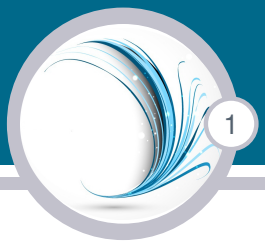
A Quantum Multiparty Packing Lemma and the Relay Channel

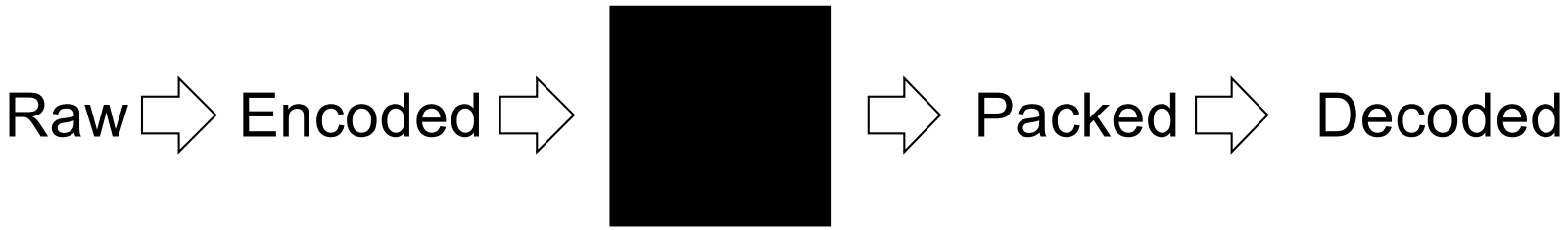
Dawei Ding
Stanford University
Joint with Hrant Gharibyan, Patrick Hayden, and Michael Walter

