Deconstruction and Conditional Erasure of Correlations Joint work with Mario Berta, Fernando Brandao, and Mark Wilde (arXiv:1609.06994)

Christian Majenz QMATH, University of Copenhagen

Beyond I.I.D. in Information Theory, National University of Singapore





Introduction: Decoupling and Erasure

► Task introduced by Groisman, Popescu and Winter in '04

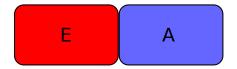
- ► Task introduced by Groisman, Popescu and Winter in '04
- goal: decorrelate two systems by applying local noise

- ► Task introduced by Groisman, Popescu and Winter in '04
- goal: decorrelate two systems by applying local noise

- ► Task introduced by Groisman, Popescu and Winter in '04
- goal: decorrelate two systems by applying local noise

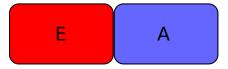
Step-by-step definition:

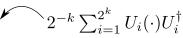
- bipartite quantum system $A\otimes E$ in mixed state ho_{AE}



- Task introduced by Groisman, Popescu and Winter in '04
- goal: decorrelate two systems by applying local noise

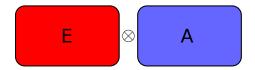
- bipartite quantum system $A\otimes E$ in mixed state ho_{AE}
- apply random unitary channel





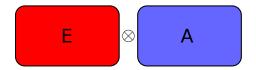
- Task introduced by Groisman, Popescu and Winter in '04
- goal: decorrelate two systems by applying local noise

- bipartite quantum system $A\otimes E$ in mixed state ho_{AE}
- apply random unitary channel
- correlations erased if approximately product



- Task introduced by Groisman, Popescu and Winter in '04
- goal: decorrelate two systems by applying local noise

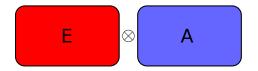
- bipartite quantum system $A\otimes E$ in mixed state ho_{AE}
- apply random unitary channel
- correlations erased if approximately product
- how big do we have to choose k?



$$2^{-k} \sum_{i=1}^{2^k} U_i(\cdot) U_i^{\dagger}$$

- Task introduced by Groisman, Popescu and Winter in '04
- goal: decorrelate two systems by applying local noise

- bipartite quantum system $A\otimes E$ in mixed state ho_{AE}
- apply random unitary channel
- correlations erased if approximately product
- how big do we have to choose k?
- optimal: $k pprox n I(A:E)_\sigma$ for $ho = \sigma^{\otimes n}$



$$2^{-k} \sum_{i=1}^{2^k} U_i(\cdot) U_i^{\dagger}$$

- Task introduced by Groisman, Popescu and Winter in '04
- goal: decorrelate two systems by applying local noise

- bipartite quantum system $A\otimes E$ in mixed state ho_{AE}
- apply random unitary channel
- correlations erased if approximately product
- how big do we have to choose k?
- optimal: $k \approx n I(A:E)_{\sigma}$ for $ho = \sigma^{\otimes n}$
- ⇒ Operational interpretation of the quantum mutual information!

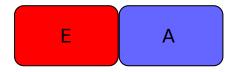
 Different erasure model: partial trace (aka decoupling, Horodecki, Oppenheim and Winter '05)

- Different erasure model: partial trace (aka decoupling, Horodecki, Oppenheim and Winter '05)
- Ubiquitous proof tool (quantum Shannon theory, thermodynamics etc.)

- Different erasure model: partial trace (aka decoupling, Horodecki, Oppenheim and Winter '05)
- Ubiquitous proof tool (quantum Shannon theory, thermodynamics etc.)

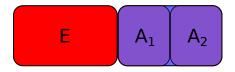
Step-by-step definition:

- bipartite quantum system $A \otimes E$ in mixed state ho_{AE}



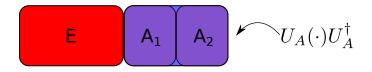
- Different erasure model: partial trace (aka decoupling, Horodecki, Oppenheim and Winter '05)
- Ubiquitous proof tool (quantum Shannon theory, thermodynamics etc.)

- bipartite quantum system $A\otimes E$ in mixed state ho_{AE}
- divide $A \cong A_1 \otimes A_2$



- Different erasure model: partial trace (aka decoupling, Horodecki, Oppenheim and Winter '05)
- Ubiquitous proof tool (quantum Shannon theory, thermodynamics etc.)

