Quantum decoupling via efficient 'classical' operations and the entanglement cost of one-shot quantum protocols

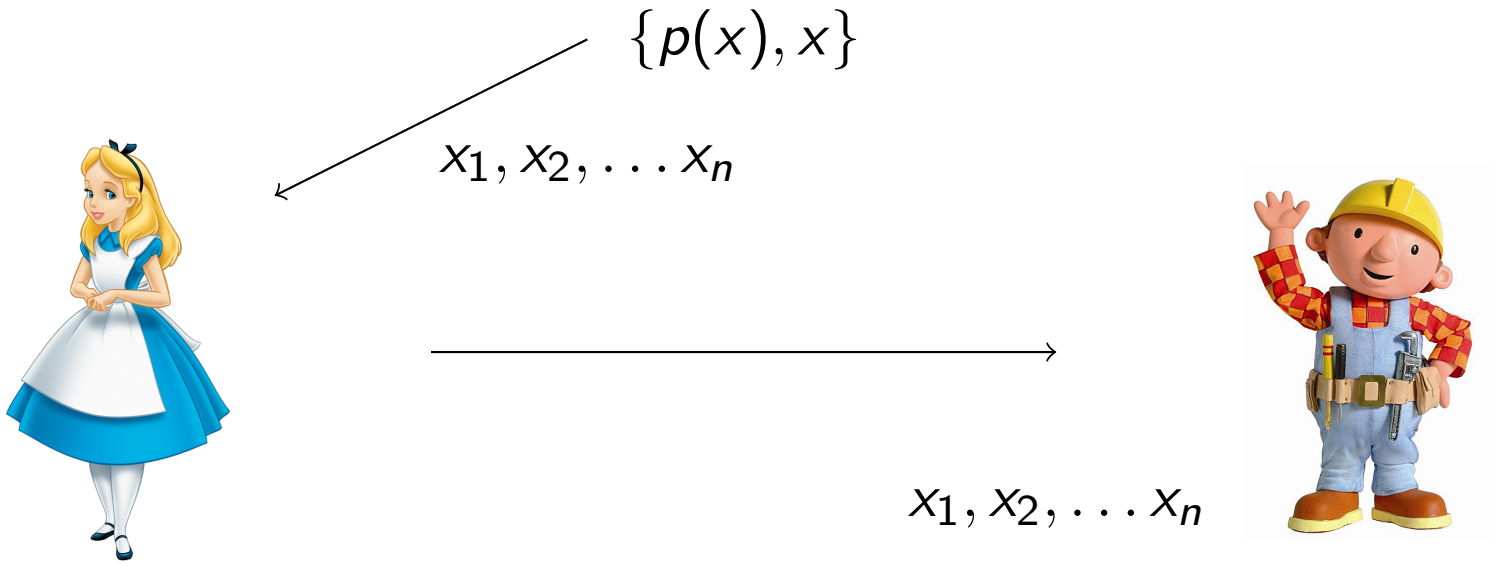
Anurag Anshu (joint work with Rahul Jain)

Institute for Quantum Computing and Perimeter Institute for Theoretical Physics, Waterloo
https://arxiv.org/abs/1809.07056

November 14, 2018

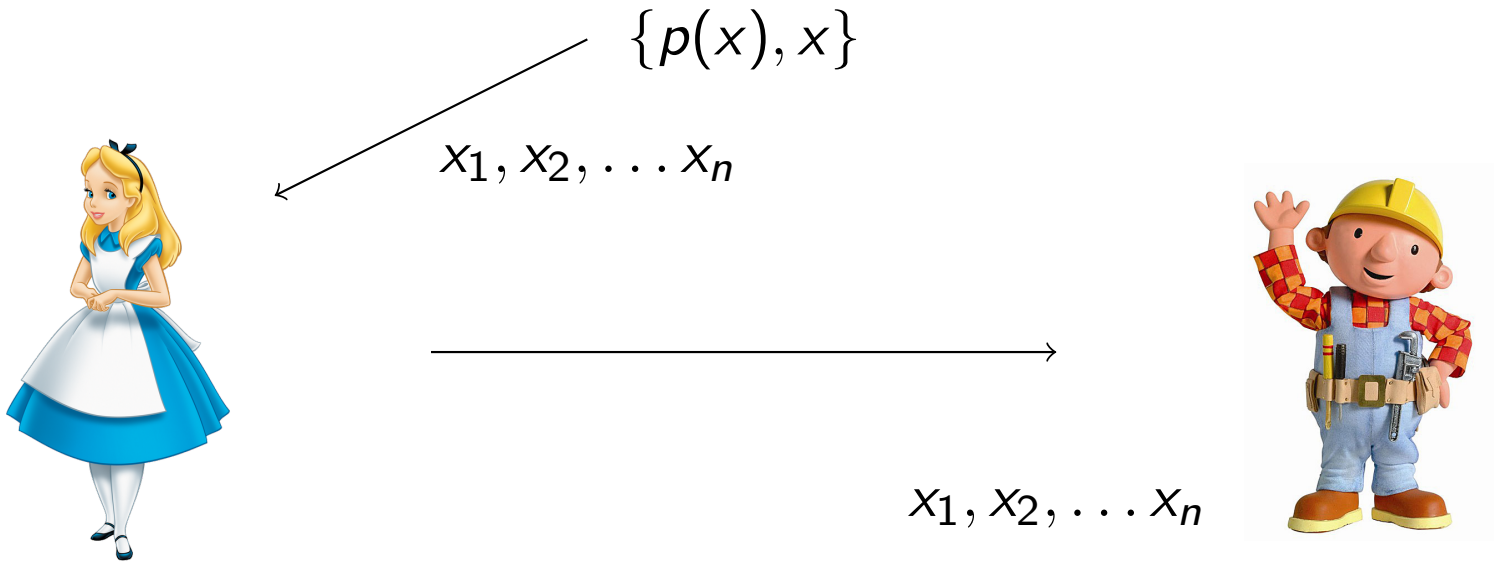
Outline for section 1

Shannon's source compression



Shannon [Bell Sys. Tech. Jour, 1948].