Outline

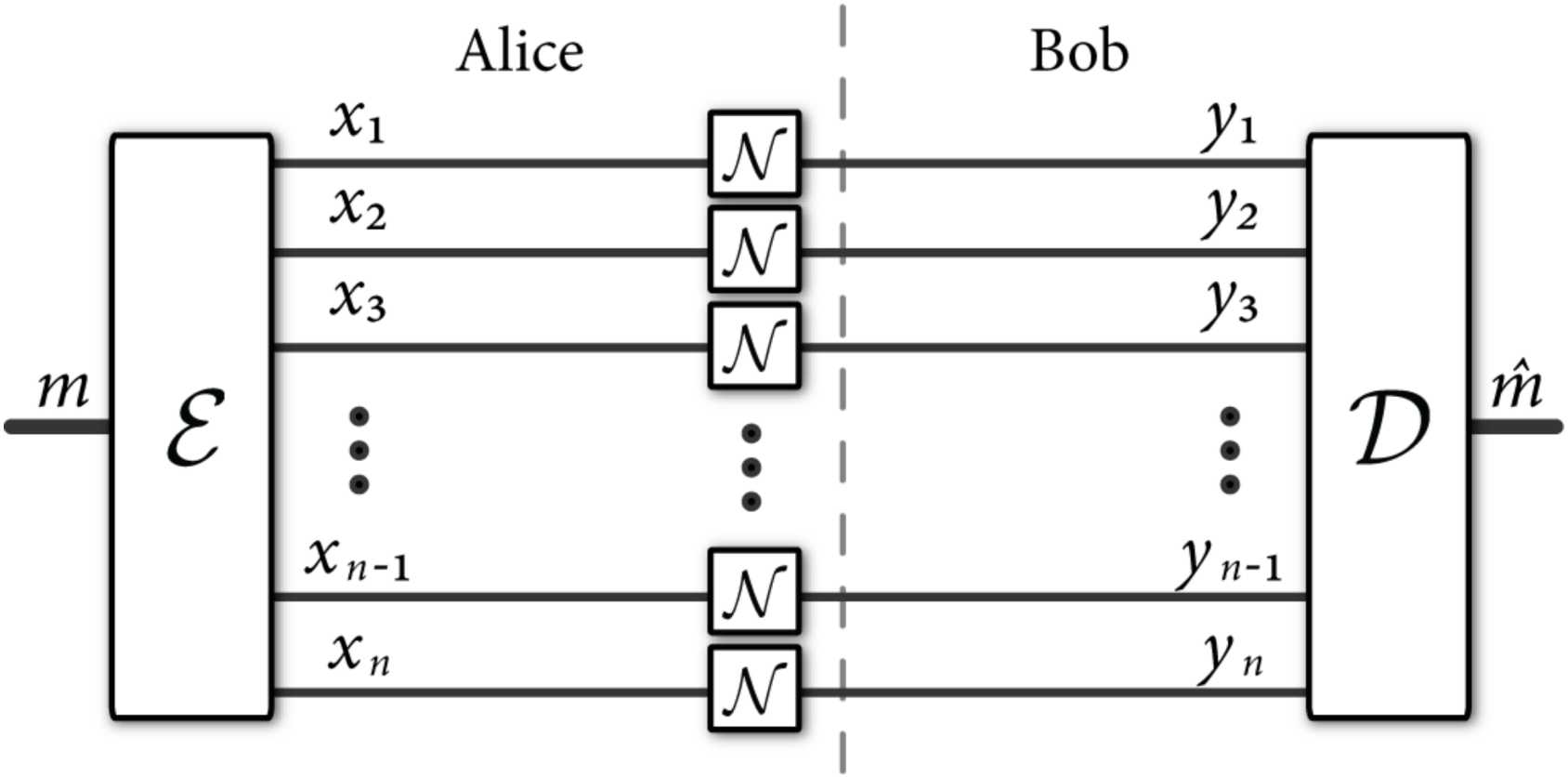


Introduction
Message packing

Introduction
Message packing



Introduction
Communication as message packing



Taken from Mark Wilde's From Classical to Quantum Shannon Theory

Introduction
Encoding messages into quantum systems

- Classical-quantum black box: Input is classical, output is quantum

- Classical-quantum black box: Input is classical, output is quantum

Theorem (Holevo-Schumacher-Westmoreland theorem)

The classical capacity of a quantum channel $\mathcal{N}_{A\to B}$ with separable encodings is

$$C(\mathcal{N}) = \max_{\{p_X, \rho_A^{(x)}\}} I(X;B)_\rho$$

where

$$\rho_{XB} \equiv \sum_x p_X(x) \left|x\right\rangle \left\langle x\right|_X \otimes \rho_B^{(x)}.$$

Introduction
Encoding messages into quantum systems

- Network information theory: multiple senders and/or multiple receivers

Introduction
Encoding messages into quantum systems

- Network information theory: multiple senders and/or multiple receivers
  - Classical-quantum channels: Multiple classical inputs, quantum output

Introduction
Encoding messages into quantum systems

- Network information theory: multiple senders and/or multiple receivers
  - Classical-quantum channels: Multiple classical inputs, quantum output
  - Mostly open for quantum channels, especially one-shot

Introduction
Encoding messages into quantum systems

- Network information theory: multiple senders and/or multiple receivers
  - Classical-quantum channels: Multiple classical inputs, quantum output
  - Mostly open for quantum channels, especially one-shot
- Multiparty packing: encoding multiple messages M_j into a quantum system B via multiple classical systems X_v

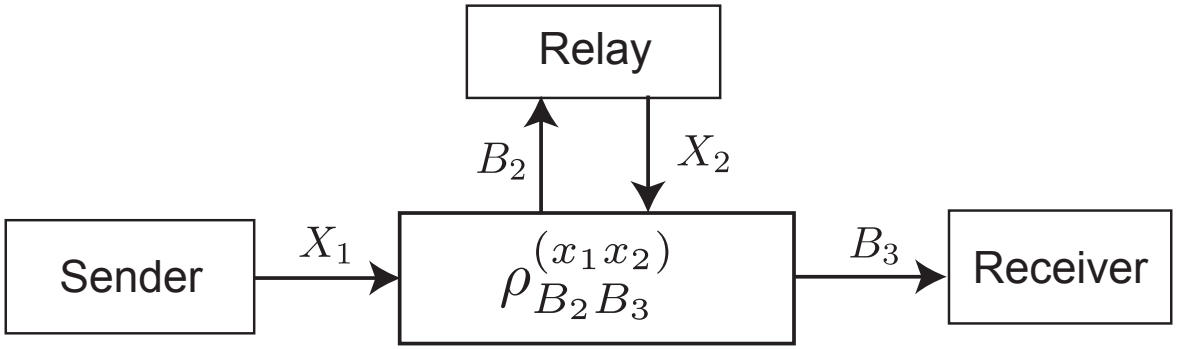
Introduction
Encoding messages into quantum systems

- Network information theory: multiple senders and/or multiple receivers
  - Classical-quantum channels: Multiple classical inputs, quantum output
  - Mostly open for quantum channels, especially one-shot
- Multiparty packing: encoding multiple messages M_j into a quantum system B via multiple classical systems X_v
  - Multiple senders: multiple access channel, relay channel