- bipartite quantum system $A\otimes E$ in mixed state ho_{AE}
- divide $A \cong A_1 \otimes A_2$
- apply a unitary to A



- Different erasure model: partial trace (aka decoupling, Horodecki, Oppenheim and Winter '05)
- Ubiquitous proof tool (quantum Shannon theory, thermodynamics etc.)

- bipartite quantum system $A\otimes E$ in mixed state ho_{AE}
- divide $A \cong A_1 \otimes A_2$
- apply a unitary to A
- trace out $A_2 \Rightarrow$ approximate product state





- Different erasure model: partial trace (aka decoupling, Horodecki, Oppenheim and Winter '05)
- Ubiquitous proof tool (quantum Shannon theory, thermodynamics etc.)

- bipartite quantum system $A\otimes E$ in mixed state ho_{AE}
- divide $A \cong A_1 \otimes A_2$
- apply a unitary to A
- trace out $A_2 \Rightarrow$ approximate product state
- how big do we have to choose A_2 ?





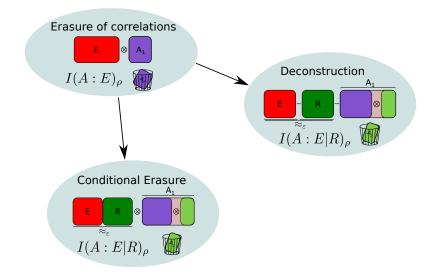
- Different erasure model: partial trace (aka decoupling, Horodecki, Oppenheim and Winter '05)
- Ubiquitous proof tool (quantum Shannon theory, thermodynamics etc.)

- bipartite quantum system $A\otimes E$ in mixed state ho_{AE}
- divide $A \cong A_1 \otimes A_2$
- apply a unitary to A
- trace out $A_2 \Rightarrow$ approximate product state
- how big do we have to choose A_2 ?
- $\log |A_2| \approx \frac{n}{2}I(A:E)_{\sigma}$ for $\rho = \sigma^{\otimes n}$ (Horodecki, Oppenheim, Winter '05)

- Different erasure model: partial trace (aka decoupling, Horodecki, Oppenheim and Winter '05)
- Ubiquitous proof tool (quantum Shannon theory, thermodynamics etc.)

- bipartite quantum system $A\otimes E$ in mixed state ho_{AE}
- divide $A \cong A_1 \otimes A_2$
- apply a unitary to A
- trace out $A_2 \Rightarrow$ approximate product state
- how big do we have to choose A_2 ?
- $\log |A_2| \approx \frac{n}{2}I(A:E)_{\sigma}$ for $\rho = \sigma^{\otimes n}$ (Horodecki, Oppenheim, Winter '05)
- ! Erasure models ar related, exact one shot equivalence if ancillary states are allowed

This talk



Erasure of conditional correlations

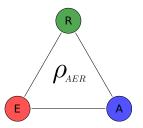


ρAER

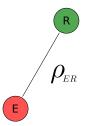
• Conditional quantum mutual information $I(A : E|R)_{\rho} = H(\rho_{AR}) + H(\rho_{ER}) - H(\rho_{AER}) - H(\rho_R)$

- Conditional quantum mutual information $I(A : E|R)_{\rho} = H(\rho_{AR}) + H(\rho_{ER}) - H(\rho_{AER}) - H(\rho_R)$
- ▶ Recoverability: if $I(A : E|R) = \varepsilon$ small, $\rho_{AER} \approx_{\mathcal{O}(\varepsilon)} \mathcal{R}_{R \to RA}(\rho_{ER})$ for some quantum channel \mathcal{R} . (Fawzi, Renner '14)

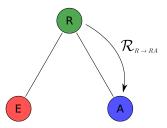
- Conditional quantum mutual information $I(A : E|R)_{\rho} = H(\rho_{AR}) + H(\rho_{ER}) - H(\rho_{AER}) - H(\rho_R)$
- ► Recoverability: if $I(A : E|R) = \varepsilon$ small, $\rho_{AER} \approx_{\mathcal{O}(\varepsilon)} \mathcal{R}_{R \to RA}(\rho_{ER})$ for some quantum channel \mathcal{R} . (Fawzi, Renner '14)