Shannon's source compression



Shannon [Bell Sys. Tech. Jour, 1948].

Most sources (telegraphy, television signal, PCM transmitter, natural languages) produce biased distribution, giving scope for compression.

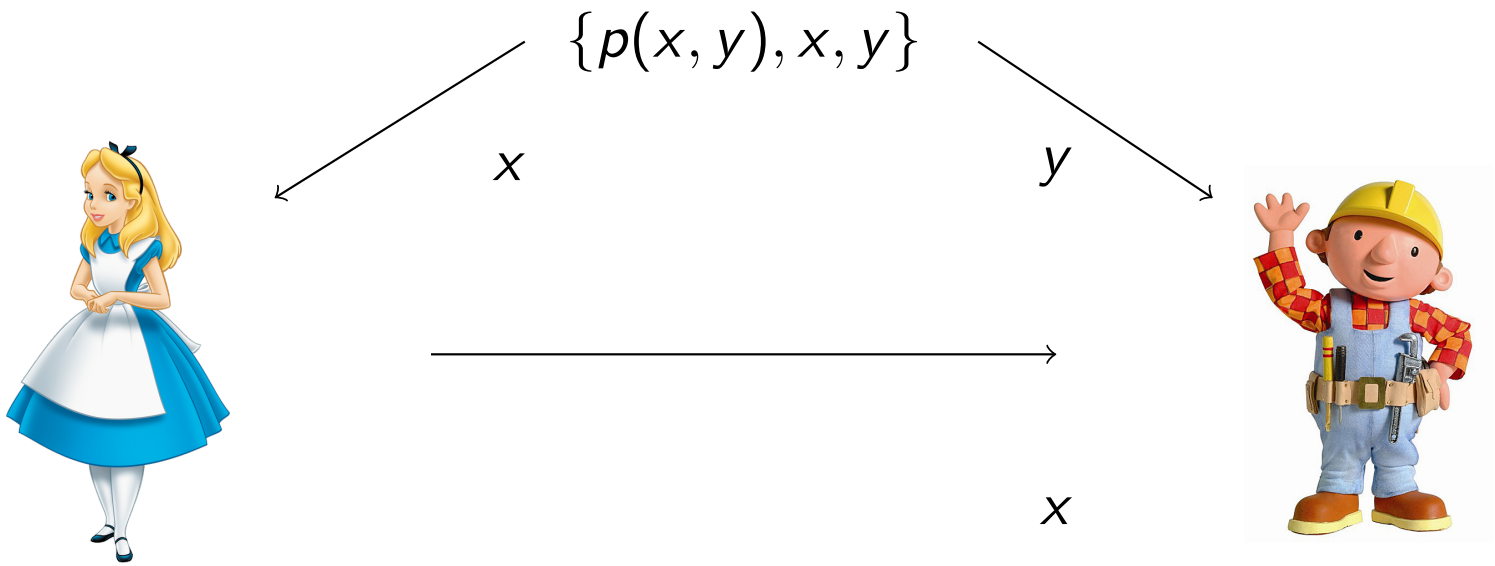
Shannon's source coding

- Shannon constructed a protocol in which
  - the "number of bits communicated *divided by* n" approached $H(X) = \sum_x p(x) \log \frac{1}{p(x)}$ (the Shannon entropy of the source)
  - error approached 0 as $n \to \infty$.

Shannon's source coding

- Shannon constructed a protocol in which
  - the "number of bits communicated *divided by* n" approached $H(X) = \sum_x p(x) \log \frac{1}{p(x)}$ (the Shannon entropy of the source)
  - error approached 0 as $n \to \infty$.
- Idea: communicate only the 'typical' sequences.
- Shannon entropy captures the 'information content' of the source.

Slepian-Wolf source compression with side information



Slepian, Wolf [IEEE IT, 1973].

Slepian-Wolf source compression with side information

- Showed that rate of communication is $H(X|Y)$, the conditional entropy, in asymptotic and i.i.d. setting.

Slepian-Wolf source compression with side information

- Showed that rate of communication is $H(X|Y)$, the conditional entropy, in asymptotic and i.i.d. setting.
- In one-shot setting, one gets a one-shot version of $H(X|Y)$, known as $H_{max}(X|Y)$.
- Note that Alice does not know y.

Slepian-Wolf source compression with side information

- Showed that rate of communication is $H(X|Y)$, the conditional entropy, in asymptotic and i.i.d. setting.
- In one-shot setting, one gets a one-shot version of $H(X|Y)$, known as $H_{max}(X|Y)$.
- Note that Alice does not know y.
- Idea of random function: Alice applies a random permutation π on $\mathcal{X}$ and sends first $H_{max}(X|Y)$ bits to Bob.
  - Chances that $\pi(x)$ and $\pi(x')$ agree on the remaining $\log|X| - H_{max}(X|Y)$ bits is very small, given Bob's knowledge of y.