Introduction
Encoding messages into quantum systems

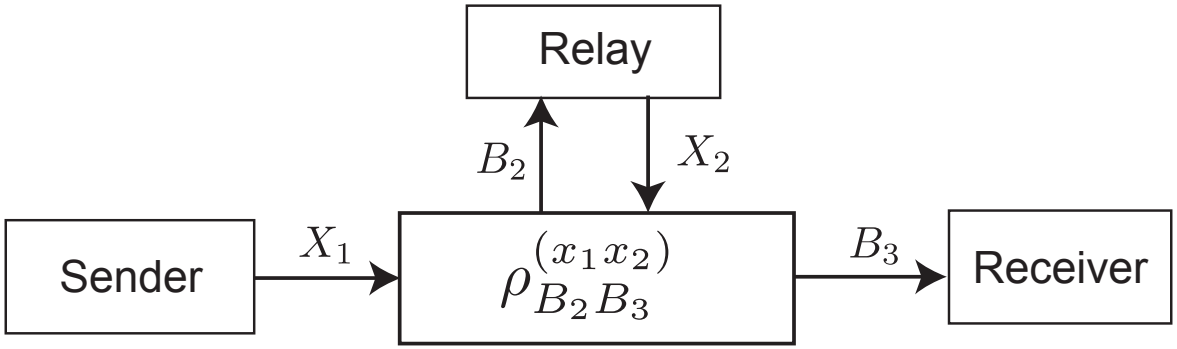
- Network information theory: multiple senders and/or multiple receivers
  - Classical-quantum channels: Multiple classical inputs, quantum output
  - Mostly open for quantum channels, especially one-shot
- Multiparty packing: encoding multiple messages M_j into a quantum system B via multiple classical systems X_v
  - Multiple senders: multiple access channel, relay channel
- Assuming classical-quantum channel, codebook is of the form $\{x_v(m)\}_{v\in V, m\in M}$, where $M = \bigtimes_{j\in J} M_j$

Relay channel
Relay channel definition



- $\mathcal{N}_{X_1X_2\to B_2B_3} : \mathcal{X}_1 \times \mathcal{X}_2 \to \mathcal{H}_{B_2} \otimes \mathcal{H}_{B_3}, (x_1, x_2) \mapsto \rho_{B_2B_3}^{(x_1x_2)}$ (SWV, 2012)

Relay channel
Relay channel definition

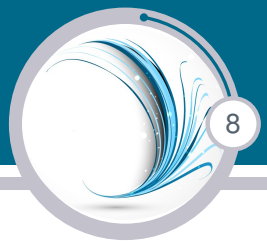


- $\mathcal{N}_{X_1X_2\to B_2B_3} : \mathcal{X}_1 \times \mathcal{X}_2 \to \mathcal{H}_{B_2} \otimes \mathcal{H}_{B_3}, (x_1, x_2) \mapsto \rho_{B_2B_3}^{(x_1x_2)}$ (SWV, 2012)
- Relay's transmission affects relay's system, sender's transmission affects receiver's: More general than concatenated channels!

Relay channel definition
Multihop bound

Quantum generalization of classical protocols

Relay channel definition
Multihop bound



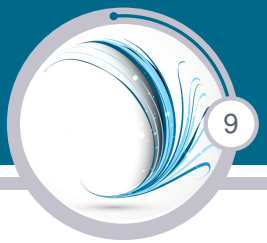
Quantum generalization of classical protocols

- Multihop

Relay channel definition
Multihop bound

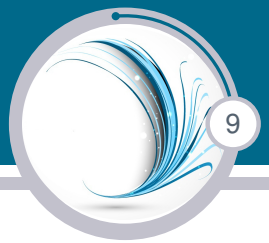
Quantum generalization of classical protocols

- Multihop
  - Treat relay channel as concatenated channel: sender transmits message to relay, relay transmits decoded message to receiver



Random codebook

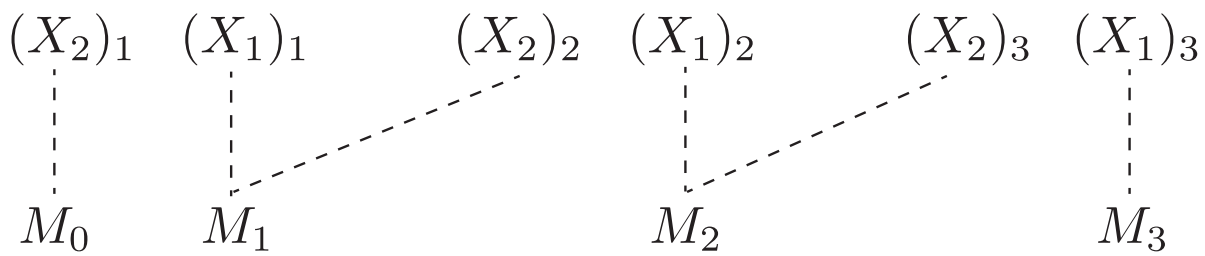
$$C = \bigcup_{j=1}^{b} \{(x_1)_j(m_j), (x_2)_j(m_{j-1})\}_{m_j \in M_j, m_{j-1} \in M_{j-1}}$$



