Noisy quantum state redistribution with promise and the Alpha-bit

Anurag Anshu[1], Min-Hsiu Hsieh[2], Rahul Jain[1,3,4]

1. Centre for Quantum Technologies, NUS, Singapore
2. Centre for Quantum Software and Information, University of Technology Sydney, Australia
3. MajuLab, UMI 3654, Singapore.
4. VAJRA Adjunct Faculty, TIFR, Mumbai, India. arXiv:1803.03414

June 30, 2018

Outline for section 1

The task

- Hayden, Pennington [2017]
- A channel $\mathcal{N}_{A\to B}$ between Alice and Bob.

The task

- Hayden, Pennington [2017]
- A channel $\mathcal{N}_{A\to B}$ between Alice and Bob.
- Alice receives a quantum state $|\psi\rangle \in \mathcal{H}^d$. Bob receives the classical description of a subspace $S \subset \mathcal{H}^d$ of dimension $d^\alpha + 1$. Guaranteed that $|\psi\rangle \in S$.

The task

- Hayden, Pennington [2017]
- A channel $\mathcal{N}_{A\to B}$ between Alice and Bob.
- Alice receives a quantum state $|\psi\rangle \in \mathcal{H}^d$. Bob receives the classical description of a subspace $S \subset \mathcal{H}^d$ of dimension $d^\alpha + 1$. Guaranteed that $|\psi\rangle \in S$.
- Alice needs to transmit $|\psi\rangle$ to Bob. For every subspace S, average error of decoding $|\psi\rangle \in S$ should be small.

The task

- Introduce a Reference.
- Fix an S. Alice and Reference share $|\Psi(S)\rangle_{RA}$, where Ψ_A is maximally mixed in S. Bob receives classical description of S.
- Transmit register A to Bob such that final state $\Psi'(S)_{RA}$ satisfies $\Psi'(S) \overset{\varepsilon}{\approx} |\Psi(S)\rangle\langle\Psi(S)|_{RA}$ for all S.

Capacities

- Think of $\alpha = 1$. Consider n uses of the channel and largest possible $d(n)$ such that decoding is successful with high fidelity.
- Capacity $= \frac{1}{n} \log d(n)$.

Capacities

- General α. Consider n uses of the channel and largest possible $d(n)$ such that decoding in the subspace S is successful with high fidelity.
- Capacity $= \frac{1}{n} \log d(n)$.

Capacities

- General α. Consider n uses of the channel and largest possible $d(n)$ such that decoding in the subspace S is successful with high fidelity.
- Capacity $= \frac{1}{n} \log d(n)$.
- Actual definition: allow many i.i.d. instances and take appropriate limit.
- Smaller α implies higher capacity: smaller α implies less quantum states to decode.

Capacities

- Entanglement assisted α-bit capacity:

$$\frac{1}{1+\alpha}\max_{\psi_{AA'}} I(B:A')_{\rho_{BA'}}.$$

Capacities

- Entanglement assisted α-bit capacity:

$$\frac{1}{1+\alpha}\max_{\psi_{AA'}} I(B:A')_{\rho_{BA'}}.$$

- Entanglement unassisted α-bit capacity:

$$\max_{\psi_{AA'}}\left[\min\left(\frac{1}{1+\alpha}\max_{\psi_{AA'}} I(B:A')_{\rho_{BA'}}, \frac{1}{\alpha}\max_{\psi_{AA'}} I(B>A')_{\rho_{BA'}}\right)\right]$$

- $\rho_{A'B} = \mathcal{N}_{A\to B}(\psi_{AA'})$.

Alpha-bit as a resource

- Entanglement assisted classical capacity of α-bit: largest C such that one can transmit nC bits by the use of n instances of α-bit.