Randomness extractor

- Given joint random variables XE, apply a function on X such that the output is uniform and independent of E.
- Usually additional randomness is required for efficient implementation of the function (Trevisan [STOC, 1999]).

Randomness extractor

- Given joint random variables XE, apply a function on X such that the output is uniform and independent of E.
- Usually additional randomness is required for efficient implementation of the function (Trevisan [STOC, 1999]).
- Simple construction: apply a random permutation π on $\mathcal{X}$ and discard all but first $H_{min}(X|E)$ bits.

Randomness extractor

- Given joint random variables XE, apply a function on X such that the output is uniform and independent of E.
- Usually additional randomness is required for efficient implementation of the function (Trevisan [STOC, 1999]).
- Simple construction: apply a random permutation π on $\mathcal{X}$ and discard all but first $H_{min}(X|E)$ bits.
- Random permutation can be replaced by pairwise independent permutations.
  - Pick $a, b \in \mathcal{X}$ at random.
  - Apply $F_{a,b}(x) = ax + b$ modulo $|X|$.

Outline for section 2

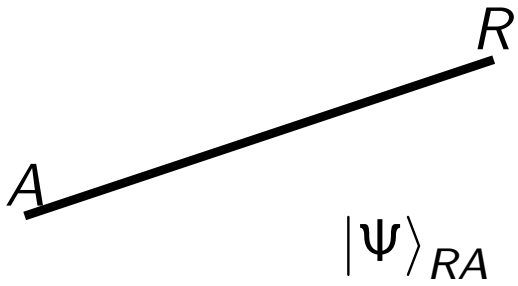
The task of decoupling

- Given a quantum state Ψ_{RA}, apply a unitary on A to output A_1A_2.
- We require R to be independent of A_1 after discarding A_2.
- May or may not want A_1 to be uniform.

The task of decoupling

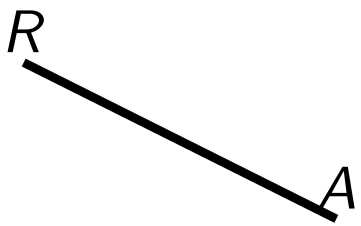
- Given a quantum state Ψ_{RA}, apply a unitary on A to output A_1A_2.
- We require R to be independent of A_1 after discarding A_2.
- May or may not want A_1 to be uniform.
- What is the minimum size of A_2 to be discarded to achieve this?
- How efficient can the unitary be?

Task: Quantum state transfer

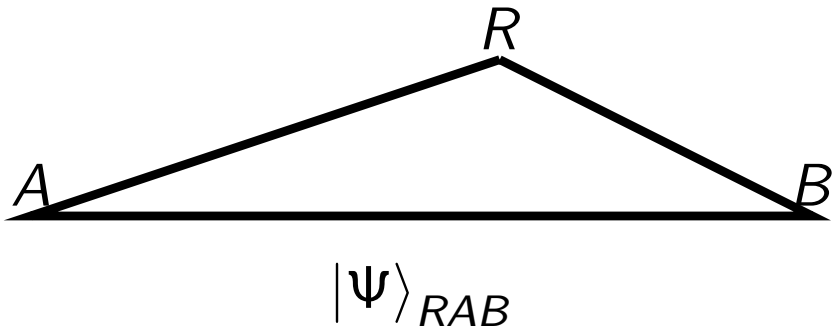


Schumacher [Phys. Rev. A., 1995]

Task: Quantum state transfer

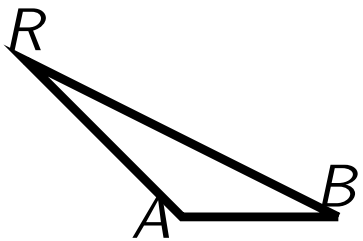


Task: Quantum state merging

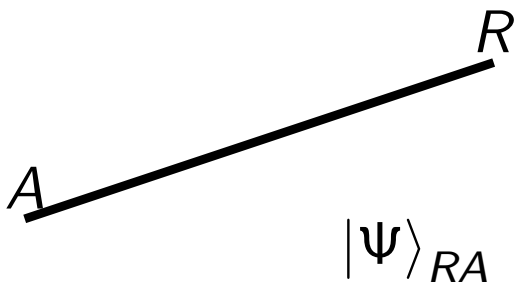


Horodecki, Oppenheim, Winter [Nature, 2005]