Random codebook

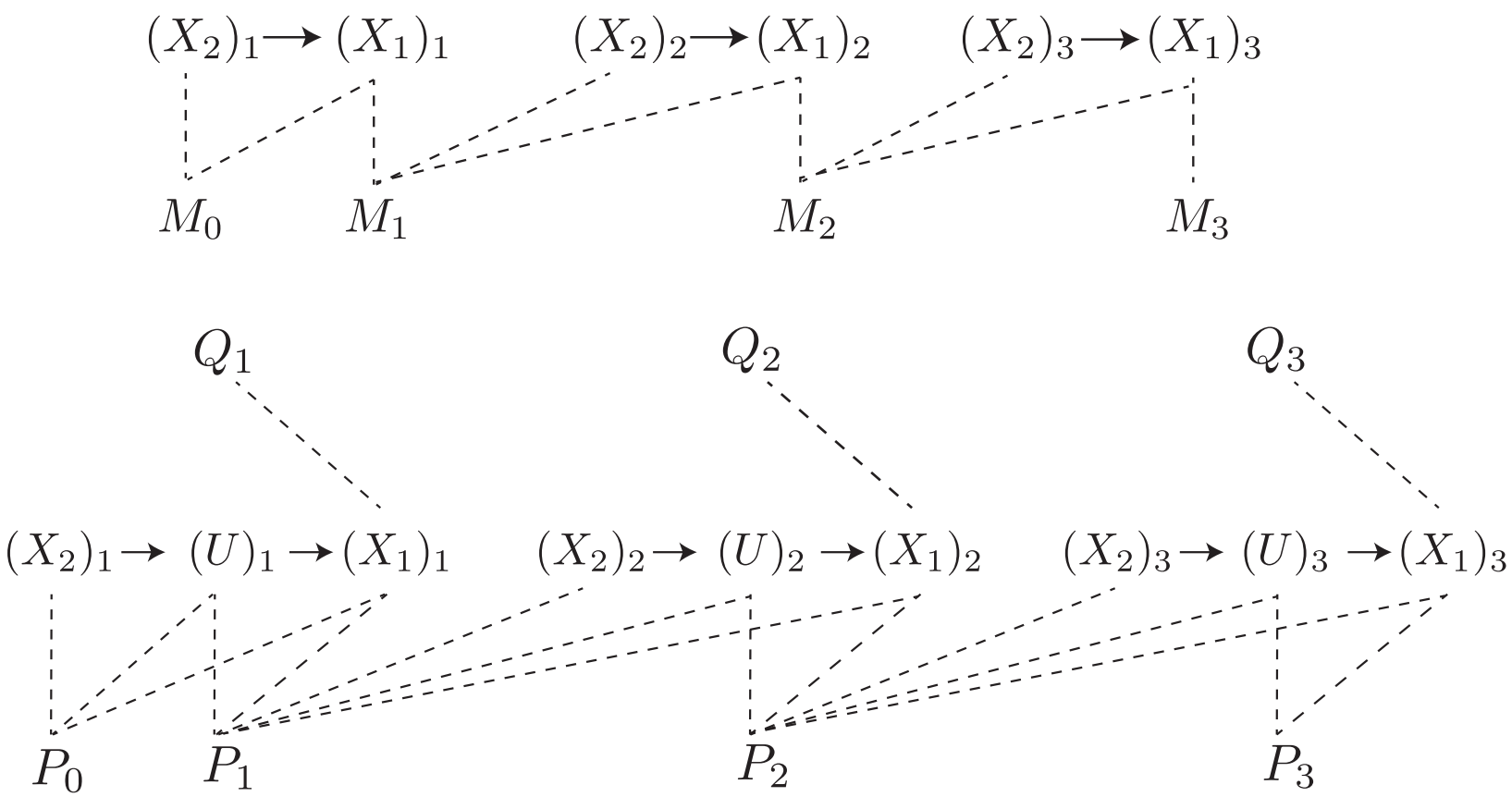
$$C = \bigcup_{j=1}^{b} \{(x_1)_j(m_j), (x_2)_j(m_{j-1})\}_{m_j \in M_j, m_{j-1} \in M_{j-1}}$$

Code:



Relay channel
Remarks

- Coherent multihop, decode forward, partial decode forward



- All straightforward generalizations of classical protocols

Random codebooks for network communication

Quantum multiparty packing lemma
Multiplex Bayesian networks

Random codebooks for network communication

- Has structure depending on network setting and protocol chosen

Quantum multiparty packing lemma
Multiplex Bayesian networks

Random codebooks for network communication

- Has structure depending on network setting and protocol chosen
- How to represent mathematically?