Alpha-bit as a resource

- Entanglement assisted classical capacity of α-bit: largest C such that one can transmit nC bits by the use of n instances of α-bit.
- Answer is $C = 1 + \alpha$. Reversible theory in asymptotic and i.i.d. setting (recall entanglement assisted capacity).
- Think of $\alpha = 1$. It is a qubit that can be transmitted perfectly. By superdense coding, 2 classical bits can be transmitted.

Features

- Key tool: subspace decoupling duality (a generalization of weak decoupling duality, Hayden, Winter [IEEE IT]) + decoupling via random unitary.
- Used for all above achievability results and converse.
- Several consequences for resource theory of quantum communication.

Our results

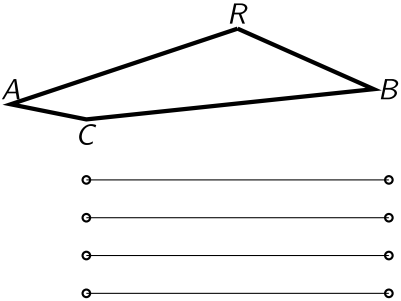
- Generalize the notion: Quantum state redistribution + quantum channel coding.

Our results

- Generalize the notion: Quantum state redistribution + quantum channel coding.
- Quantum state redistribution as a resource: asymptotically reversible theory.
- Reminiscent: Quantum Reverse Shannon Theorem (Bennett, Devetak, Harrow, Shor, Winter [arXiv 2009, IEEE IT 2014]; Berta, Christandl, Renner [CMP 2011]).

Outline for section 2

Quantum state redistribution (QSR)



Devetak and Yard [PRL 2008, IEEE IT 2009].
Communication rate in the asymptotic and i.i.d. setting:
$I(R : C|B)$.

Noisy quantum state redistribution

- Channel $\mathcal{N}_{J\to K}$.
- How many channel uses required to perform n instances of QSR for $|\Psi\rangle_{RABC}$?

Noisy quantum state redistribution

- Channel $\mathcal{N}_{J\to K}$.
- How many channel uses required to perform n instances of QSR for $|\Psi\rangle_{RABC}$?
- Approximately
$$\frac{\max_{\mu} I(R:C|B)}{C_{ea}(\mathcal{N}_{J\to K})},$$
where $C_{ea}(\mathcal{N})$ is entanglement assisted classical capacity of $\mathcal{N}_{J\to K}$. Bennett, Shor, Smolin, Thapliyal [IEEE IT 2002].

Noisy quantum state redistribution

- Channel $\mathcal{N}_{J\to K}$.
- How many channel uses required to perform n instances of QSR for $|\Psi\rangle_{RABC}$?
- Approximately

$$\frac{\max_{\mu} I(R:C|B)}{C_{ea}(\mathcal{N}_{J\to K})},$$

  where $C_{ea}(\mathcal{N})$ is entanglement assisted classical capacity of $\mathcal{N}_{J\to K}$. Bennett, Shor, Smolin, Thapliyal [IEEE IT 2002].
- Optimal in the asymptotic and i.i.d. setting. Quantum Reverse Shannon Theorem (Bennett, Devetak, Harrow, Shor, Winter [arXiv 2009, IEEE IT 2014]; Berta, Christandl, Renner [CMP 2011]).

A generalization of Alpha-bit task

- Quantum state redistribution with promise (Promise-QSR).
- Alice, Bob and Reference share the state $|\Psi^y\rangle_{RABC}$. Reference and Bob know y.

A generalization of Alpha-bit task

- Quantum state redistribution with promise (Promise-QSR).
- Alice, Bob and Reference share the state $|\Psi^y\rangle_{RABC}$. Reference and Bob know y.
- Alice needs to send a message to Bob, such that after Bob's decoding, the final state Φ^y_{RABC} satisfies $\Phi^y_{RABC} \overset{\varepsilon}{\approx} |\Psi^y\rangle\langle\Psi^y|_{RABC}$ for all y.