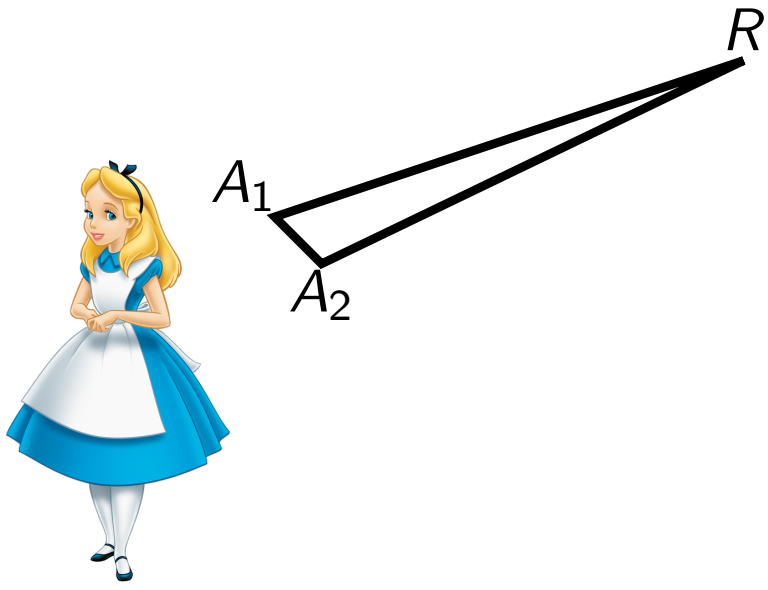
Task: Quantum state merging



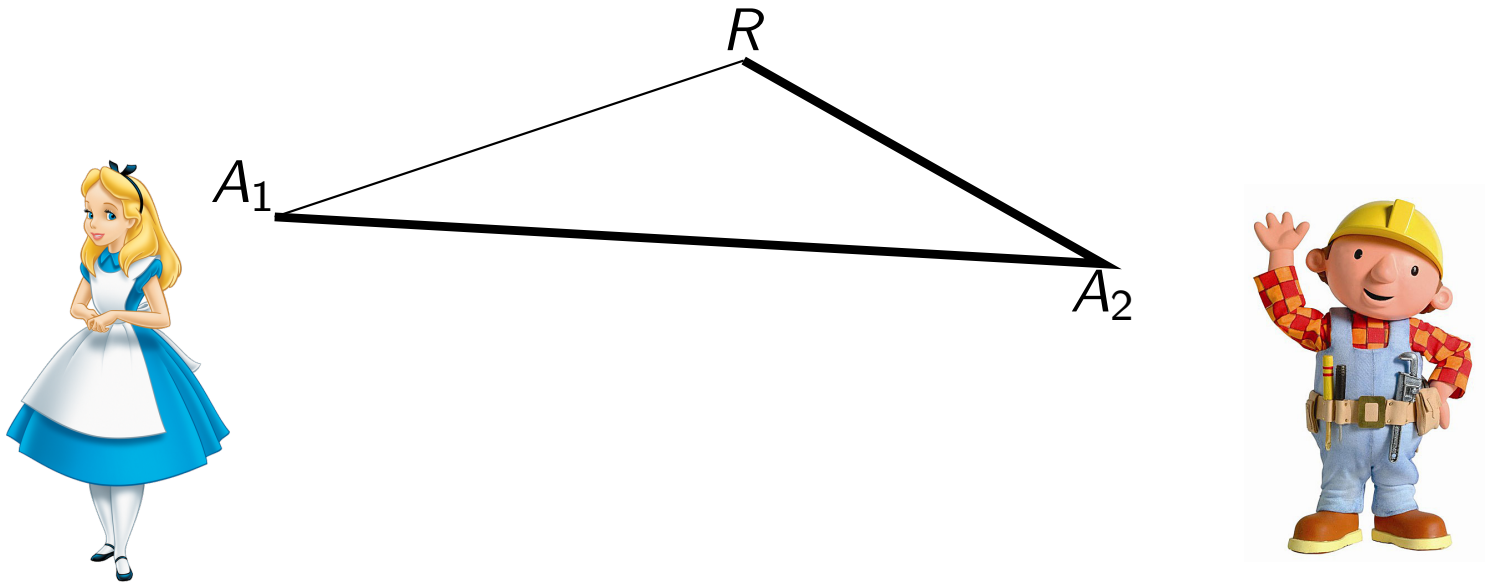
Protocol: Quantum state transfer



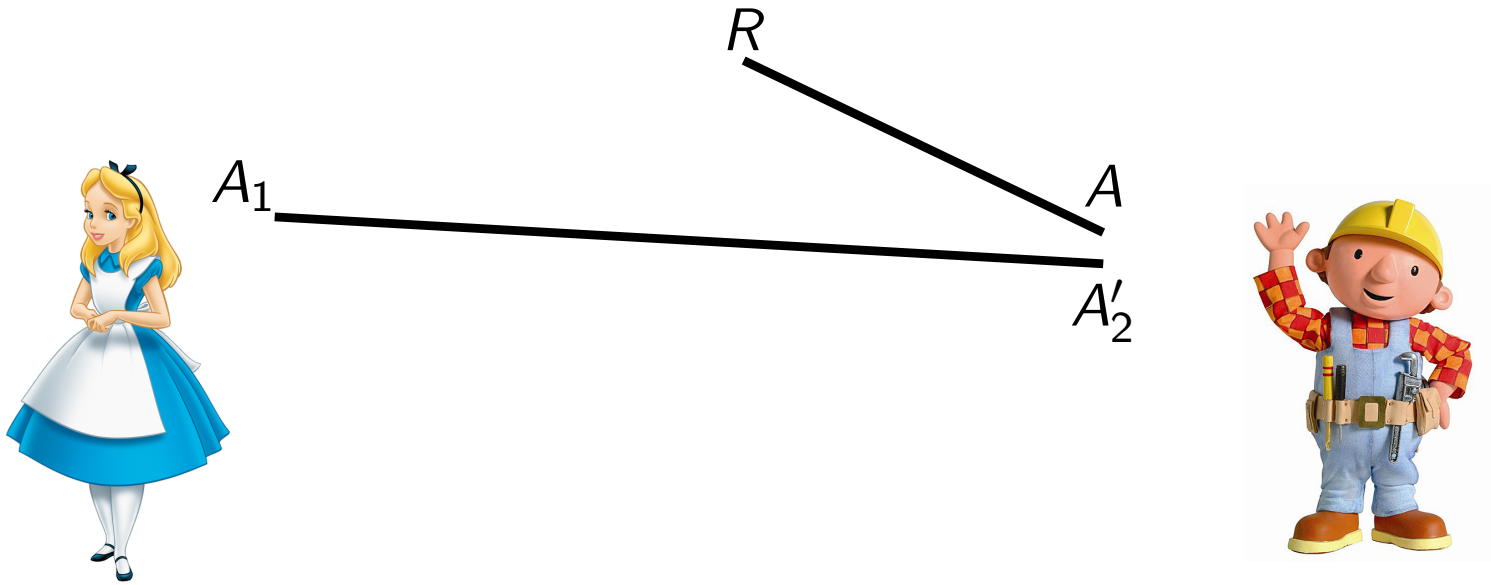
Alice applies decoupling unitary



Alice sends A_2 to Bob



Bob separates out the purification of R



Other uses of decoupling

- Almost all quantum communication paradigms (quantum state merging, Horodecki, Oppenheim, Winter [Nature, 2005]; quantum state redistribution, Devetak, Yard [PRL, 2008]; quantum channel coding, Hayden, Horodecki, Winter, Yard [OSID, 2008],...).

Other uses of decoupling

- Almost all quantum communication paradigms (quantum state merging, Horodecki, Oppenheim, Winter [Nature, 2005]; quantum state redistribution, Devetak, Yard [PRL, 2008]; quantum channel coding, Hayden, Horodecki, Winter, Yard [OSID, 2008],...).
- Randomness extraction (Renner [PhD Thesis, 2005]; Berta [PhD Thesis, 2013]).

Other uses of decoupling

- Almost all quantum communication paradigms (quantum state merging, Horodecki, Oppenheim, Winter [Nature, 2005]; quantum state redistribution, Devetak, Yard [PRL, 2008]; quantum channel coding, Hayden, Horodecki, Winter, Yard [OSID, 2008],...).
- Randomness extraction (Renner [PhD Thesis, 2005]; Berta [PhD Thesis, 2013]).
- Quantum thermodynamics (del Rio, Aberg, Renner, Dahlsten, Vedral [Nature, 2011]).

Other uses of decoupling

- Almost all quantum communication paradigms (quantum state merging, Horodecki, Oppenheim, Winter [Nature, 2005]; quantum state redistribution, Devetak, Yard [PRL, 2008]; quantum channel coding, Hayden, Horodecki, Winter, Yard [OSID, 2008],...).