Quantum multiparty packing lemma
Multiplex Bayesian networks

Random codebooks for network communication

- Has structure depending on network setting and protocol chosen
- How to represent mathematically?
  - Muliplex Bayesian network

Quantum multiparty packing lemma
Multiplex Bayesian networks

Detailed definition:

Detailed definition:

- Let X be a Bayesian network with respect to (DAG) $G = (V, E)$

Detailed definition:

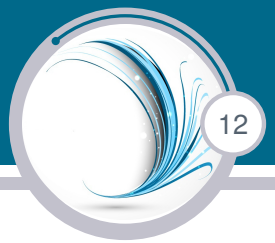
- Let X be a Bayesian network with respect to (DAG) $G = (V, E)$
  - Bayesian network: statistical model that represents a set of random variables and their conditional dependencies via a DAG

Detailed definition:

- Let X be a Bayesian network with respect to (DAG) $G = (V, E)$
  - Bayesian network: statistical model that represents a set of random variables and their conditional dependencies via a DAG
- X composed of X_v for $v \in V$

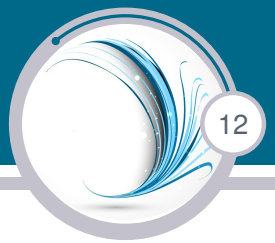
Detailed definition:

- Let X be a Bayesian network with respect to (DAG) $G = (V, E)$
  - Bayesian network: statistical model that represents a set of random variables and their conditional dependencies via a DAG
- X composed of X_v for $v \in V$
- For $v \in V$, let $\mathrm{pa}(v) \equiv \{v' \in V | (v', v) \in E\}$



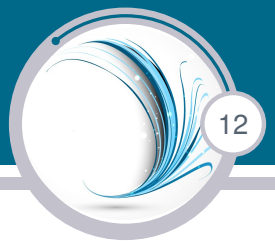
Detailed definition:

- Let X be a Bayesian network with respect to (DAG) $G = (V, E)$
  - Bayesian network: statistical model that represents a set of random variables and their conditional dependencies via a DAG
- X composed of X_v for $v \in V$
- For $v \in V$, let $\mathrm{pa}(v) \equiv \{v' \in V | (v', v) \in E\}$
- Message sets: let J be an index set labeling the multiple message sets



Detailed definition:

- Let X be a Bayesian network with respect to (DAG) $G = (V, E)$
  - Bayesian network: statistical model that represents a set of random variables and their conditional dependencies via a DAG
- X composed of X_v for $v \in V$
- For $v \in V$, let $\text{pa}(v) \equiv \{v' \in V | (v', v) \in E\}$
- Message sets: let J be an index set labeling the multiple message sets
- Let $\text{ind} : V \to \mathcal{P}(J)$ denote the (indices of) the message sets the random variable X_v will be generated over



Detailed definition:

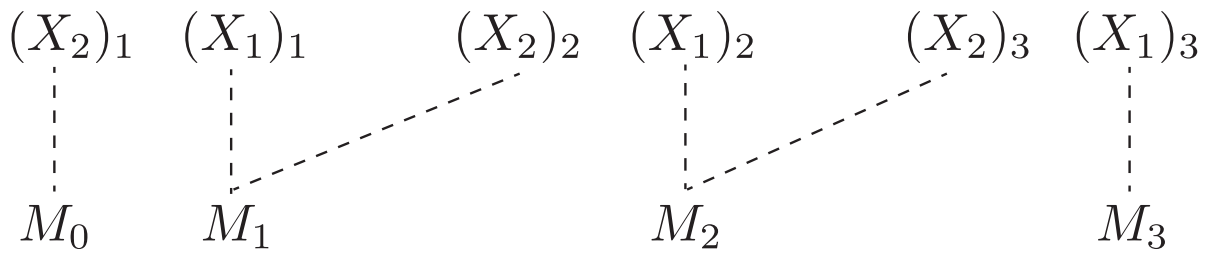
- Let X be a Bayesian network with respect to (DAG) $G = (V, E)$
  - Bayesian network: statistical model that represents a set of random variables and their conditional dependencies via a DAG
- X composed of X_v for $v \in V$
- For $v \in V$, let $\mathrm{pa}(v) \equiv \{v' \in V | (v', v) \in E\}$
- Message sets: let J be an index set labeling the multiple message sets
- Let $\mathrm{ind} : V \to \mathcal{P}(J)$ denote the (indices of) the message sets the random variable X_v will be generated over
  - Index inheritance: For $v \in V$, $\mathrm{ind}(v') \subseteq \mathrm{ind}(v)$ for all $v' \in \mathrm{pa}(v)$

Definition of multiplex Bayesian network

We call the tuple $\mathcal{B} = (G, X, M, \text{ind})$, where $M \equiv \bigtimes_{j \in J} M_j$, a **multiplex Bayesian network**.