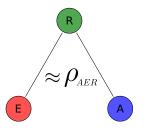
- Conditional quantum mutual information $I(A : E|R)_{\rho} = H(\rho_{AR}) + H(\rho_{ER}) - H(\rho_{AER}) - H(\rho_R)$
- ▶ Recoverability: if $I(A : E|R) = \varepsilon$ small, $\rho_{AER} \approx_{\mathcal{O}(\varepsilon)} \mathcal{R}_{R \to RA}(\rho_{ER})$ for some quantum channel \mathcal{R} . (Fawzi, Renner '14)



- Conditional quantum mutual information $I(A : E|R)_{\rho} = H(\rho_{AR}) + H(\rho_{ER}) - H(\rho_{AER}) - H(\rho_R)$
- ► Recoverability: if $I(A : E|R) = \varepsilon$ small, $\rho_{AER} \approx_{\mathcal{O}(\varepsilon)} \mathcal{R}_{R \to RA}(\rho_{ER})$ for some quantum channel \mathcal{R} . (Fawzi, Renner '14)



- Conditional quantum mutual information $I(A : E|R)_{\rho} = H(\rho_{AR}) + H(\rho_{ER}) - H(\rho_{AER}) - H(\rho_R)$
- ► Recoverability: if $I(A : E|R) = \varepsilon$ small, $\rho_{AER} \approx_{\mathcal{O}(\varepsilon)} \mathcal{R}_{R \to RA}(\rho_{ER})$ for some quantum channel \mathcal{R} . (Fawzi, Renner '14)



- Conditional quantum mutual information $I(A : E|R)_{\rho} = H(\rho_{AR}) + H(\rho_{ER}) - H(\rho_{AER}) - H(\rho_R)$
- ► Recoverability: if $I(A : E|R) = \varepsilon$ small, $\rho_{AER} \approx_{\mathcal{O}(\varepsilon)} \mathcal{R}_{R \to RA}(\rho_{ER})$ for some quantum channel \mathcal{R} . (Fawzi, Renner '14)
- \Rightarrow All correlations of A and E mediated by R

- Conditional quantum mutual information $I(A : E|R)_{\rho} = H(\rho_{AR}) + H(\rho_{ER}) - H(\rho_{AER}) - H(\rho_R)$
- ► Recoverability: if $I(A : E|R) = \varepsilon$ small, $\rho_{AER} \approx_{\mathcal{O}(\varepsilon)} \mathcal{R}_{R \to RA}(\rho_{ER})$ for some quantum channel \mathcal{R} . (Fawzi, Renner '14)
- \Rightarrow All correlations of A and E mediated by R
- $\Rightarrow E R A$ is approximate quantum Markov chain

- Conditional quantum mutual information $I(A : E|R)_{\rho} = H(\rho_{AR}) + H(\rho_{ER}) - H(\rho_{AER}) - H(\rho_R)$
- ► Recoverability: if $I(A : E|R) = \varepsilon$ small, $\rho_{AER} \approx_{\mathcal{O}(\varepsilon)} \mathcal{R}_{R \to RA}(\rho_{ER})$ for some quantum channel \mathcal{R} . (Fawzi, Renner '14)
- \Rightarrow All correlations of A and E mediated by R
- $\Rightarrow E R A$ is approximate quantum Markov chain
 - ► I(A : E|R) measures conditional correlations

Erasure of conditional correlations

▶ i.i.d. setting

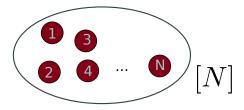
- i.i.d. setting
- Recall: Erasure of correlations in ρ_{AE} operating on A costs I(A : E) bits of noise.

- i.i.d. setting
- Recall: Erasure of correlations in ρ_{AE} operating on A costs I(A : E) bits of noise.
- ? Can we erase conditional correlations by injecting $I(A : E|R)_{\rho}$ bits of noise into A?