- Randomness extraction (Renner [PhD Thesis, 2005]; Berta [PhD Thesis, 2013]).
- Quantum thermodynamics (del Rio, Aberg, Renner, Dahlsten, Vedral [Nature, 2011]).
- Black hole physics (Page [PRL, 1993]; Hayden, Preskill [JHEP, 2007]).

Known decouplers

- Random unitary (Horodecki, Oppenheim, Winter [Nature, 2005]; Dupuis [PhD thesis, 2010]; Szehr [Masters thesis, 2011]; Dupuis, Berta, Wullschleger, Renner [Comm. Math. Phys, 2014]).

Known decouplers

- Random unitary (Horodecki, Oppenheim, Winter [Nature, 2005]; Dupuis [PhD thesis, 2010]; Szehr [Masters thesis, 2011]; Dupuis, Berta, Wullschleger, Renner [Comm. Math. Phys, 2014]).
- Unitary 2-designs, such as random Clifford circuits (DiVincenzo, Leung, Terhal [IEEE IT, 2002]; Chau [IEEE IT, 2006]; Dankert, Cleve, Emerson, Livine [PRA, 2009]; Cleve, Leung, Liu, Wang [QIC 2016]).
  - Cleve, Leung, Liu, Wang [QIC 2016] achieve $O(n \log n)$ circuit size, $O(\log n \log\log n)$ depth, using $O(n)$ additional qubits.

Known decouplers

- Random unitary (Horodecki, Oppenheim, Winter [Nature, 2005]; Dupuis [PhD thesis, 2010]; Szehr [Masters thesis, 2011]; Dupuis, Berta, Wullschleger, Renner [Comm. Math. Phys, 2014]).
- Unitary 2-designs, such as random Clifford circuits (DiVincenzo, Leung, Terhal [IEEE IT, 2002]; Chau [IEEE IT, 2006]; Dankert, Cleve, Emerson, Livine [PRA, 2009]; Cleve, Leung, Liu, Wang [QIC 2016]).
  - Cleve, Leung, Liu, Wang [QIC 2016] achieve $O(n \log n)$ circuit size, $O(\log n \log\log n)$ depth, using $O(n)$ additional qubits.
- Brown, Fawzi [Comm Math Phys, 2015] give a decoupling unitary using random quantum circuits.

