Title: Information Theoretic Benefit of Entanglement in Classical Communication Settings

Date: May 27, 2013 04:00 PM

URL: http://pirsa.org/13050077

Abstract: Expressions of several information theoretic quantities involve an optimization over auxiliary quantum registers. Entanglement-assisted version of some classical communication problems provides examples of such expressions. Evaluating these expressions requires bounds on the dimension of these auxiliary registers. In the classical case such a bound can usually be obtained based on the
Caratheodory theorem, but we know almost no method to bound the dimension of auxiliary quantum registers. In this talk to compare the classical and quantum sides of the problem the notion of â€œquantum convexificationâ€• will be defined. It will be shown that quantum convexification is strictly richer that the usual classical convexification. Moreover some techniques will be discussed which might be useful for bounding the dimension of quantum auxiliary registers.

Information Theoretic Benefit of Entanglement in Classical Communication Settings

Salman Beigi

Institute for Research in Fundamental Sciences (IPM), Tehran, Iran

May, 2013

Joint work with

Amin Gohari

Sharif University of Technology, Tehran, Iran

Optimizations over auxiliar quantum systems

- [Christandl, Winter '04] Squashed entanglement: given ρ_{AB}

$$E_{\mathrm{sq}}(\rho_{AB}) = \frac{1}{2} \inf_{\rho_{ABC}} I(A;B|C)$$

$H(\rho) = -\mathrm{tr}(\rho \log \rho)$: von Neumann entropy,
$H(A|B) = H(AB) - H(B)$
$I(A;B|C) = H(A|C) + H(B|C) - H(AB|C)$

Optimizations over auxiliar quantum systems

- [Christandl, Winter '04] Squashed entanglement: given ρ_{AB}

$$E_{\text{sq}}(\rho_{AB}) = \frac{1}{2} \inf_{\rho_{ABC}} I(A;B|C)$$

$H(\rho) = -\text{tr}(\rho \log \rho)$: von Neumann entropy,
$H(A|B) = H(AB) - H(B)$
$I(A;B|C) = H(A|C) + H(B|C) - H(AB|C)$

- [Bennett et al '02] Entangling capacity of a bipartite unitary
- [Smith et al '08] Quantum channel capacity assisted with symmetric side channels

Optimizations over auxiliar quantum systems

- [Christandl, Winter '04] Squashed entanglement: given ρ_{AB}

$$E_{\text{sq}}(\rho_{AB}) = \frac{1}{2} \inf_{\rho_{ABC}} I(A;B|C)$$

$H(\rho) = -\text{tr}(\rho \log \rho)$: von Neumann entropy,
$H(A|B) = H(AB) - H(B)$
$I(A;B|C) = H(A|C) + H(B|C) - H(AB|C)$

- [Bennett et al '02] Entangling capacity of a bipartite unitary
- [Smith et al '08] Quantum channel capacity assisted with symmetric side channels

Optimizations over auxiliar quantum systems

- [Christandl, Winter '04] Squashed entanglement: given ρ_{AB}

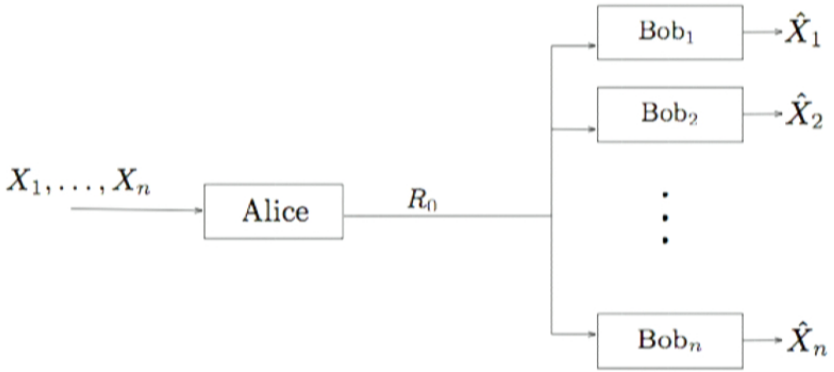
$$E_{\mathrm{sq}}(\rho_{AB}) = \frac{1}{2} \inf_{\rho_{ABC}} I(A;B|C)$$

$H(\rho) = -\mathrm{tr}(\rho \log \rho)$: von Neumann entropy,
$H(A|B) = H(AB) - H(B)$
$I(A;B|C) = H(A|C) + H(B|C) - H(AB|C)$

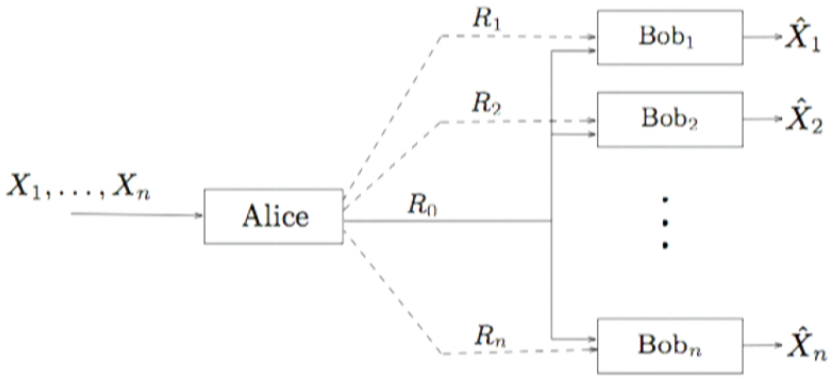
- [Bennett et al '02] Entangling capacity of a bipartite unitary
- [Smith et al '08] Quantum channel capacity assisted with symmetric side channels

- Entanglement-assisted Gray-Wynner problem

The Gray-Wyner problem

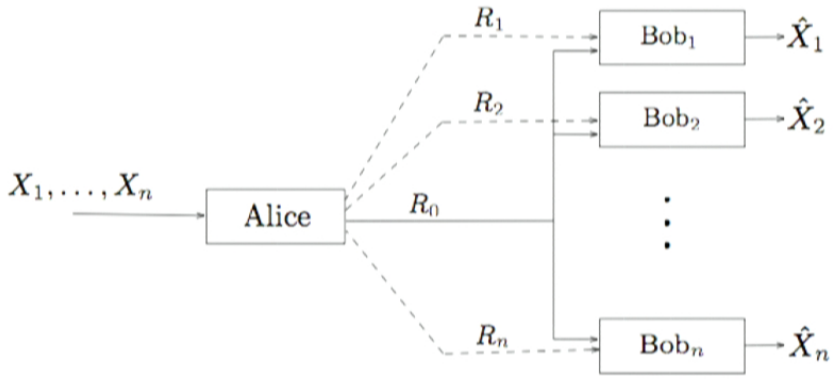


The Gray-Wyner problem



- Public message at rate R_0 to all Bobs
- Private message at rate R_j to Bob$_j$
- The goal of Bob$_j$ is to recover X_j

The Gray-Wyner problem



- Public message at rate R_0 to all Bobs
- Private message at rate R_j to Bob_j
- The goal of Bob_j is to recover X_j

Theorem [Gray, Wyner '74]: $(R_0, R_1, \ldots, R_n)$ is achievable iff $\exists\ C$ s.t.

$$R_0 \geq I(X_1 \ldots X_n; C) \qquad \& \qquad R_j \geq H(X_j|C)$$

The Gray-Wyner problem

Question: What if the sender and receivers share entanglement?