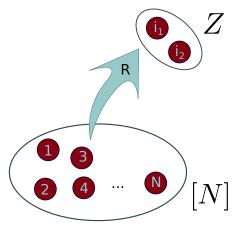
- i.i.d. setting
- Recall: Erasure of correlations in ρ_{AE} operating on A costs I(A : E) bits of noise.
- ? Can we erase conditional correlations by injecting $I(A : E|R)_{\rho}$ bits of noise into A?
- ! No, as shown by Wakakuwa et al. (2016, Poster at BIID2016)

- ? Can we erase conditional correlations by injecting $I(A : E|R)_{\rho}$ bits of noise into A?
- Does not even hold classically. Counterexample:

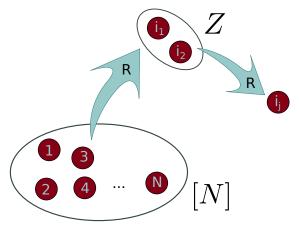
- ? Can we erase conditional correlations by injecting $I(A : E|R)_{\rho}$ bits of noise into A?
- ► Does not even hold classically. Counterexample:



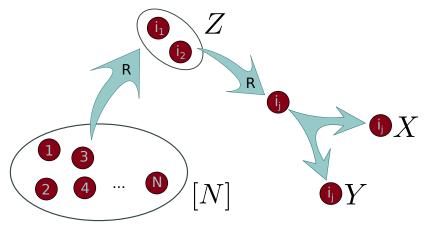
- ? Can we erase conditional correlations by injecting $I(A : E|R)_{\rho}$ bits of noise into A?
- Does not even hold classically. Counterexample:

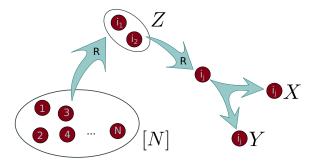


- ? Can we erase conditional correlations by injecting $I(A : E|R)_{\rho}$ bits of noise into A?
- ► Does not even hold classically. Counterexample:

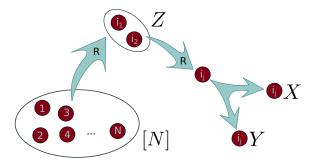


- ? Can we erase conditional correlations by injecting $I(A : E|R)_{\rho}$ bits of noise into A?
- ► Does not even hold classically. Counterexample:

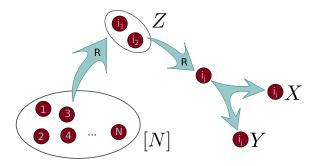




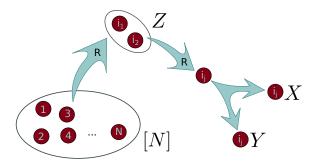
• I(X : Y|Z) = 1 =erasure cost when *conditioning* on Z



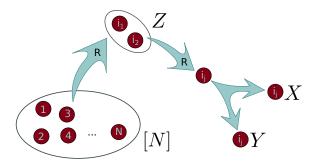
- I(X : Y|Z) = 1 =erasure cost when *conditioning* on Z
- $\mathcal{O}(\log N)$ bits of noise necessary acting on X only



- I(X : Y|Z) = 1 =erasure cost when *conditioning* on Z
- ▶ O(log N) bits of noise necessary acting on X only
- ▶ intuition: surjective $f : [N] \rightarrow [M]$, M < N analogue of partial trace



- I(X : Y|Z) = 1 =erasure cost when *conditioning* on Z
- ▶ O(log N) bits of noise necessary acting on X only
- ▶ intuition: surjective $f : [N] \rightarrow [M]$, M < N analogue of partial trace
- ▶ for $Z = (i_1, i_2)$, correlation of X and Y are destroyed iff $f(i_1) = f(i_2)$



- I(X : Y|Z) = 1 =erasure cost when *conditioning* on Z
- ▶ O(log N) bits of noise necessary acting on X only
- ▶ intuition: surjective $f : [N] \rightarrow [M]$, M < N analogue of partial trace
- for $Z = (i_1, i_2)$, correlation of X and Y are destroyed iff $f(i_1) = f(i_2)$
- need this for most pairs $(i_1, i_2) \Rightarrow M$ small



- ► State *ρ_{AER}*
- quantum conditional operation on A conditioned on R:

- ► State *ρ_{AER}*
- quantum conditional operation on A conditioned on R: operation on AR, but ρ_{RE} approximately unchanged

- ► State *ρ*_{AER}
- quantum conditional operation on A conditioned on R:
 operation on AR, but ρ_{RE} approximately unchanged
- erasure model: partial trace, ancilla

- ► State *ρ*AER
- quantum conditional operation on A conditioned on R:
 operation on AR, but ρ_{RE} approximately unchanged
- erasure model: partial trace, ancilla