A simplification: min-max duality

- Consider the task: for a distribution $\mu(y)$, perform the QSR of

$$\sum_y \sqrt{\mu(y)}\,|y\rangle_Y\,|y\rangle_{R_Y}\,|\Psi^y\rangle_{RABC}\,.$$

A simplification: min-max duality

- Consider the task: for a distribution $\mu(y)$, perform the QSR of

$$\sum_y \sqrt{\mu(y)} \left|y\right\rangle_Y \left|y\right\rangle_{R_Y} \left|\Psi^y\right\rangle_{RABC}.$$

- Let $\mathcal{P}_C$ be the set of all protocols with communication at most C (finite amount of entanglement used).

A simplification: min-max duality

- Consider the task: for a distribution $\mu(y)$, perform the QSR of

$$\sum_{y} \sqrt{\mu(y)} \, |y\rangle_{Y} \, |y\rangle_{R_Y} \, |\Psi^{y}\rangle_{RABC} .$$

- Let $\mathcal{P}_C$ be the set of all protocols with communication at most C (finite amount of entanglement used).
- Min-max principle [Yao, FOCS 1979]:

$$\max_{\mu} \min_{P \in \mathcal{P}_C} \mathrm{error}(\mu, P) = \min_{P \in \mathcal{P}_C} \max_{\mu} \mathrm{error}(\mu, P).$$

- Promise-QSR $<=$ QSR for all distributions μ.

Promise-QSR through noisy channel

- Compose the noiseless protocol for QSR with noisy channel coding.

Promise-QSR through noisy channel

- Compose the noiseless protocol for QSR with noisy channel coding.
- Number of channel uses required to achieve one instance of Promise-QSR (in asymptotic and i.i.d. setting) is upper bounded by

$$\frac{\max_{\mu} I(RR_Y : C|BY)}{C_{ea}(\mathcal{N}_{J\to K})}.$$

Promise-QSR through noisy channel

- Compose the noiseless protocol for QSR with noisy channel coding.
- Number of channel uses required to achieve one instance of Promise-QSR (in asymptotic and i.i.d. setting) is upper bounded by

$$\frac{\max_{\mu} I(RR_Y : C|BY)}{C_{ea}(\mathcal{N}_{J\to K})}.$$

- Similar statements (carefully done) for the one-shot setting.
- But is it optimal?

Decoupling Alice's entanglement

- QSR protocols have the property that Alice's final entanglement is independent of y.
- A protocol for Promise-QSR may not have this property.

Decoupling Alice's entanglement

- QSR protocols have the property that Alice's final entanglement is independent of y.
- A protocol for Promise-QSR may not have this property.
- But subspace decoupling duality implies that this is the case for Alpha-bit.
- Alpha-bit = Alpha-bit for all μ.

Recovering Alpha-bit capacities

- Consider $\sum_S \sqrt{\mu(S)} \left|S\right\rangle_Y \left|S\right\rangle_{R_Y} \left|\Psi(S)\right\rangle_{RC}$.

Recovering Alpha-bit capacities

- Consider $\sum_S \sqrt{\mu(S)} \left|S\right\rangle_Y \left|S\right\rangle_{R_Y} \left|\Psi(S)\right\rangle_{RC}$.
- $\max_\mu I(RR_Y : C|Y) = (1+\alpha)\log d$, where $d = |C|$.

Recovering Alpha-bit capacities

- Consider $\sum_S \sqrt{\mu(S)}\,|S\rangle_Y\,|S\rangle_{R_Y}\,|\Psi(S)\rangle_{RC}$.
- $\max_\mu I(RR_Y : C|Y) = (1+\alpha)\log d$, where $d = |C|$.
- Number of channel uses per instance of Alpha-bit task

$$= \frac{(1+\alpha)\log d}{C_{ea}(\mathcal{N}_{J\to K})}.$$

- Capacity is largest d for one channel use.