Theorem [Winter '12]: $(R_0, R_1, \ldots, R_n)$ is achievable iff $\exists\, Q_1, \ldots, Q_n$ s.t.

$$R_0 \geq I(X_1 \ldots X_n; Q_1 \ldots Q_n) \qquad \& \qquad R_j \geq H(X_j|Q_j)$$

The Gray-Wyner problem

Question: What if the sender and receivers share entanglement?

Theorem [Winter '12]: $(R_0, R_1, \ldots, R_n)$ is achievable iff $\exists\, Q_1, \ldots, Q_n$ s.t.

$$R_0 \geq I(X_1 \ldots X_n; Q_1 \ldots Q_n) \qquad \& \qquad R_j \geq H(X_j|Q_j)$$

- Does entanglement help?
- Entanglement does not increase the capacity of point-to-point classical channels.

The Gray-Wyner problem

Question: What if the sender and receivers share entanglement?

Theorem [Winter '12]: $(R_0, R_1, \ldots, R_n)$ is achievable iff $\exists\, Q_1, \ldots, Q_n$ s.t.

$$R_0 \geq I(X_1 \ldots X_n; Q_1 \ldots Q_n) \qquad \& \qquad R_j \geq H(X_j|Q_j)$$

- Does entanglement help?
- Entanglement does not increase the capacity of point-to-point classical channels.
- Given $X_1, \ldots, X_n$ and auxiliary quantum Q does there exists auxiliary classical C s.t.

$$\big(I(X_1 \ldots X_n; Q), H(X_1|Q), \ldots, H(X_n|Q)\big)$$

$$= \big(I(X_1 \ldots X_n; C), H(X_1|C), \ldots, H(X_n|C)\big)$$

Another example

- Let X, Y, Z be (classical) with a given distribution.
- Compute

$$\sup_{C-X-YZ} I(C;Y) - I(C;Z)$$

$E - F - G$ means $I(E;G|F) = 0$

Another example

- Let X, Y, Z be (classical) with a given distribution.

- Compute

$$\sup_{C-X-YZ} I(C;Y) - I(C;Z)$$

$E - F - G$ means $I(E;G|F) = 0$

Claim: WLOG we may assume $|\mathcal{C}|$ is bounded

Proof: $I(C;Y) - I(C;Z) = H(Y) - H(Z) + H(Z|C) - H(Y|C)$

$H(Y|C) = \sum_{c \in \mathcal{C}} p(c) H(Y|C=c)$

Use Caratheodory theorem: every point in ConvHull$(\mathcal{S})$ where $\mathcal{S} \subseteq \mathbb{R}^n$ can be written as a convex combination of at most $n+1$ points of $\mathcal{S}$.

Another example

- Let X, Y, Z be (classical) with a given distribution.

- Compute

$$\sup_{C-X-YZ} I(C;Y) - I(C;Z)$$

$E - F - G$ means $I(E;G|F) = 0$

Claim: WLOG we may assume $|\mathcal{C}|$ is bounded

Proof: $I(C;Y) - I(C;Z) = H(Y) - H(Z) + H(Z|C) - H(Y|C)$

$H(Y|C) = \sum_{c \in \mathcal{C}} p(c) H(Y|C=c)$

Use Caratheodory theorem: every point in ConvHull$(\mathcal{S})$ where $\mathcal{S} \subseteq \mathbb{R}^n$ can be written as a convex combination of at most $n+1$ points of $\mathcal{S}$.

Another example

- Let X, Y, Z be (classical) with a given distribution.

- Compute

$$\sup_{C-X-YZ} I(C;Y) - I(C;Z)$$

$E - F - G$ means $I(E;G|F) = 0$

Claim: WLOG we may assume $|\mathcal{C}|$ is bounded

Proof: $I(C;Y) - I(C;Z) = H(Y) - H(Z) + H(Z|C) - H(Y|C)$

$H(Y|C) = \sum_{c \in \mathcal{C}} p(c) H(Y|C=c)$

Use Caratheodory theorem: every point in ConvHull$(\mathcal{S})$ where $\mathcal{S} \subseteq \mathbb{R}^n$ can be written as a convex combination of at most $n+1$ points of $\mathcal{S}$.

Question: What happens if we take C to be quantum?

What we like...

- Compute regions defined by conditioning on a quantum auxiliary register
- Conditioning on quantum auxiliary registers vs auxiliary random variables
- Is entanglement ever helpful in a classical communication setting?

Convexification

- Let $\mathcal{X}_1, \ldots, \mathcal{X}_n$ be finite sets. Consider the set of distributions $p(x_1, \ldots, x_n)$ on $\mathcal{X}_1 \times \cdots \times \mathcal{X}_n$
- Consider the maps $p(x_1, \ldots, x_n) \mapsto (H(X_1), \ldots, H(X_n))$.

Convexification

- Let $\mathcal{X}_1, \ldots, \mathcal{X}_n$ be finite sets. Consider the set of distributions $p(x_1, \ldots, x_n)$ on $\mathcal{X}_1 \times \cdots \times \mathcal{X}_n$
- Consider the maps $p(x_1, \ldots, x_n) \mapsto (H(X_1), \ldots, H(X_n))$.
- $\mathcal{G}$ the graph of this maps consists of tuples

$$\big(p(x_1, \ldots, x_n), H(X_1), \ldots, H(X_n)\big)$$

Convexification

- Let $\mathcal{X}_1, \ldots, \mathcal{X}_n$ be finite sets. Consider the set of distributions $p(x_1, \ldots, x_n)$ on $\mathcal{X}_1 \times \cdots \times \mathcal{X}_n$
- Consider the maps $p(x_1, \ldots, x_n) \mapsto (H(X_1), \ldots, H(X_n))$.
- $\mathcal{G}$ the graph of this maps consists of tuples

$$\big(p(x_1, \ldots, x_n), H(X_1), \ldots, H(X_n)\big)$$

- ConvHull$(\mathcal{G})$ consists of all tuples

$$\big(p(x_1, \ldots, x_n), H(X_1|C), \ldots, H(X_n|C)\big), \qquad \forall p(x_1, \ldots, x_n, c)$$

- ConvHull$(\mathcal{G})$ is computable (have a bound on $|\mathcal{C}|$)