- ► State *ρ_{AER}*
- quantum conditional operation on A conditioned on R:
 operation on AR, but ρ_{RE} approximately unchanged
- erasure model: partial trace, ancilla

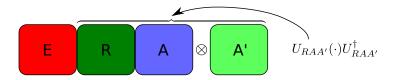
Step-by-step definition:

- add ancillary system A' in a fixed state



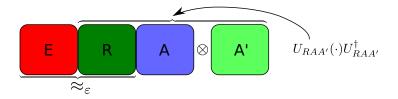
- ► State *ρ_{AER}*
- quantum conditional operation on A conditioned on R:
 operation on AR, but ρ_{RE} approximately unchanged
- erasure model: partial trace, ancilla

- add ancillary system A' in a fixed state
- apply a unitary $U_{RAA'}$



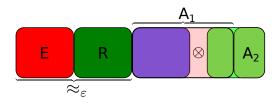
- ► State *ρ*AER
- quantum conditional operation on A conditioned on R:
 operation on AR, but ρ_{RE} approximately unchanged
- erasure model: partial trace, ancilla

- add ancillary system A' in a fixed state
- apply a unitary $U_{RAA'}$ that negligibly disturbs ho_{ER}



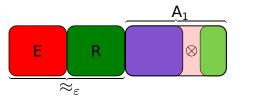
- ► State *ρ*AER
- quantum conditional operation on A conditioned on R: operation on AR, but ρ_{RE} approximately unchanged
- erasure model: partial trace, ancilla

- add ancillary system A' in a fixed state
- apply a unitary $U_{RAA'}$ that negligibly disturbs ho_{ER}
- divide system AA' into two parts, $AA'\cong A_1A_2$

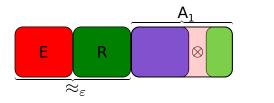


- ► State *ρ*_{AER}
- quantum conditional operation on A conditioned on R: operation on AR, but ρ_{RE} approximately unchanged
- erasure model: partial trace, ancilla

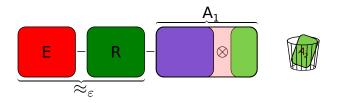
- add ancillary system A' in a fixed state
- apply a unitary $U_{RAA'}$ that negligibly disturbs ho_{ER}
- divide system AA' into two parts, $AA'\cong A_1A_2$
- trace out A_2



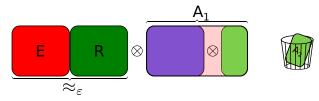
Different goals:

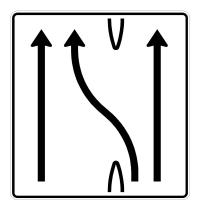


- Different goals:
- ► make E R A₁ an approximate quantum Markov chain, deconstruction of correlations

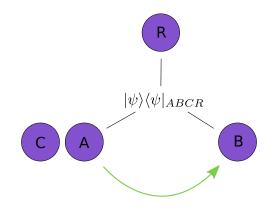


- Different goals:
- ► make E R A₁ an approximate quantum Markov chain, deconstruction of correlations
- ► make A₁ product with ER, conditional erasure of correlations (⇒ deconstruction of correlations)

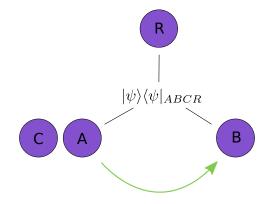




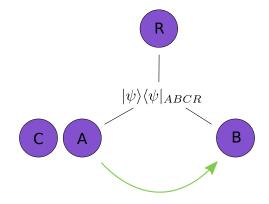
- Alice, Bob and a referee share a pure state $|\psi\rangle\langle\psi|_{ABCR}$



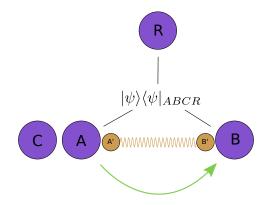
- Alice, Bob and a referee share a pure state $|\psi\rangle\langle\psi|_{ABCR}$
- ▶ Alice has AC, Bob has B, Referee has R



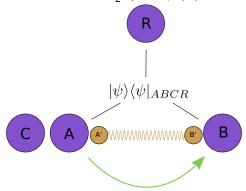
- \blacktriangleright Alice, Bob and a referee share a pure state $|\psi\rangle\langle\psi|_{ABCR}$
- Alice has AC, Bob has B, Referee has R
- their task: Alice has to send A to Bob