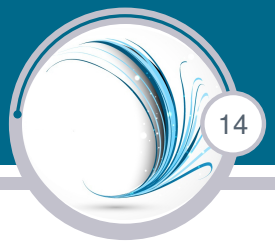
Visualization:

- Adjoin to G additional vertices M_j for each $j \in J$
- Connect with edge X_v to all M_j where $j \in \text{ind}(v)$



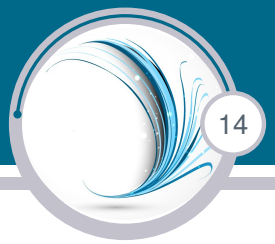
Quantum multiparty packing lemma

Multiplex Bayesian networks



Fixing multiplex Bayesian network (G, X, M, ind), generate a random codebook $\{x_v(m)\}_{v \in V, m \in M}$

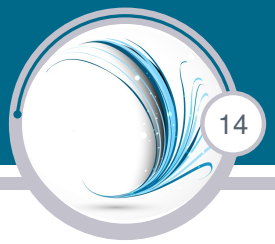
Quantum multiparty packing lemma
Multiplex Bayesian networks



Fixing multiplex Bayesian network (G, X, M, ind), generate a random codebook $\{x_v(m)\}_{v \in V, m \in M}$

- x_v corresponds to vertices of G

Quantum multiparty packing lemma
Multiplex Bayesian networks



Fixing multiplex Bayesian network (G, X, M, ind), generate a random codebook $\{x_v(m)\}_{v \in V, m \in M}$

- x_v corresponds to vertices of G
- M is message set

Quantum multiparty packing lemma
Multiplex Bayesian networks

Fixing multiplex Bayesian network (G, X, M, ind), generate a random codebook $\{x_v(m)\}_{v \in V, m \in M}$

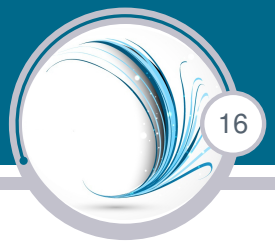
- x_v corresponds to vertices of G
- M is message set
- $x_v(m)$ only depends on m_j where $j \in \text{ind}(v)$

Algorithm for generating random codebook:

for $v \in V$ **do**
  for $m_v \in M_{\mathrm{ind}(v)}$ **do**
    generate $x_v(m_v)$ according to $p_{X_v|X_{\mathrm{pa}(v)}}\left(\cdot|x_{\mathrm{pa}(v)}(m_{\mathrm{pa}(v)})\right)$
    for $m_{\bar{v}} \in M_{\overline{\mathrm{ind}(v)}}$ **do**
      $x_v(m_v, m_{\bar{v}}) = x_v(m_v)$
    end for
  end for
end for

Quantum Multiparty Packing Lemma

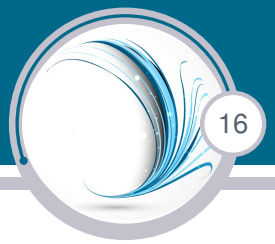
Simultaneous Decoding



- How to find a decoder?

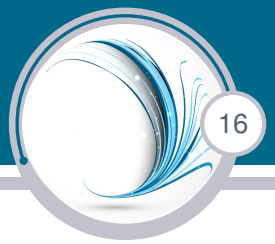
Quantum Multiparty Packing Lemma

Simultaneous Decoding



- How to find a decoder?
- First guess: sequential cancellation decoding

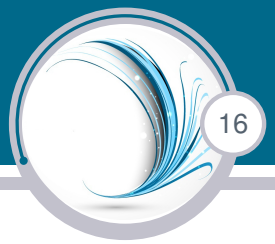
Quantum Multiparty Packing Lemma
Simultaneous Decoding



- How to find a decoder?
- First guess: sequential cancellation decoding
  - Measurement disturbance

Quantum Multiparty Packing Lemma

Simultaneous Decoding



- How to find a decoder?
- First guess: sequential cancellation decoding
  - Measurement disturbance
  - Necessity of time sharing

Quantum Multiparty Packing Lemma
Simultaneous Decoding

- How to find a decoder?
- First guess: sequential cancellation decoding
  - Measurement disturbance
  - Necessity of time sharing
- Simultaneous decoder!