Convexification

- Let $\mathcal{X}_1, \ldots, \mathcal{X}_n$ be finite sets. Consider the set of distributions $p(x_1, \ldots, x_n)$ on $\mathcal{X}_1 \times \cdots \times \mathcal{X}_n$
- Consider the maps $p(x_1, \ldots, x_n) \mapsto (H(X_1), \ldots, H(X_n))$.
- $\mathcal{G}$ the graph of this maps consists of tuples

$$\big(p(x_1, \ldots, x_n), H(X_1), \ldots, H(X_n)\big)$$

- ConvHull$(\mathcal{G})$ consists of all tuples

$$\big(p(x_1, \ldots, x_n), H(X_1|C), \ldots, H(X_n|C)\big), \qquad \forall p(x_1, \ldots, x_n, c)$$

- ConvHull$(\mathcal{G})$ is computable (have a bound on $|\mathcal{C}|$)

Convexification

- Let $\mathcal{X}_1, \ldots, \mathcal{X}_n$ be finite sets. Consider the set of distributions $p(x_1, \ldots, x_n)$ on $\mathcal{X}_1 \times \cdots \times \mathcal{X}_n$
- Consider the maps $p(x_1, \ldots, x_n) \mapsto (H(X_1), \ldots, H(X_n))$.
- $\mathcal{G}$ the graph of this maps consists of tuples

$$\big(p(x_1, \ldots, x_n), H(X_1), \ldots, H(X_n)\big)$$

- ConvHull$(\mathcal{G})$ consists of all tuples

$$\big(p(x_1, \ldots, x_n), H(X_1|C), \ldots, H(X_n|C)\big), \qquad \forall p(x_1, \ldots, x_n, c)$$

- ConvHull$(\mathcal{G})$ is computable (have a bound on $|\mathcal{C}|$)
- Define QConvHull$(\mathcal{G})$ to be the set of points

$$\big(p(x_1, \ldots, x_n), H(X_1|Q), \ldots, H(X_n|Q)\big), \qquad \forall p(x_1, \ldots, x_n), \rho^{Q}_{x_1 \ldots x_n}$$

Question: Is the inclusion ConvHull$(\mathcal{G}) \subseteq$ QConvHull$(\mathcal{G})$ strict or not?

Main Result (1)

Theorem: The followings are equivalent

(1) $\mathrm{QConvHull}(\mathcal{G}) = \mathrm{ConvHull}(\mathcal{G})$.

Main Result (1)

Theorem: The followings are equivalent

(1) $\mathrm{QConvHull}(\mathcal{G}) = \mathrm{ConvHull}(\mathcal{G})$.

(2) For any $p(x, y, z)$ consider the optimization problem

$$\sup_{\mathbf{Q}-X-YZ} I(\mathbf{Q}; Y) - I(\mathbf{Q}; Z).$$

Then the supremum is attained at a classical $\mathbf{Q}$.

Main Result (1)

Theorem: The followings are equivalent

(1) $\mathrm{QConvHull}(\mathcal{G}) = \mathrm{ConvHull}(\mathcal{G})$.

(2) For any $p(x, y, z)$ consider the optimization problem

$$\sup_{\mathbf{Q}-X-YZ} I(\mathbf{Q}; Y) - I(\mathbf{Q}; Z).$$

Then the supremum is attained at a classical $\mathbf{Q}$.

(3) For a c-q channel $X \to Q$, consider the function $p(x) \mapsto I(X; \mathbf{Q})$. Then for every $\epsilon > 0$ there exists a c-c channel $X \to C$ such that $\left|I(X; \mathbf{Q}) - I(X; C)\right| \leq \epsilon$ for all $p(x)$.

Main Result (1)

Theorem: The followings are equivalent

(1) $\mathrm{QConvHull}(\mathcal{G}) = \mathrm{ConvHull}(\mathcal{G})$.

(2) For any $p(x, y, z)$ consider the optimization problem

$$\sup_{\mathbf{Q}-X-YZ} I(\mathbf{Q}; Y) - I(\mathbf{Q}; Z).$$

Then the supremum is attained at a classical $\mathbf{Q}$.

(3) For a c-q channel $X \to Q$, consider the function $p(x) \mapsto I(X; \mathbf{Q})$. Then for every $\epsilon > 0$ there exists a c-c channel $X \to C$ such that $\left|I(X; \mathbf{Q}) - I(X; C)\right| \leq \epsilon$ for all $p(x)$.

Main Result (1)

Theorem: The followings are equivalent

(1) $\mathrm{QConvHull}(\mathcal{G}) = \mathrm{ConvHull}(\mathcal{G})$.

(2) For any $p(x, y, z)$ consider the optimization problem

$$\sup_{\mathbf{Q}-X-YZ} I(\mathbf{Q}; Y) - I(\mathbf{Q}; Z).$$

Then the supremum is attained at a classical $\mathbf{Q}$.

(3) For a c-q channel $X \to Q$, consider the function $p(x) \mapsto I(X; \mathbf{Q})$. Then for every $\epsilon > 0$ there exists a c-c channel $X \to C$ such that $\left|I(X; \mathbf{Q}) - I(X; C)\right| \leq \epsilon$ for all $p(x)$.

Proof: (1) $\Rightarrow$ (2) is immediate.

Main Result (1)

Theorem: The followings are equivalent

(1) $\mathrm{QConvHull}(\mathcal{G}) = \mathrm{ConvHull}(\mathcal{G})$.

(2) For any $p(x,y,z)$ consider the optimization problem

$$\sup_{\mathbf{Q}-X-YZ} I(\mathbf{Q};Y) - I(\mathbf{Q};Z).$$

Then the supremum is attained at a classical $\mathbf{Q}$.

(3) For a c-q channel $X \to Q$, consider the function $p(x) \mapsto I(X;\mathbf{Q})$. Then for every $\epsilon > 0$ there exists a c-c channel $X \to C$ such that $\left|I(X;\mathbf{Q}) - I(X;C)\right| \leq \epsilon$ for all $p(x)$.

Proof: (1) $\Rightarrow$ (2) is immediate.

(3) $\Rightarrow$ (1): Let

$$\left(p(x_1,\ldots,x_n), H(X_1|\mathbf{Q}),\ldots,H(X_n|\mathbf{Q})\right) \in \mathrm{QConvHull}(\mathcal{G})$$

Define $X = X_1 \ldots X_n$, consider $X \to \mathbf{Q}$ as a channel, and then use (3).

Proof of (2) $\Rightarrow$ (3)

Fix a channel $X \to \mathbf{Q}$, and a distribution $p(x)$ on X.