- Alice, Bob and a referee share a pure state $|\psi\rangle\langle\psi|_{ABCR}$
- Alice has AC, Bob has B, Referee has R
- their task: Alice has to send A to Bob
- they can use entanglement



- Alice, Bob and a referee share a pure state $|\psi\rangle\langle\psi|_{ABCR}$
- ▶ Alice has AC, Bob has B, Referee has R
- their task: Alice has to send A to Bob
- they can use entanglement
- optimal comunication rate $\frac{1}{2}I(A : R|C)$ (Devetak & Yard '06)



Conditional erasure of correlations is equivalent to quantum state redistribution. Asymptotically, deconstruction needs at least a rate of I(A : E|R) bits of noise.

Conditional erasure of correlations is equivalent to quantum state redistribution. Asymptotically, deconstruction needs at least a rate of I(A : E|R) bits of noise.

 Equivalence: state redistribution is possible with communication rate r/2 iff conditional erasure of correlations is possible with noise rate r

Conditional erasure of correlations is equivalent to quantum state redistribution. Asymptotically, deconstruction needs at least a rate of I(A : E|R) bits of noise.

- Equivalence: state redistribution is possible with communication rate r/2 iff conditional erasure of correlations is possible with noise rate r
- Both tasks have same optimal rate I(A : E|R) of noise asymptotically

Conditional erasure of correlations is equivalent to quantum state redistribution. Asymptotically, deconstruction needs at least a rate of I(A : E|R) bits of noise.

- Equivalence: state redistribution is possible with communication rate r/2 iff conditional erasure of correlations is possible with noise rate r
- Both tasks have same optimal rate I(A : E|R) of noise asymptotically
- Operational interpretation of quantum conditional mutual information!

Applications

► 2-party state ρ_{AB} , measurement $\Lambda_{A \to X}$

Applications

- ► 2-party state ρ_{AB} , measurement $\Lambda_{A \to X}$
- ► (unoptimized) quantum discord: D(A: B)_{ρ,Λ} = I(A: B)_ρ − I(X: B)_{Λ(ρ)}

Applications

- ► 2-party state ρ_{AB} , measurement $\Lambda_{A \to X}$
- ► (unoptimized) quantum discord: D(Ā: B)_{ρ,Λ} = I(A: B)_ρ − I(X: B)_{Λ(ρ)}
- original interpretation: decrease of correlations under interaction with environment ("einselection", Zurek '00)

- ► 2-party state ρ_{AB} , measurement $\Lambda_{A \to X}$
- ► (unoptimized) quantum discord: D(A: B)_{ρ,Λ} = I(A: B)_ρ − I(X: B)_{Λ(ρ)}
- original interpretation: decrease of correlations under interaction with environment ("einselection", Zurek '00)
- if $\Lambda = \Lambda_{A \to X}^{(2)} \circ \Lambda_{A \to A}^{(1)}$, and the action of $\Lambda^{(2)}$ is reversible on $\Lambda^{(1)}(\rho)$ then the loss of correlations has already occurred

Theorem (Berta, Brandao, CM, Wilde)

 $D(\overline{A} : B)_{\rho,\Lambda}$ is equal to the rate of noise necessary to implement the loss of correlations incurred by $\rho^{\otimes n}$ under the action of $\Lambda^{\otimes n}$.

- ► 2-party state ρ_{AB} , measurement $\Lambda_{A \to X}$
- ► (unoptimized) quantum discord: D(A: B)_{ρ,Λ} = I(A: B)_ρ − I(X: B)_{Λ(ρ)}
- original interpretation: decrease of correlations under interaction with environment ("einselection", Zurek '00)
- if $\Lambda = \Lambda_{A \to X}^{(2)} \circ \Lambda_{A \to A}^{(1)}$, and the action of $\Lambda^{(2)}$ is reversible on $\Lambda^{(1)}(\rho)$ then the loss of correlations has already occurred

Theorem (Berta, Brandao, CM, Wilde)

 $D(\overline{A} : B)_{\rho,\Lambda}$ is equal to the rate of noise necessary to implement the loss of correlations incurred by $\rho^{\otimes n}$ under the action of $\Lambda^{\otimes n}$.