Recovering Alpha-bit capacities

- Consider $\sum_S \sqrt{\mu(S)}\,|S\rangle_Y\,|S\rangle_{R_Y}\,|\Psi(S)\rangle_{RC}$.
- $\max_\mu I(RR_Y : C|Y) = (1+\alpha)\log d$, where $d = |C|$.
- Number of channel uses per instance of Alpha-bit task

$$= \frac{(1+\alpha)\log d}{C_{ea}(\mathcal{N}_{J\to K})}.$$

- Capacity is largest d for one channel use.
- $\log d = \frac{C_{ea}(\mathcal{N}_{J\to K})}{(1+\alpha)}$.
- Similar one-shot results available as well.

Recovering Alpha-bit capacities

- QSR for $\sum_S \sqrt{\mu(S)} \left|S\right\rangle_Y \left|S\right\rangle_{R_Y} \left|\Psi(S)\right\rangle_{RC}$ is actually quantum state merging.

Recovering Alpha-bit capacities

- QSR for $\sum_S \sqrt{\mu(S)}\,|S\rangle_Y\,|S\rangle_{R_Y}\,|\Psi(S)\rangle_{RC}$ is actually quantum state merging.
- Entanglement always gained (for above instance).
- Using protocol for either entanglement assisted or unassisted (Lloyd, Shor, Devetak [1997-2005]) capacities of $\mathcal{N}_{J\to K}$ leads to an optimal protocol for unassisted capacity of Alpha-bit in asymptotic and i.i.d. setting.

Recovering Alpha-bit capacities

- QSR for $\sum_S \sqrt{\mu(S)} \left|S\right\rangle_Y \left|S\right\rangle_{R_Y} \left|\Psi(S)\right\rangle_{RC}$ is actually quantum state merging.
- Entanglement always gained (for above instance).
- Using protocol for either entanglement assisted or unassisted (Lloyd, Shor, Devetak [1997-2005]) capacities of $\mathcal{N}_{J\to K}$ leads to an optimal protocol for unassisted capacity of Alpha-bit in asymptotic and i.i.d. setting.
- Weakness: capacity for one instance of Alpha-dit not recovered (feature implicit in Hayden, Pennington [2017] owing to subspace decouping duality).

A classical Alpha-bit

- Bob receives a subset $S \in [1, 2, \ldots d]$ and Alice receives an $i \in S$.
- Communicate i to Bob.

A classical Alpha-bit

- Bob receives a subset $S \in [1, 2, \ldots d]$ and Alice receives an $i \in S$.
- Communicate i to Bob.
- Entanglement assisted classical capacity of classical Alpha-bit:

$$\frac{1}{\alpha} \max_{\psi_{JJ'}} I(K : J')_{\mathcal{N}_{J \to K}(\psi_{JJ'})}.$$

Outline for section 3

Definition of simulation

- Fix a quantum state Ψ_{RABC} and a protocol P for QSR of Ψ_{RABC}.
- Alice needs to communicate a message $m \in [1, 2, \ldots 2^N]$.

Definition of simulation

- Fix a quantum state Ψ_{RABC} and a protocol P for QSR of Ψ_{RABC}.
- Alice needs to communicate a message $m \in [1, 2, \ldots 2^N]$.
- In a simulation via QSR, Alice and Bob have preshared entanglement $|\omega\rangle_{E_A E_B}$.
- Given a m, Alice singles out some registers A_m, C_m, which are subsets of E_A.

Definition of simulation

- Fix a quantum state Ψ_{RABC} and a protocol P for QSR of Ψ_{RABC}.
- Alice needs to communicate a message $m \in [1, 2, \ldots 2^N]$.
- In a simulation via QSR, Alice and Bob have preshared entanglement $|\omega\rangle_{E_A E_B}$.
- Given a m, Alice singles out some registers A_m, C_m, which are subsets of E_A.
- She runs P on A_m, C_m. Communication to Bob is implicit in P.
- Bob decodes on his final state, to recover m.