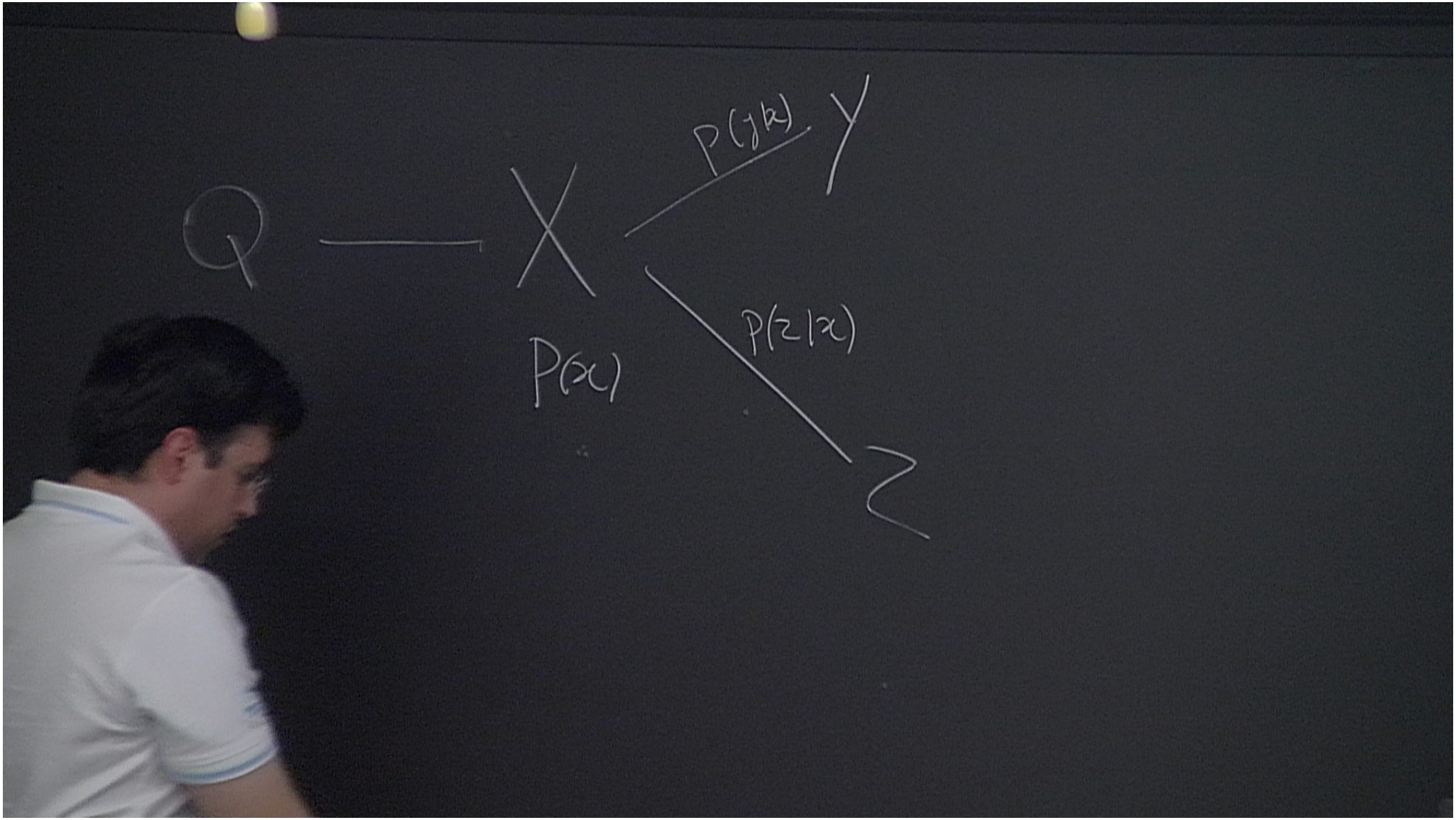
$$I(\mathbf{Q}; Y) - I(\mathbf{Q}; Z) \leq \max_{p(c|x)} I(C; Y) - I(C; Z), \quad \forall p(y|x), p(z|x).$$

Proof of (2) $\Rightarrow$ (3)

Fix a channel $X \to \mathbf{Q}$, and a distribution $p(x)$ on X.

$$I(\mathbf{Q};Y) - I(\mathbf{Q};Z) \leq \max_{p(c|x)} I(C;Y) - I(C;Z), \quad \forall p(y|x), p(z|x).$$

$$\max_{p(y|x),p(z|x)} \left[I(\mathbf{Q};Y) - I(\mathbf{Q};Z) - \max_{p(c|x)} I(C;Y) - I(C;Z) \right] \leq 0.$$


Q
X
P(y|x)
Y
P(x)
P(z|x)
Z

Proof of (2) $\Rightarrow$ (3)

Fix a channel $X \to \mathbf{Q}$, and a distribution $p(x)$ on X.

$$I(\mathbf{Q};Y) - I(\mathbf{Q};Z) \leq \max_{p(c|x)} I(C;Y) - I(C;Z), \quad \forall p(y|x), p(z|x).$$

$$\max_{p(y|x),p(z|x)} \left[I(\mathbf{Q};Y) - I(\mathbf{Q};Z) - \max_{p(c|x)} I(C;Y) - I(C;Z) \right] \leq 0.$$

Take an ϵ-net of channels $\{X \to C_m\}$

$$\max_{p(y|x),p(z|x)} \left[I(\mathbf{Q};Y) - I(\mathbf{Q};Z) - \max_{1 \leq m \leq M_\epsilon} I(C_m;Y) - I(C_m;Z) \right] \leq \epsilon.$$

$$\max_{p(y|x),p(z|x)} \left[I(\mathbf{Q};Y) - I(\mathbf{Q};Z) - \max_{\sum_m \lambda_m = 1} \sum_m \lambda_m \big(I(C_m;Y) - I(C_m;Z) \big) \right] \leq \epsilon.$$

Proof of (2) $\Rightarrow$ (3)

Fix a channel $X \to \mathbf{Q}$, and a distribution $p(x)$ on X.

$$I(\mathbf{Q};Y) - I(\mathbf{Q};Z) \leq \max_{p(c|x)} I(C;Y) - I(C;Z), \quad \forall p(y|x), p(z|x).$$

$$\max_{p(y|x),p(z|x)} \left[I(\mathbf{Q};Y) - I(\mathbf{Q};Z) - \max_{p(c|x)} I(C;Y) - I(C;Z) \right] \leq 0.$$

Take an ϵ-net of channels $\{X \to C_m\}$

$$\max_{p(y|x),p(z|x)} \left[I(\mathbf{Q};Y) - I(\mathbf{Q};Z) - \max_{1 \leq m \leq M_\epsilon} I(C_m;Y) - I(C_m;Z) \right] \leq \epsilon.$$

$$\max_{p(y|x),p(z|x)} \left[I(\mathbf{Q};Y) - I(\mathbf{Q};Z) - \max_{\sum_m \lambda_m = 1} \sum_m \lambda_m \big(I(C_m;Y) - I(C_m;Z) \big) \right] \leq \epsilon.$$

