B)_\rho \geq D_F(\overline{A}; B)_\rho$$

- So discord nearly equal to zero if and only if state is approximately unchanged after performing some entanglement breaking channel
- Suggests that discord-like measures should be based on this principle, rather than closeness to classical-quantum states

Properties of surprisal of measurement recoverability

- Non-negative and equal to zero if and only if state is classical-quantum
- Invariant under local unitaries
- Dimension bound: $D_F \leq \log |A|$
- Equal to $\log |A|$ for maximally entangled state
- Monotone under local operations on the unmeasured system
- Continuous
- Hierarchy of efficiently computable, discord-like measures that approximate it (Piani arXiv:1501.06855)

Conclusions

- Fidelity of recovery introduced to quantify an approximate quantum Markov chain
- Similar to conditional mutual information and is a meaningful lower bound for it
- Can derive entanglement and discord-like measures from it
- Can extend to the multipartite case, but more work to be done here
- Is there a “pretty good recovery” (transpose channel) which does nearly as well as optimal?
- Applications to topologically ordered systems, communication complexity, measure of Markovianity (go to next slide)

I'M SURE YOU'VE HEARD ALL ABOUT THIS SORDID AFFAIR IN THOSE GOSSIPY CRYPTOGRAPHIC PROTOCOL SPECS WITH THOSE BUSYBODIES SCHNEIER AND RIVEST, ALWAYS TAKING ALICE'S SIDE, ALWAYS LABELING ME THE ATTACKER.



YES, IT'S TRUE. I BROKE BOB'S PRIVATE KEY AND EXTRACTED THE TEXT OF HER MESSAGES. BUT DOES ANYONE REALIZE HOW MUCH IT HURT?



HE SAID IT WAS NOTHING, BUT EVERYTHING FROM THE PUBLIC-KEY AUTHENTICATED SIGNATURES ON THE FILES TO THE LIPSTICK HEART SMEARED ON THE DISK SCREAMED "ALICE."



I DIDN'T WANT TO BELIEVE. OF COURSE ON SOME LEVEL I REALIZED IT WAS A KNOWN-PLAINTEXT ATTACK. BUT I COULDN'T ADMIT IT UNTIL I SAW FOR MYSELF.



SO BEFORE YOU SO QUICKLY LABEL ME A THIRD PARTY TO THE COMMUNICATION, JUST REMEMBER: I LOVED HIM FIRST. WE HAD SOMETHING AND SHE TORE IT AWAY. SHE'S THE ATTACKER, NOT ME.



NOT EVE.