- ► 2-party state ρ_{AB} , measurement $\Lambda_{A \to X}$
- ► (unoptimized) quantum discord: D(A: B)_{ρ,Λ} = I(A: B)_ρ − I(X: B)_{Λ(ρ)}
- original interpretation: decrease of correlations under interaction with environment ("einselection", Zurek '00)
- if $\Lambda = \Lambda_{A \to X}^{(2)} \circ \Lambda_{A \to A}^{(1)}$, and the action of $\Lambda^{(2)}$ is reversible on $\Lambda^{(1)}(\rho)$ then the loss of correlations has already occurred

Theorem (Berta, Brandao, CM, Wilde)

 $D(\overline{A} : B)_{\rho,\Lambda}$ is equal to the rate of noise necessary to implement the loss of correlations incurred by $\rho^{\otimes n}$ under the action of $\Lambda^{\otimes n}$.

Proof idea: D(Ā: B)_{ρ,Λ} = I(E : B|X)_{V(ρ)}, V_{A→XE} Stinespring dilation of Λ

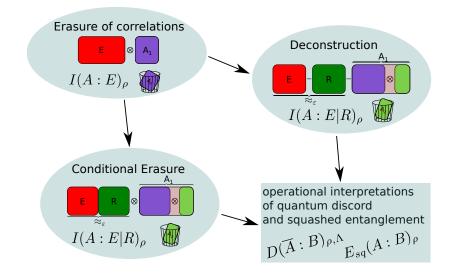
- ► 2-party state ρ_{AB} , measurement $\Lambda_{A \to X}$
- ► (unoptimized) quantum discord: D(A: B)_{ρ,Λ} = I(A: B)_ρ − I(X: B)_{Λ(ρ)}
- original interpretation: decrease of correlations under interaction with environment ("einselection", Zurek '00)
- if $\Lambda = \Lambda_{A \to X}^{(2)} \circ \Lambda_{A \to A}^{(1)}$, and the action of $\Lambda^{(2)}$ is reversible on $\Lambda^{(1)}(\rho)$ then the loss of correlations has already occurred

Theorem (Berta, Brandao, CM, Wilde)

 $D(\overline{A} : B)_{\rho,\Lambda}$ is equal to the rate of noise necessary to implement the loss of correlations incurred by $\rho^{\otimes n}$ under the action of $\Lambda^{\otimes n}$.

- ▶ proof idea: D(Ā: B)_{ρ,Λ} = I(E: B|X)_{V(ρ)}, V_{A→XE} Stinespring dilation of Λ
- Other application related to Squashed entanglement: $E_{sq}(A:B)_{\rho} = \inf_{\sigma} I(A:B|E)_{\sigma}$, inf over all σ_{ABE} with $\operatorname{tr}_{E} \sigma_{ABE} = \rho_{AB}$

The End



backup slide

"⇒"∶

- $"\Rightarrow$ ":
 - Alice's part of a state redistribution protocol:

$"\Rightarrow$ ":

Alice's part of a state redistribution protocol:

append mixed ancilla (Alice's half of entangled states)

$"\Rightarrow$ ":

- Alice's part of a state redistribution protocol:
 - append mixed ancilla (Alice's half of entangled states)
 - apply a unitary

$"\Rightarrow$ ":

- Alice's part of a state redistribution protocol:
 - append mixed ancilla (Alice's half of entangled states)
 - apply a unitary
 - get rid of a subsystem (the message to bob)

"⇒":

- Alice's part of a state redistribution protocol:
 - append mixed ancilla (Alice's half of entangled states)
 - apply a unitary
 - get rid of a subsystem (the message to bob)
- correctness of SRD protocol implies negligible disturbance and approximate decoupling condition

"⇒":

- Alice's part of a state redistribution protocol:
 - append mixed ancilla (Alice's half of entangled states)
 - apply a unitary
 - get rid of a subsystem (the message to bob)
- correctness of SRD protocol implies negligible disturbance and approximate decoupling condition

"⇐":

"⇒":

- Alice's part of a state redistribution protocol:
 - append mixed ancilla (Alice's half of entangled states)
 - apply a unitary
 - get rid of a subsystem (the message to bob)
- correctness of SRD protocol implies negligible disturbance and approximate decoupling condition

"⇐":

 Replace the decoupling protocol in the standard state merging protocol by the conditional erasure protocol at hand