Proof of (2) $\Rightarrow$ (3)

$$\max_{p(y|x),p(z|x)} \min_{\lambda_m} \left[I(\mathbf{Q};Y) - I(\mathbf{Q};Z) - \sum_m \lambda_m \big(I(C_m;Y) - I(C_m;Z) \big) \right] \leq \epsilon$$

Proof of (2) $\Rightarrow$ (3)

$$\max_{p(y|x),p(z|x)} \min_{\lambda_m} \left[I(\mathbf{Q};Y) - I(\mathbf{Q};Z) - \sum_m \lambda_m \big(I(C_m;Y) - I(C_m;Z) \big) \right] \leq \epsilon$$

Proof of (2) $\Rightarrow$ (3)

$$\max_{p(y|x),p(z|x)} \min_{\lambda_m} \left[I(\mathbf{Q};Y) - I(\mathbf{Q};Z) - \sum_m \lambda_m \big(I(C_m;Y) - I(C_m;Z) \big) \right] \leq \epsilon$$

By the minimax theorem $\exists \lambda_m$ such that

$$\max_{p(y|x),p(z|x)} \left[I(\mathbf{Q};Y) - I(\mathbf{Q};Z) - \sum_m \lambda_m \big(I(C_m;Y) - I(C_m;Z) \big) \right] \leq \epsilon$$

Proof of (2) $\Rightarrow$ (3)

$$\max_{p(y|x),p(z|x)} \min_{\lambda_m} \left[I(\mathbf{Q};Y) - I(\mathbf{Q};Z) - \sum_m \lambda_m \big(I(C_m;Y) - I(C_m;Z) \big) \right] \leq \epsilon$$

By the minimax theorem $\exists \lambda_m$ such that

$$\max_{p(y|x),p(z|x)} \left[I(\mathbf{Q};Y) - I(\mathbf{Q};Z) - \sum_m \lambda_m \big(I(C_m;Y) - I(C_m;Z) \big) \right] \leq \epsilon$$

$$\max_{p(y|x),p(z|x)} \left[H(\mathbf{Q}|Z) - H(\mathbf{Q}|Y) - \sum_m \lambda_m \big(H(C_m|Z) - H(C_m|Y) \big) \right] \leq \epsilon$$

Proof of (2) $\Rightarrow$ (3)

$$\max_{p(y|x),p(z|x)} \min_{\lambda_m} \left[I(\mathbf{Q};Y) - I(\mathbf{Q};Z) - \sum_m \lambda_m \big(I(C_m;Y) - I(C_m;Z) \big) \right] \leq \epsilon$$

By the minimax theorem $\exists \lambda_m$ such that

$$\max_{p(y|x),p(z|x)} \left[I(\mathbf{Q};Y) - I(\mathbf{Q};Z) - \sum_m \lambda_m \big(I(C_m;Y) - I(C_m;Z) \big) \right] \leq \epsilon$$

$$\max_{p(y|x),p(z|x)} \left[H(\mathbf{Q}|Z) - H(\mathbf{Q}|Y) - \sum_m \lambda_m \big(H(C_m|Z) - H(C_m|Y) \big) \right] \leq \epsilon$$

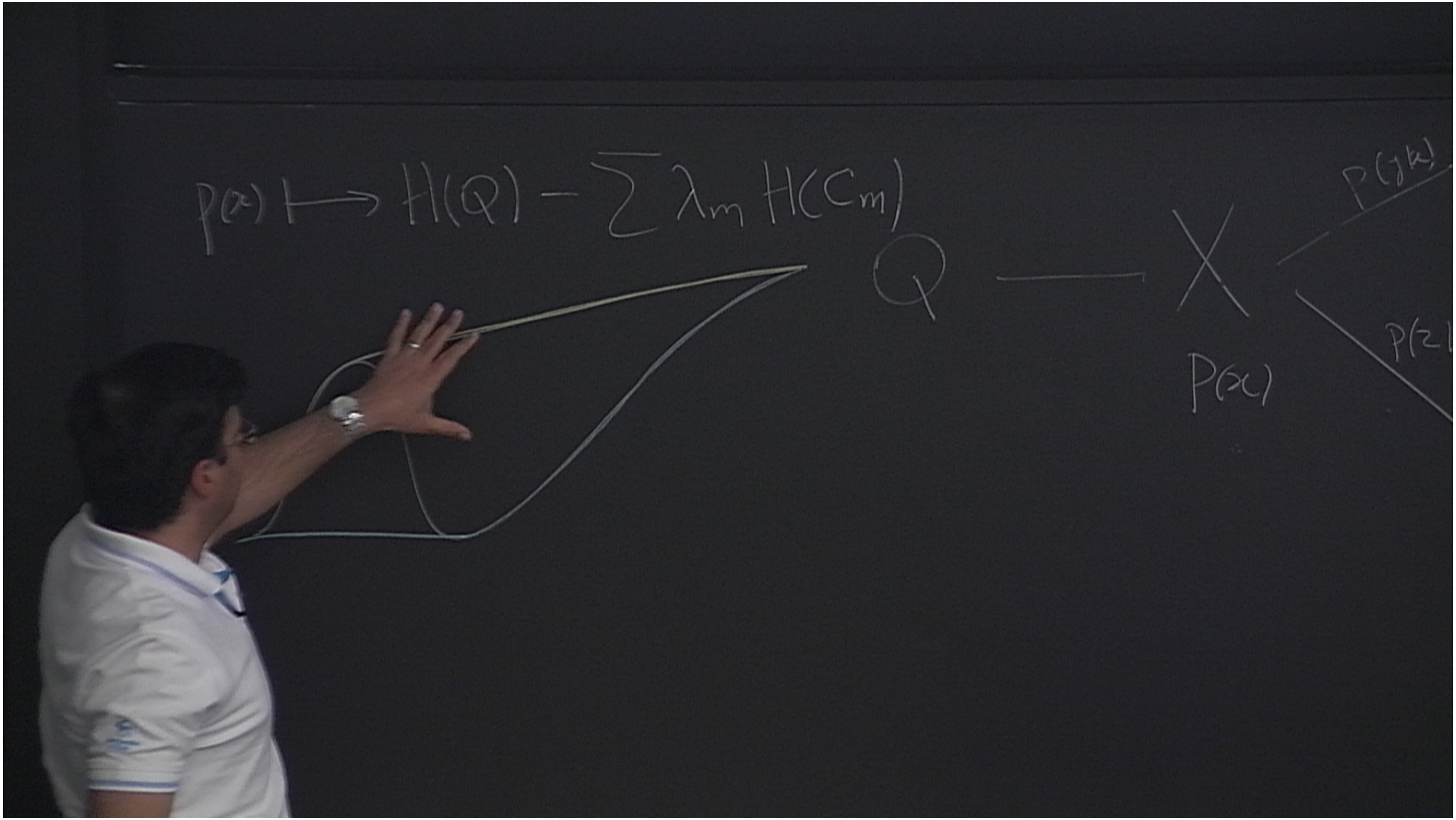
Proof of (2) $\Rightarrow$ (3)

$$\max_{p(z|x)} \left[H(\mathbf{Q}|Z) - \sum_m \lambda_m H(C_m|Z) \right] \leq \epsilon + \min_{p(z|x)} \left[H(\mathbf{Q}|Z) - \sum_m \lambda_m H(C_m|Z) \right]$$