Known decouplers

- Random unitary (Horodecki, Oppenheim, Winter [Nature, 2005]; Dupuis [PhD thesis, 2010]; Szehr [Masters thesis, 2011]; Dupuis, Berta, Wullschleger, Renner [Comm. Math. Phys, 2014]).
- Unitary 2-designs, such as random Clifford circuits (DiVincenzo, Leung, Terhal [IEEE IT, 2002]; Chau [IEEE IT, 2006]; Dankert, Cleve, Emerson, Livine [PRA, 2009]; Cleve, Leung, Liu, Wang [QIC 2016]).
  - Cleve, Leung, Liu, Wang [QIC 2016] achieve $O(n \log n)$ circuit size, $O(\log n \log\log n)$ depth, using $O(n)$ additional qubits.
- Brown, Fawzi [Comm Math Phys, 2015] give a decoupling unitary using random quantum circuits.
- Convex-split method (A., Devabathini, Jain [PRL, 2017]).

Known decouplers

- Random unitary (Horodecki, Oppenheim, Winter [Nature, 2005]; Dupuis [PhD thesis, 2010]; Szehr [Masters thesis, 2011]; Dupuis, Berta, Wullschleger, Renner [Comm. Math. Phys, 2014]).
- Unitary 2-designs, such as random Clifford circuits (DiVincenzo, Leung, Terhal [IEEE IT, 2002]; Chau [IEEE IT, 2006]; Dankert, Cleve, Emerson, Livine [PRA, 2009]; Cleve, Leung, Liu, Wang [QIC 2016]).
  - Cleve, Leung, Liu, Wang [QIC 2016] achieve $O(n \log n)$ circuit size, $O(\log n \log\log n)$ depth, using $O(n)$ additional qubits.
- Brown, Fawzi [Comm Math Phys, 2015] give a decoupling unitary using random quantum circuits.
- Convex-split method (A., Devabathini, Jain [PRL, 2017]).
- Unitary inside a black hole?

Outline for section 3

Quantum decoupler verses randomness extractor

- Randomness extractor uses pairwise independent permutations.

Quantum decoupler verses randomness extractor

- Randomness extractor uses pairwise independent permutations.
- Quantum decoupling requires unitary 2-designs or random circuit.

Quantum decoupler verses randomness extractor

- Randomness extractor uses pairwise independent permutations.
- Quantum decoupling requires unitary 2-designs or random circuit.
- Random permutations don't seem to be good quantum decouplers (Szehr [Master's thesis, 2011]).

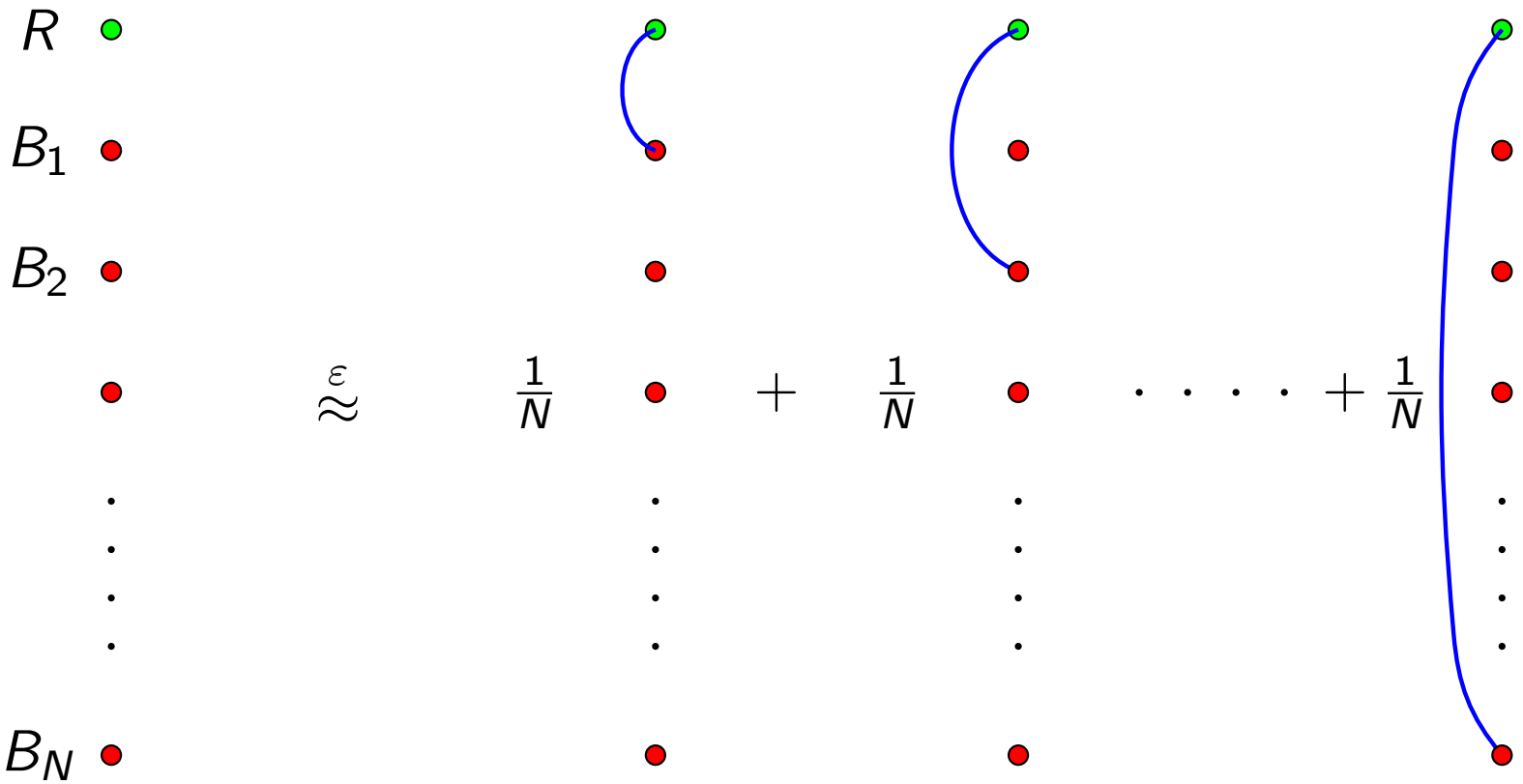
Quantum decoupler verses randomness extractor

- Randomness extractor uses pairwise independent permutations.
- Quantum decoupling requires unitary 2-designs or random circuit.
- Random permutations don't seem to be good quantum decouplers (Szehr [Master's thesis, 2011]).