Our result

- Any protocol P for QSR of Ψ_{RABC} can be used to communicate a message in $[1, 2, \ldots 2^N]$ with error $\varepsilon + 2\delta$, where N is equal to

$$I_H^{\varepsilon}(R : BC)_{\Psi} - I_{\max}^{\delta}(R : B)_{\Psi} + \log \varepsilon\delta.$$

Our result

- Any protocol P for QSR of Ψ_{RABC} can be used to communicate a message in $[1, 2, \ldots 2^N]$ with error $\varepsilon + 2\delta$, where N is equal to

$$I_H^{\varepsilon}(R : BC)_{\Psi} - I_{\max}^{\delta}(R : B)_{\Psi} + \log \varepsilon\delta.$$

- Equal to $I(R : C|B)_{\Psi}$ in the asymptotic and i.i.d. setting.
- Simulation rate equal to communication rate in asymptotic and i.i.d. setting.

Our result

- Any protocol P for QSR of Ψ_{RABC} can be used to communicate a message in $[1, 2, \ldots 2^N]$ with error $\varepsilon + 2\delta$, where N is equal to

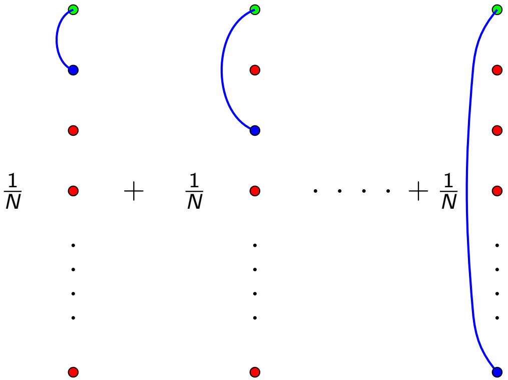
$$I_H^{\varepsilon}(R : BC)_{\Psi} - I_{\max}^{\delta}(R : B)_{\Psi} + \log \varepsilon\delta.$$

- Equal to $I(R : C|B)_{\Psi}$ in the asymptotic and i.i.d. setting.
- Simulation rate equal to communication rate in asymptotic and i.i.d. setting.
- Reminiscent: Quantum Reverse Shannon Theorem (Bennett, Devetak, Harrow, Shor, Winter [arXiv 2009, IEEE IT 2014]; Berta, Christandl, Renner [CMP 2011]).

Recovering entanglement assisted classical capacity of Alpha-bit

- Appeal to subspace-decoupling duality: any protocol for Alpha-bit is also a protocol for state redistribution under distribution μ.
- Alice's operations ensure that state is transmitted to Bob with remaining registers independent of S.
- Use result in previous slide.

Position-based decoding



If $N < I_H(R : B)$, correlation can be located (A., Jain, Warsi [IEEE IT, 2018]).

Outline for section 4

Take-home message

Any QSR task can be used as a resource, with optimal simulation cost in asymptotic and i.i.d. setting.

Future work

- Consequences in theory of quantum communication?

Future work

- Consequences in theory of quantum communication?
- What are the communication costs and simulation capabilities of Promise-QSR?
- In general, a protocol for Promise-QSR may not lead to a protocol for QSR with distribution over y.

Future work

- Consequences in theory of quantum communication?
- What are the communication costs and simulation capabilities of Promise-QSR?
- In general, a protocol for Promise-QSR may not lead to a protocol for QSR with distribution over y.
- Alpha-bit is an exception, also results discussed in Andreas' talk.
- General problem: cost of forgetting C? Lauriere, Touchette [ISIT 2017].

Future work

- Consequences in theory of quantum communication?
- What are the communication costs and simulation capabilities of Promise-QSR?
- In general, a protocol for Promise-QSR may not lead to a protocol for QSR with distribution over y.
- Alpha-bit is an exception, also results discussed in Andreas' talk.
- General problem: cost of forgetting C? Lauriere, Touchette [ISIT 2017].
- Extending above results to multi-party setting.

Thank you!