Proof of (2) $\Rightarrow$ (3)

$$\max_{p(z|x)} \left[H(\mathbf{Q}|Z) - \sum_m \lambda_m H(C_m|Z) \right] \leq \epsilon + \min_{p(z|x)} \left[H(\mathbf{Q}|Z) - \sum_m \lambda_m H(C_m|Z) \right]$$

- Therefore, the function $p(x) \mapsto H(\mathbf{Q}) - \sum_m \lambda_m H(C_m)$ is almost linear.


$p(x) \mapsto H(Q) - \sum \lambda_m H(C_m)$
Q
X
P(x)
P(y|x)
P(z|

Proof of (2) $\Rightarrow$ (3)

$$\max_{p(z|x)} \left[H(\mathbf{Q}|Z) - \sum_m \lambda_m H(C_m|Z) \right] \leq \epsilon + \min_{p(z|x)} \left[H(\mathbf{Q}|Z) - \sum_m \lambda_m H(C_m|Z) \right]$$

- Therefore, the function $p(x) \mapsto H(\mathbf{Q}) - \sum_m \lambda_m H(C_m)$ is almost linear.
- Define $D = (M, C_M)$ where $p(M = m) = \lambda_m$.

Proof of (2) $\Rightarrow$ (3)

$$\max_{p(z|x)} \left[H(\mathbf{Q}|Z) - \sum_m \lambda_m H(C_m|Z) \right] \leq \epsilon + \min_{p(z|x)} \left[H(\mathbf{Q}|Z) - \sum_m \lambda_m H(C_m|Z) \right]$$

- Therefore, the function $p(x) \mapsto H(\mathbf{Q}) - \sum_m \lambda_m H(C_m)$ is almost linear.
- Define $D = (M, C_M)$ where $p(M = m) = \lambda_m$. Then

$$p(x) \mapsto I(\mathbf{Q}; X) - I(D; X)$$

is almost linear.

Proof of (2) $\Rightarrow$ (3)

$$\max_{p(z|x)} \left[H(\mathbf{Q}|Z) - \sum_m \lambda_m H(C_m|Z) \right] \leq \epsilon + \min_{p(z|x)} \left[H(\mathbf{Q}|Z) - \sum_m \lambda_m H(C_m|Z) \right]$$

- Therefore, the function $p(x) \mapsto H(\mathbf{Q}) - \sum_m \lambda_m H(C_m)$ is almost linear.
- Define $D = (M, C_M)$ where $p(M = m) = \lambda_m$. Then

$$p(x) \mapsto I(\mathbf{Q}; X) - I(D; X)$$

  is almost linear.
- $I(\mathbf{Q}; X) - I(D; X)$ is zero at extreme points.
- Thus $I(\mathbf{Q}; X) - I(D; X)$ is almost zero everywhere!

Main Result (2)

Theorem: The followings are equivalent

(1) $\mathrm{QConvHull}(\mathcal{G}) = \mathrm{ConvHull}(\mathcal{G})$.

(2) For any $p(x, y, z)$ consider the optimization problem

$$\sup_{\mathbf{Q}-X-YZ} I(\mathbf{Q}; Y) - I(\mathbf{Q}; Z).$$

(3) For a c-q channel $X \to \mathbf{Q}$, consider the function $p(x) \mapsto I(X; \mathbf{Q})$. Then for every $\epsilon > 0$ there exists a c-c channel $X \to C$ such that $\left| I(X; \mathbf{Q}) - I(X; C) \right| \leq \epsilon$ for all $p(x)$. Then the supremum is attained at a classical $\mathbf{Q}$.

Main Result (2)

Theorem: The followings are equivalent

(1) $\mathrm{QConvHull}(\mathcal{G}) = \mathrm{ConvHull}(\mathcal{G})$.

(2) For any $p(x, y, z)$ consider the optimization problem

$$\sup_{\mathbf{Q}-X-YZ} I(\mathbf{Q}; Y) - I(\mathbf{Q}; Z).$$

(3) For a c-q channel $X \to \mathbf{Q}$, consider the function $p(x) \mapsto I(X; \mathbf{Q})$. Then for every $\epsilon > 0$ there exists a c-c channel $X \to C$ such that $\left| I(X; \mathbf{Q}) - I(X; C) \right| \leq \epsilon$ for all $p(x)$. Then the supremum is attained at a classical $\mathbf{Q}$.

Theorem: There is a counterexample for part (1).

Counterexample Based on Zero-Error Capacity

- Let $X \to Y$ be a channel
- Fix a distribution on X
- Suppose $\exists M, C$ such that

$$I(C;M) = 0, \quad H(X|CM) = 0, \quad MC - X - Y, \quad H(M|CY) = 0$$

Counterexample Based on Zero-Error Capacity

- Let $X \to Y$ be a channel
- Fix a distribution on X
- Suppose $\exists M, C$ such that

$$I(C;M) = 0, \quad H(X|CM) = 0, \quad MC - X - Y, \quad H(M|CY) = 0$$

- Then we have a (one-shot) zero-error communication protocol with rate $\log |\mathcal{M}|$ over the channel $X \to Y$

Counterexample Based on Zero-Error Capacity

- Let $X \to Y$ be a channel
- Fix a distribution on X
- Suppose $\exists M, C$ such that

$$I(C;M) = 0, \quad H(X|CM) = 0, \quad MC - X - Y, \quad H(M|CY) = 0$$

- Then we have a (one-shot) zero-error communication protocol with rate $\log |\mathcal{M}|$ over the channel $X \to Y$
  - Classical $C \quad \to \quad$ shared randomness
  - Quantum $C \quad \to \quad$ shared entanglement

Counterexample Based on Zero-Error Capacity

- Let $X \to Y$ be a channel
- Fix a distribution on X
- Suppose $\exists M, C$ such that

$$I(C;M) = 0, \quad H(X|CM) = 0, \quad MC - X - Y, \quad H(M|CY) = 0$$

- Then we have a (one-shot) zero-error communication protocol with rate $\log |\mathcal{M}|$ over the channel $X \to Y$
  - Classical $C \quad \to \quad$ shared randomness
  - Quantum $C \quad \to \quad$ shared entanglement
- [Leung et al '10] Entanglement may increase the one-shot zero-error capacity of classical channels.
- The above equations can be written in terms of the *conditioning* problem $\to$ counterexample

Main Result (3)

Theorem: The followings are equivalent

(1) $\mathrm{QConvHull}(\mathcal{G}) = \mathrm{ConvHull}(\mathcal{G})$.