Theorem (This talk)

There is a quantum decoupling method that just does addition/multiplication modulo a prime.

Convex-split lemma



If $\log N \geq \mathrm{I}_{max}(R:B)_\psi + \log \frac{1}{\varepsilon}$.

Properties of convex-split method

- A quantum analogue of 'rejection sampling based protocols' in communication complexity.

Properties of convex-split method

- A quantum analogue of 'rejection sampling based protocols' in communication complexity.
- Along with position-based decoding (A., Jain, Warsi [IEEE IT, 2018]), can be used to construct protocols for various information theoretic tasks. A unified view for obtaining protocols for

Properties of convex-split method

- A quantum analogue of 'rejection sampling based protocols' in communication complexity.
- Along with position-based decoding (A., Jain, Warsi [IEEE IT, 2018]), can be used to construct protocols for various information theoretic tasks. A unified view for obtaining protocols for
  - Channel coding scenarios, Source compression scenarios and Randomness extractor.

Properties of convex-split method

- A quantum analogue of 'rejection sampling based protocols' in communication complexity.
- Along with position-based decoding (A., Jain, Warsi [IEEE IT, 2018]), can be used to construct protocols for various information theoretic tasks. A unified view for obtaining protocols for
  - Channel coding scenarios, Source compression scenarios and Randomness extractor.
  - Achieves near optimal communication in many such scenarios. Else provably smaller communication than previous methods.

Properties of convex-split method

- A quantum analogue of 'rejection sampling based protocols' in communication complexity.
- Along with position-based decoding (A., Jain, Warsi [IEEE IT, 2018]), can be used to construct protocols for various information theoretic tasks. A unified view for obtaining protocols for
  - Channel coding scenarios, Source compression scenarios and Randomness extractor.
  - Achieves near optimal communication in many such scenarios. Else provably smaller communication than previous methods.
- Has found use in problems beyond Shannon theory: such as in quantum Resource theory (A., Hsieh, Jain [PRL, 2018]; Majenz, Berta [PRL, 2018]).

Comparison with decoupling via random unitary

- Decoupling via random unitaries leads to uniform state on decoupled register (similar to randomness extractor).
  - This is too much work in one-shot settings. Such as when R and A are already independent, yet A is not uniform (Berta, Christandl, Renner [Comm. Math. Phys., 2011]).

Comparison with decoupling via random unitary

- Decoupling via random unitaries leads to uniform state on decoupled register (similar to randomness extractor).
  - This is too much work in one-shot settings. Such as when R and A are already independent, yet A is not uniform (Berta, Christandl, Renner [Comm. Math. Phys., 2011]).
- Convex-split lemma avoids this extra work.

Comparison with decoupling via random unitary

- Decoupling via random unitaries leads to uniform state on decoupled register (similar to randomness extractor).
  - This is too much work in one-shot settings. Such as when R and A are already independent, yet A is not uniform (Berta, Christandl, Renner [Comm. Math. Phys., 2011]).
- Convex-split lemma avoids this extra work.
- But decoupling via random unitary requires exponentially less entanglement.

Comparison with decoupling via random unitary

- Decoupling via random unitaries leads to uniform state on decoupled register (similar to randomness extractor).
  - This is too much work in one-shot settings. Such as when R and A are already independent, yet A is not uniform (Berta, Christandl, Renner [Comm. Math. Phys., 2011]).
- Convex-split lemma avoids this extra work.
- But decoupling via random unitary requires exponentially less entanglement.
- Can we get best of both?

Theorem

Yes we can, with entanglement required $\frac{1}{\epsilon}$ *times that used in decoupling via random unitary, for error* ϵ.

Decoupling via efficient classical operations

- Fix a preferred basis such as computational basis. A unitary is classical if it takes basis vectors to basis vectors.

Decoupling via efficient classical operations

- Fix a preferred basis such as computational basis. A unitary is classical if it takes basis vectors to basis vectors.
- Convex-split is cyclic shift of registers and hence classical.

Decoupling via efficient classical operations

- Fix a preferred basis such as computational basis. A unitary is classical if it takes basis vectors to basis vectors.
- Convex-split is cyclic shift of registers and hence classical.
- We obtain unitaries that mimick the behaviour of cyclic shift (among other requirements), but using just two additional registers.

Decoupling via efficient classical operations

- Introduce registers A_2, J, where $A_2 \equiv A$ and J is the register that will be discarded.