Quantum Multiparty Packing Lemma
Simultaneous Decoding

- How to find a decoder?
- First guess: sequential cancellation decoding
  - Measurement disturbance
  - Necessity of time sharing
- Simultaneous decoder!
  - Needs quantum joint typicality

Quantum Multiparty Packing Lemma

Sen's quantum joint typicality

- Quantum joint typicality

Quantum Multiparty Packing Lemma

Sen's quantum joint typicality

- Quantum joint typicality
  - Long open question

Quantum Multiparty Packing Lemma

Sen's quantum joint typicality

- Quantum joint typicality
  - Long open question
- Recent breakthrough: Pranab Sen, arXiv 1806.0727 "A one-shot quantum joint typicality lemma"
  - [Insert complicated equations here.]

Quantum Multiparty Packing Lemma

Sen's quantum joint typicality

- Quantum joint typicality
  - Long open question
- Recent breakthrough: Pranab Sen, arXiv 1806.0727 "A one-shot quantum joint typicality lemma"
  - [Insert complicated equations here.]

Typicality $\Longleftrightarrow$ Packing lemma $\Longleftrightarrow$ Capacity theorem

Quantum multiparty packing lemma
Packing lemma statement

- Let C be codebook generated by multiplex Bayesian network

Quantum multiparty packing lemma

Packing lemma statement

- Let C be codebook generated by multiplex Bayesian network
- Let $\{\rho_B^{(x)}\}_{x\in\mathcal{X}}$ be family of quantum states

Quantum multiparty packing lemma
Packing lemma statement

- Let C be codebook generated by multiplex Bayesian network
- Let $\{\rho_B^{(x)}\}_{x\in\mathcal{X}}$ be family of quantum states
  - Defines the black box

Quantum multiparty packing lemma

Packing lemma statement

- Let C be codebook generated by multiplex Bayesian network
- Let $\{\rho_B^{(x)}\}_{x\in\mathcal{X}}$ be family of quantum states
  - Defines the black box
- Let $D \subseteq J$ be subset of messages to be decoded, $\overline{D}$ be guess for other messages

Asymptotic quantum multiparty packing lemma (simplified)

Let $\mathcal{B} = (G, X, M, \text{ind})$, $C^n = \{x^n(m)\}_{m \in M}$, $\{\rho_B^{(x)}\}_{x \in \mathcal{X}}$, $D \subseteq J$, and $\varepsilon \in (0, 1)$.

Then there exists a POVM $\{Q_B^{(m_D|m_{\overline{D}})}\}_{m_D \in M_D}$ for each $m_{\overline{D}} \in M_{\overline{D}}$ that, assuming the guess was right, can decode $(m_D, m_{\overline{D}}) \in M$ encoded into $\bigotimes_{i=1}^n \rho_{B_i}^{(x_i(m_D, m_{\overline{D}}))}$ with vanishing probability of error as $n \to \infty$ if

$$\forall\, \emptyset \neq T \subseteq D, \quad \sum_{t \in T} R_t < I(X_{S_T}; B|X_{\overline{S_T}})_\rho,$$

where $R_t \equiv \log |M_t|$, $S_T \equiv \{v \in V \mid \text{ind}(v) \cap T \neq \emptyset\} \subseteq V$,

$$\rho_{XB} \equiv \sum_{x \in \mathcal{X}} p_X(x) |x\rangle \langle x|_X \otimes \rho_B^{(x)}.$$

Conclusion
Summary

- Established a one-shot quantum multiparty packing lemma

Conclusion
Summary

- Established a one-shot quantum multiparty packing lemma
  - Multiplex Bayesian networks

Conclusion
Summary

- Established a one-shot quantum multiparty packing lemma
  - Multiplex Bayesian networks
  - Cornerstone of classical network information theory is packing lemma

Conclusion
Summary

- Established a one-shot quantum multiparty packing lemma
  - Multiplex Bayesian networks
  - Cornerstone of classical network information theory is packing lemma
  - Allows hitherto impossible direct quantum generalization

Conclusion
Summary

- Established a one-shot quantum multiparty packing lemma
  - Multiplex Bayesian networks
  - Cornerstone of classical network information theory is packing lemma
  - Allows hitherto impossible direct quantum generalization
- Demonstrated direct quantum generalization for classical-quantum relay channel

Conclusion
Summary

- Established a one-shot quantum multiparty packing lemma
  - Multiplex Bayesian networks
  - Cornerstone of classical network information theory is packing lemma
  - Allows hitherto impossible direct quantum generalization
- Demonstrated direct quantum generalization for classical-quantum relay channel
  - Multihop
  - Cohere multihop
  - Decode forward
  - Partial decode forward

Conclusion
Open questions

Open questions and future work:

Conclusion
Open questions

Open questions and future work:

- Apply packing lemma to other settings?

Conclusion
Open questions

Open questions and future work:

- Apply packing lemma to other settings?
- Other notions of joint typicality?

Conclusion
Open questions

Open questions and future work:

- Apply packing lemma to other settings?
- Other notions of joint typicality?
- Rate region simplification?