(2) For any $p(x, y, z)$ consider the optimization problem

$$\sup_{\mathbf{Q}-X-YZ} I(\mathbf{Q}; Y) - I(\mathbf{Q}; Z).$$

Then the supremum is attained at a classical $\mathbf{Q}$.

(3) For a c-q channel $X \to \mathbf{Q}$, consider the function $p(x) \mapsto I(X; \mathbf{Q})$. Then for every $\epsilon > 0$ there exists a c-c channel $X \to C$ such that $\left|I(X; \mathbf{Q}) - I(X; C)\right| \leq \epsilon$ for all $p(x)$.

Theorem: There is a counterexample for part (1).

Main Result (3)

Theorem: The followings are equivalent

(1) $\mathrm{QConvHull}(\mathcal{G}) = \mathrm{ConvHull}(\mathcal{G})$.

(2) For any $p(x, y, z)$ consider the optimization problem

$$\sup_{\mathbf{Q}-X-YZ} I(\mathbf{Q}; Y) - I(\mathbf{Q}; Z).$$

Then the supremum is attained at a classical $\mathbf{Q}$.

(3) For a c-q channel $X \to \mathbf{Q}$, consider the function $p(x) \mapsto I(X; \mathbf{Q})$. Then for every $\epsilon > 0$ there exists a c-c channel $X \to C$ such that $\left|I(X; \mathbf{Q}) - I(X; C)\right| \leq \epsilon$ for all $p(x)$.

Theorem: There is a counterexample for part (1).

Theorem: Part (3) holds if $|X| = \dim\mathbf{Q} = 2$.

Dimension bounds on quantum auxiliary systems

- We compared $\sup_{\mathbf{Q}-X-YZ} I(\mathbf{Q};Y) - I(\mathbf{Q};Z)$ in the two cases
  - $\mathbf{Q}$ is classical
  - $\mathbf{Q}$ is quantum
- What if we compare the followings
  - $\mathbf{Q}$ is quantum
  - $\mathbf{Q}$ is quantum of dimension $\leq d$
- How the curves (surfaces) $p(x) \mapsto I(X;\mathbf{Q})$ behave when we increase dim$\mathbf{Q}$?

Dimension bounds on quantum auxiliary systems

- We compared $\sup_{\mathbf{Q}-X-YZ} I(\mathbf{Q};Y) - I(\mathbf{Q};Z)$ in the two cases
  - $\mathbf{Q}$ is classical
  - $\mathbf{Q}$ is quantum
- What if we compare the followings
  - $\mathbf{Q}$ is quantum
  - $\mathbf{Q}$ is quantum of dimension $\leq d$
- How the curves (surfaces) $p(x) \mapsto I(X;\mathbf{Q})$ behave when we increase dim$\mathbf{Q}$?

Is entanglement ever helpful in classical communication setting?

- [Bennett et al '02] Entanglement does not increase the capacity of point-to-point classical channels.

Is entanglement ever helpful in classical communication setting?

- [Bennett et al '02] Entanglement does not increase the capacity of point-to-point classical channels.
- Entanglement helps in Bell settings → simulation of non-local correlations

Is entanglement ever helpful in classical communication setting?

- [Bennett et al '02] Entanglement does not increase the capacity of point-to-point classical channels.
- Entanglement helps in Bell settings → simulation of non-local correlations
- Does entanglement helps in parallel repetitions of Bell settings?

Simulation of bipartite correlations

Alice x^n — Bob y^n with distribution $\prod_j p(x_j, y_j)$

f

a^n — b^n with distribution $\tilde{p}(a^n, b^n | x^n, y^n)$

Classical case: shared randomness

Theorem [Yassaee et al '12]: A rate R is achievable iff there exists an auxiliary random variable F such that

$$R \geq I(X;F|Y)$$

and

$$\begin{aligned} &F - X - Y, \\ &A - FX - YB, \\ &B - FY - XA, \\ &|\mathcal{F}| \leq |\mathcal{X}||\mathcal{Y}||\mathcal{A}||\mathcal{B}| + 1. \end{aligned}$$

Classical case: shared randomness

Theorem [Yassaee et al '12]: A rate R is achievable iff there exists an auxiliary random variable F such that

$$R \geq I(X;F|Y)$$

and

$$\begin{aligned} &F - X - Y, \\ &A - FX - YB, \\ &B - FY - XA, \\ &|\mathcal{F}| \leq |\mathcal{X}||\mathcal{Y}||\mathcal{A}||\mathcal{B}| + 1. \end{aligned}$$

Quantum Case: shared entanglement

$$\mathcal{S}_\epsilon = \{R : \exists \mathbf{Q} \text{ satisfying the following conditions } \}$$

$$R \geq I(X;\mathbf{Q}|Y)$$

$$A, X, Y, \mathbf{Q} \sim \{\tilde{p}(a,x,y); \rho^{\mathbf{Q}}_{a,x,y}\}$$

$$A, B, X, Y \sim \tilde{p}(a,b,x,y) = \tilde{p}(a,x,y)\tilde{p}(b|a,x,y),$$

$$\|\tilde{p}(a,b,x,y) - p(a,b,x,y)\|_1 \leq \epsilon,$$

$$\mathbf{Q} - X - Y,$$

$$A - \mathbf{Q}X - Y,$$

$$\exists \text{ CPTP map } \Psi \text{ s.t. } \Psi(\mathbf{Q}, Y) = B.$$

Theorem [B., Gohari, '12]:

(1) Every achievable R is in $\bigcap_{\epsilon>0} \mathcal{S}_\epsilon$

(2) All $R \in \mathcal{S}_0$ are achievable

Classical case: shared randomness

Theorem [Yassaee et al '12]: A rate R is achievable iff there exists an auxiliary random variable F such that

$$R \geq I(X;F|Y)$$

and

$$\begin{aligned} &F - X - Y, \\ &A - FX - YB, \\ &B - FY - XA, \\ &|\mathcal{F}| \leq |\mathcal{X}||\mathcal{Y}||\mathcal{A}||\mathcal{B}| + 1. \end{aligned}$$

Quantum Case: shared entanglement

$$\mathcal{S}_\epsilon = \{R : \exists \mathbf{Q} \text{ satisfying the following conditions } \}$$

$$R \geq I(X;\mathbf{Q}|Y)$$

$$A, X, Y, \mathbf{Q} \sim \{\tilde{p}(a,x,y); \rho^{\mathbf{Q}}_{a,x,y}\}$$

$$A, B, X, Y \sim \tilde{p}(a,b,x,y) = \tilde{p}(a,x,y)\tilde{p}(b|a,x,y),$$

$$\|\tilde{p}(a,b,x,y) - p(a,b,x,y)\|_1 \leq \epsilon,$$

$$\mathbf{Q} - X - Y,$$

$$A - \mathbf{Q}X - Y,$$

$$\exists \text{ CPTP map } \Psi \text{ s.t. } \Psi(\mathbf{Q}, Y) = B.$$

Theorem [B., Gohari, '12]:

(1) Every achievable R is in $\bigcap_{\epsilon>0} \mathcal{S}_\epsilon$

(2) All $R \in \mathcal{S}_0$ are achievable

Classical case: shared randomness

Theorem [Yassaee et al '12]: A rate R is achievable iff there exists an auxiliary random variable F such that

$$R \geq I(X;F|Y)$$

and

$$\begin{aligned} &F - X - Y, \\ &A - FX - YB, \\ &B - FY - XA, \\ &|\mathcal{F}| \leq |\mathcal{X}||\mathcal{Y}||\mathcal{A}||\mathcal{B}| + 1. \end{aligned}$$

Quantum Case: shared entanglement

$$\mathcal{S}_\epsilon = \{R : \exists \mathbf{Q} \text{ satisfying the following conditions } \}$$

$$R \geq I(X;\mathbf{Q}|Y)$$

$$A, X, Y, \mathbf{Q} \sim \{\tilde{p}(a,x,y); \rho^{\mathbf{Q}}_{a,x,y}\}$$

$$A, B, X, Y \sim \tilde{p}(a,b,x,y) = \tilde{p}(a,x,y)\tilde{p}(b|a,x,y),$$

$$\|\tilde{p}(a,b,x,y) - p(a,b,x,y)\|_1 \leq \epsilon,$$

$$\mathbf{Q} - X - Y,$$

$$A - \mathbf{Q}X - Y,$$

$$\exists \text{ CPTP map } \Psi \text{ s.t. } \Psi(\mathbf{Q}, Y) = B.$$

Theorem [B., Gohari, '12]:

(1) Every achievable R is in $\bigcap_{\epsilon>0} \mathcal{S}_\epsilon$

(2) All $R \in \mathcal{S}_0$ are achievable

Proof: (1) follows from similar steps as in the classical case.
(2) follows from a remote state preparation protocol with side information

Example: CHSH-type correlations

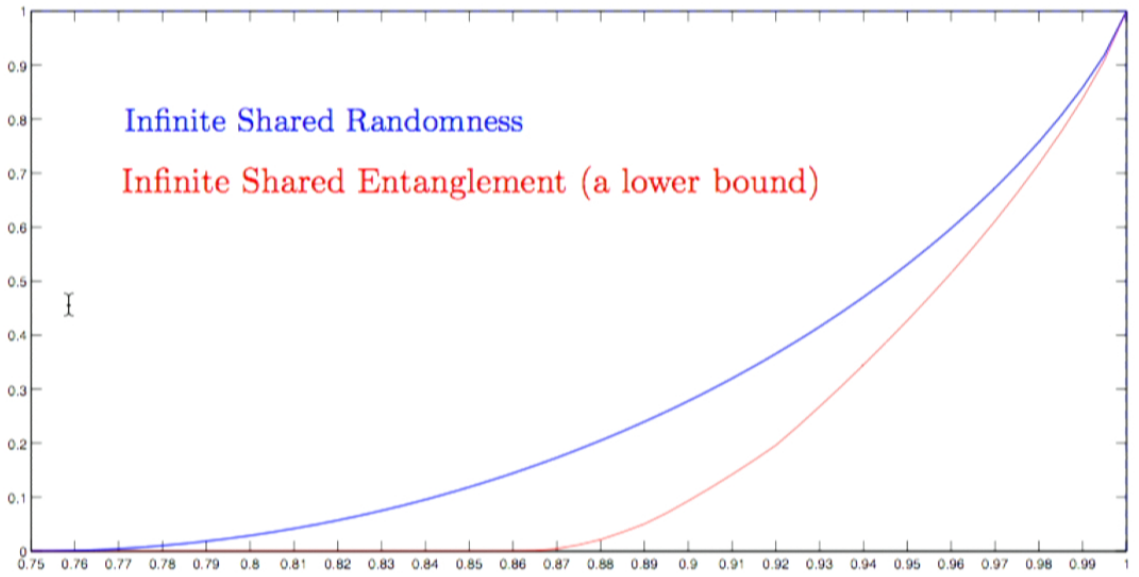
$$p_\alpha(a,b|x,y)=\begin{cases}\frac{\alpha}{2} & a\oplus b=xy\\ \frac{1-\alpha}{2} & \text{otherwise}\end{cases}$$

$$p_\alpha(x,y)=1/4$$

Example: CHSH-type correlations

$$p_\alpha(a,b|x,y)=\begin{cases}\frac{\alpha}{2} & a\oplus b=xy\\ \frac{1-\alpha}{2} & \text{otherwise}\end{cases}$$

$$p_\alpha(x,y) = 1/4$$



Summary

- Simulation of bipartite correlations (an information theoretic approach)

Summary

- Simulation of bipartite correlations (an information theoretic approach)
- Quantum conditioning: $\mathrm{QConvHull}(\mathcal{G}) \neq \mathrm{ConvHull}(\mathcal{G})$
  - Equality may hold in certain directions

Summary

- Simulation of bipartite correlations (an information theoretic approach)
- Quantum conditioning: $\mathrm{QConvHull}(\mathcal{G}) \neq \mathrm{ConvHull}(\mathcal{G})$
  - Equality may hold in certain directions
- Techniques may be used to find dimension bounds on auxiliary quantum registers

Summary

- Simulation of bipartite correlations (an information theoretic approach)
- Quantum conditioning: $\text{QConvHull}(\mathcal{G}) \neq \text{ConvHull}(\mathcal{G})$
  - Equality may hold in certain directions
- Techniques may be used to find dimension bounds on auxiliary quantum registers
- Is multi-letter-$\text{ConvHull}(\mathcal{G}) =$ multi-letter-$\text{QConvHull}(\mathcal{G})$?

$$\left(p(x_1,\ldots,x_n), \frac{1}{m}H(X_1^m|C), \ldots, \frac{1}{m}H(X_n^m|C)\right)$$

Summary

- Simulation of bipartite correlations (an information theoretic approach)
- Quantum conditioning: $\text{QConvHull}(\mathcal{G}) \neq \text{ConvHull}(\mathcal{G})$
  - Equality may hold in certain directions
- Techniques may be used to find dimension bounds on auxiliary quantum registers
- Is multi-letter-$\text{ConvHull}(\mathcal{G}) =$ multi-letter-$\text{QConvHull}(\mathcal{G})$?

$$\left(p(x_1,\ldots,x_n), \frac{1}{m}H(X_1^m|C), \ldots, \frac{1}{m}H(X_n^m|C)\right)$$

arXiv:1207.3911