Decoupling via efficient classical operations

- Introduce registers A_2, J, where $A_2 \equiv A$ and J is the register that will be discarded.
- Perform the following unitary on A, A_2, J:

$$U \left|i\right\rangle_A \left|i'\right\rangle_{A_2} \left|j\right\rangle_J =$$

$$\left|i + (i' - i) \cdot j \bmod |A|\right\rangle_A \left|i' + (i' - i) \cdot j \bmod |A|\right\rangle_{A_2} \left|j\right\rangle_J .$$

Decoupling via efficient classical operations

- Introduce registers A_2, J, where $A_2 \equiv A$ and J is the register that will be discarded.
- Perform the following unitary on A, A_2, J:

$$U \left|i\right\rangle_A \left|i'\right\rangle_{A_2} \left|j\right\rangle_J =$$

$$\left|i + (i' - i) \cdot j \bmod |A|\right\rangle_A \left|i' + (i' - i) \cdot j \bmod |A|\right\rangle_{A_2} \left|j\right\rangle_J .$$

- Discarding J achieves decoupling.

Decoupling via efficient classical operations

- Introduce registers A_2, J, where $A_2 \equiv A$ and J is the register that will be discarded.
- Perform the following unitary on A, A_2, J:

$$U |i\rangle_A \left|i'\right\rangle_{A_2} |j\rangle_J =$$

$$\left|i + (i' - i) \cdot j \bmod |A|\right\rangle_A \left|i' + (i' - i) \cdot j \bmod |A|\right\rangle_{A_2} |j\rangle_J .$$

- Discarding J achieves decoupling.
- Technicality: $|A|$ needs to be prime and its dimension has to be increased by quadratic amount (easily fixed by using additional $2 \log |A|$ ancillas).

How to make a register uniform

- Previously done in Berta, Christandl, Renner [Comm. Math. Phys, 2011]. Method used implicitly in Bennett, Shor, Smolin, Thapliyal [IEEE IT, 2002].

How to make a register uniform

- Previously done in Berta, Christandl, Renner [Comm. Math. Phys, 2011]. Method used implicitly in Bennett, Shor, Smolin, Thapliyal [IEEE IT, 2002].
- Idea: divide the eigenvalues of Ψ_A into $O(\log |A|)$ blocks. Then run decoupling in superposition using approximate embezzling states (van Dam, Hayden [PRA, 2003]).

How to make a register uniform

- Previously done in Berta, Christandl, Renner [Comm. Math. Phys, 2011]. Method used implicitly in Bennett, Shor, Smolin, Thapliyal [IEEE IT, 2002].
- Idea: divide the eigenvalues of Ψ_A into $O(\log |A|)$ blocks. Then run decoupling in superposition using approximate embezzling states (van Dam, Hayden [PRA, 2003]).
- Leads to a loss of $O(\log \log |A|)$ in communication cost.

How to make a register uniform

- Previously done in Berta, Christandl, Renner [Comm. Math. Phys, 2011]. Method used implicitly in Bennett, Shor, Smolin, Thapliyal [IEEE IT, 2002].
- Idea: divide the eigenvalues of Ψ_A into $O(\log |A|)$ blocks. Then run decoupling in superposition using approximate embezzling states (van Dam, Hayden [PRA, 2003]).
- Leads to a loss of $O(\log \log |A|)$ in communication cost.
- Does not achieve near optimal one-shot communication over entanglement assisted quantum channel (Bennett, Shor, Smolin, Thapliyal [IEEE IT, 2002]; Datta, Tomamichel, Wilde [Quant Inf Proc, 2016]).

Make a register uniform using correlated sampling

- We use an idea from correlated sampling (Broder [CCS, 1997]; Charikar [STOC 2002]; Kleinberg, Tardos [JACM, 2002]; Holenstein [STOC 2007]; Barak et. al. [FOCS, 2008]; Braverman, Rao [FOCS, 2011]; A.-Jain-Mukhopadhyay-Shayeghi-Yao [IEEE IT, 2016]).

Make a register uniform using correlated sampling

- We use an idea from correlated sampling (Broder [CCS, 1997]; Charikar [STOC 2002]; Kleinberg, Tardos [JACM, 2002]; Holenstein [STOC 2007]; Barak et. al. [FOCS, 2008]; Braverman, Rao [FOCS, 2011]; A.-Jain-Mukhopadhyay-Shayeghi-Yao [IEEE IT, 2016]).
- Realize Ψ_A as a marginal of a state σ_{AE} uniform in its support.

Make a register uniform using correlated sampling

- Since $E|A = a$ depends on a, we perform it coherently using approximate embezzling states.

Make a register uniform using correlated sampling

- Since $E|A = a$ depends on a, we perform it coherently using approximate embezzling states.
- Two important property of this approach:
  - One-shot information quantities change by an additive factor of at most a constant.
  - Off-diagonal terms of Ψ_{RA} not an issue, since we show approximate embezzling in a strong notion of approximation.

Outlook

- A uniform approach that achieves near optimal one-shot communication for entanglement-assisted quantum channel coding and quantum state merging, along with using small entanglement.

Outlook

- A uniform approach that achieves near optimal one-shot communication for entanglement-assisted quantum channel coding and quantum state merging, along with using small entanglement.
- Reproduces all results obtained via convex-split method (such as quantum state redistribution), without changing the communication cost.

Outlook

- A uniform approach that achieves near optimal one-shot communication for entanglement-assisted quantum channel coding and quantum state merging, along with using small entanglement.
- Reproduces all results obtained via convex-split method (such as quantum state redistribution), without changing the communication cost.
- Exponential improvement in entanglement required; of the order of that in decoupling via random unitary.

Thank you for your attention!