Conclusion
Open questions

Open questions and future work:

- Apply packing lemma to other settings?
- Other notions of joint typicality?
- Rate region simplification?
- More general packing lemma?

Thank you!

Lemma (Classical packing lemma)

Let (U, X, Y) be a triple of random variables with joint distribution p_{UXY}. For each n, let $(\widetilde{U}^n, \widetilde{Y}^n)$ be a pair of arbitrarily distributed random sequences and $\{\widetilde{X}^n(m)\}$ a family of at most 2^{nR} random sequences such that each $\widetilde{X}^n(m)$ is conditionally independent of $\widetilde{Y}^n$ given $\widetilde{U}^n$. Further assume that each $\widetilde{X}^n(m)$ is distributed as $\otimes_{i=1}^n p_{X|U=\widetilde{U}_i}$ given $\widetilde{U}^n$. Then, there exists $\delta(\varepsilon)$ that tends to zero as $\varepsilon \to 0$ such that

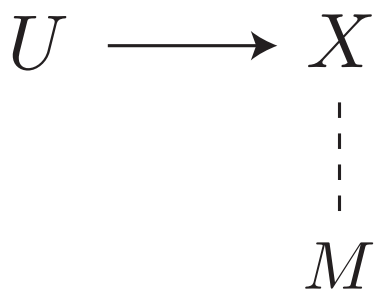
$$\lim_{n\to\infty} \Pr((\widetilde{U}^n, \widetilde{X}^n(m), \widetilde{Y}^n) \in \mathcal{T}_\varepsilon^{(n)} \text{ for some } m) = 0$$

if $R < I(X; Y|U) - \delta(\varepsilon)$, where $\mathcal{T}_\varepsilon^{(n)}$ is the set of ε-typical strings of length n with respect to p_{UXY}.

Usual channel coding follows from $U = \emptyset$ and $\widetilde{Y}^n \sim p_Y^{\otimes n}$.

Backup
Reduction to classical packing lemma

i.i.d. version of classical packing lemma is a corollary of our quantum multiparty packing lemma.



- Run algorithm n times, codebook generated is $\widetilde{U}^n, \widetilde{X}^n(m)$
- Set of quantum states
  $\left\{\rho_{\widetilde{Y}}^{(u,x)} \equiv \sum_{\widetilde{y}\in\mathcal{Y}} p_{Y|UX}(\widetilde{y}|u,x)\,|\widetilde{y}\rangle\,\langle\widetilde{y}|_{\widetilde{Y}}\right\}_{u\in\mathcal{U},x\in\mathcal{X}}$
- "Typicality test" POVM $\left\{Q_{\widetilde{Y}^n}^{(m)}\right\}_{m\in M}$

Backup

Sen's quantum joint typicality lemma (baby version)

Let $B_1 \dots B_k$ be a k-partite quantum system with each B_i isomorphic to a Hilbert space $\mathcal{H}$. Let $\rho_{B_1 \dots B_k}$ be a quantum state in $B_1 \dots B_k$. For a subset $S \subseteq [k]$, let B_S denote the systems $\{B_s : s \in S\}$. Let ρ_{B_S} denote the marginal state on B_S obtained by tracing out the systems in $\bar{S} := [k] \setminus S$ from $\rho_{B_1 \dots B_k}$. Let $0 < \epsilon < 1$. Let $\mathcal{K}$ be a Hilbert space of dimension $d_{\mathcal{K}}$ There exist a state $\tau_{\mathcal{K} \otimes [k]}$ independent of $\rho_{B_{[k]}}$, a state $(\rho')_{B'_{[k]}}$, and a POVM element $\Pi'_{B'_{[k]}}$ on $B'_1 \dots B'_k$ where $B'_i \cong B_i \otimes \mathcal{K}$, with the following properties:

1. $\|(\rho')_{B'_{[k]}} - \rho_{B_{[k]}} \otimes \tau_{\mathcal{K} \otimes [k]}\|_1 \leq f(k, \varepsilon)$;
2. $\mathrm{tr}[(\Pi')_{B'_{[k]}} (\rho')_{B'_{[k]}}] \geq 1 - g(k, \varepsilon)$;
3. For every set S, $\{\} \neq S \subset [k]$,

$$\mathrm{tr}[(\Pi')_{B'_{[k]}} ((\rho')_{B'_S} \otimes (\rho')_{B'_{\bar{S}}})] \leq 2^{-D_H^{\epsilon}(\rho_{B_{[k]}} \| \rho_{B_S} \otimes \rho_{B_{\bar{S}}}) \cdot + h(k, d_{\mathcal{H}}, d_{\mathcal{K}})}$$

From Pranab Sen, "A one-shot quantum joint typicality lemma"