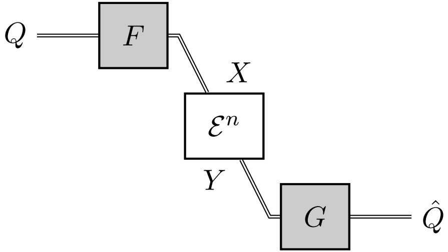
Classical communication over classical channels using non-classical correlation.

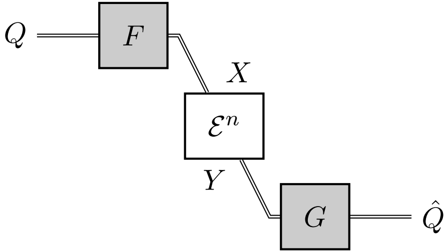
Will Matthews
IQC @ University of Waterloo

Classical data over classical channels



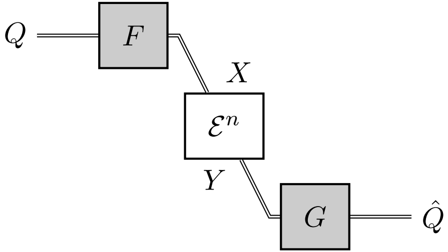
- Finite input alphabet A, output alphabet B.

Classical data over classical channels



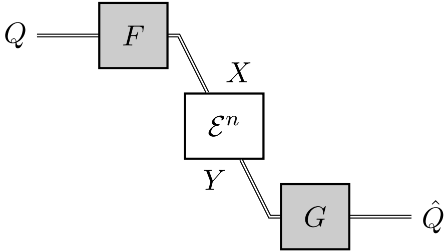
- Finite input alphabet A, output alphabet B.
- Channel input X in A^n, output Y in B^n (random variables).

Classical data over classical channels



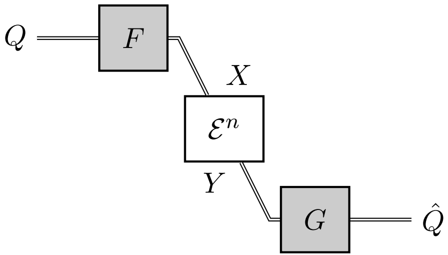
- Finite input alphabet A, output alphabet B.
- Channel input X in A^n, output Y in B^n (random variables).
- $\Pr(Y = y|X = x, \mathcal{E}) = \mathcal{E}^n(y|x)$.
  Discrete **M**emoryless **C**hannel: $\mathcal{E}^n(y|x) = \prod_{i=1}^n \mathcal{E}(y_i|x_i)$.

Classical data over classical channels



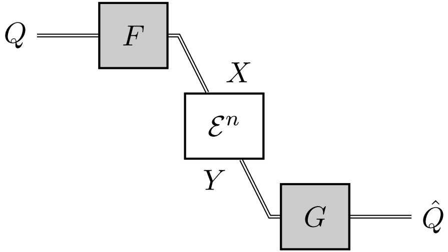
- Finite input alphabet A, output alphabet B.
- Channel input X in A^n, output Y in B^n (random variables).
- $\Pr(Y = y|X = x, \mathcal{E}) = \mathcal{E}^n(y|x)$.
  Discrete **M**emoryless **C**hannel: $\mathcal{E}^n(y|x) = \prod_{i=1}^n \mathcal{E}(y_i|x_i)$.
- Message Q, decoded message $\hat{Q}$ in $[M] := \{1, \ldots, M\}$

Classical data over classical channels



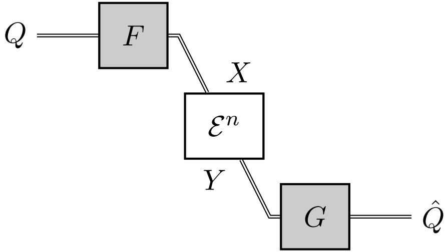
- Finite input alphabet A, output alphabet B.
- Channel input X in A^n, output Y in B^n (random variables).
- $\Pr(Y = y|X = x, \mathcal{E}) = \mathcal{E}^n(y|x)$.
  Discrete **M**emoryless **C**hannel: $\mathcal{E}^n(y|x) = \prod_{i=1}^n \mathcal{E}(y_i|x_i)$.
- Message Q, decoded message $\hat{Q}$ in $[M] := \{1, \ldots, M\}$
- Classical code: Encoder $\Pr(X = x|Q = q) = F(x|q)$;

Classical data over classical channels



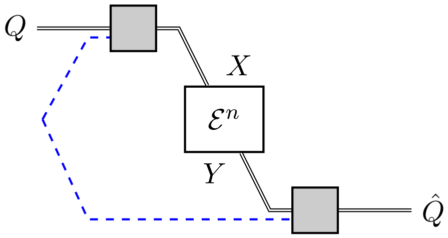
- Finite input alphabet A, output alphabet B.
- Channel input X in A^n, output Y in B^n (random variables).
- $\Pr(Y = y|X = x, \mathcal{E}) = \mathcal{E}^n(y|x)$.
  Discrete **M**emoryless **C**hannel: $\mathcal{E}^n(y|x) = \prod_{i=1}^n \mathcal{E}(y_i|x_i)$.
- Message Q, decoded message $\hat{Q}$ in $[M] := \{1, \ldots, M\}$
- Classical code: Encoder $\Pr(X = x|Q = q) = F(x|q)$;
  Decoder $\Pr(\hat{Q} = \hat{q}|Y = y) = G(\hat{q}|y)$.

Classical data over classical channels



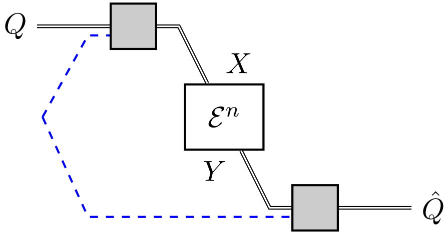
- Finite input alphabet A, output alphabet B.
- Channel input X in A^n, output Y in B^n (random variables).
- $\Pr(Y = y|X = x, \mathcal{E}) = \mathcal{E}^n(y|x)$.
  Discrete **M**emoryless **C**hannel: $\mathcal{E}^n(y|x) = \prod_{i=1}^n \mathcal{E}(y_i|x_i)$.
- Message Q, decoded message $\hat{Q}$ in $[M] := \{1, \ldots, M\}$
- Classical code: Encoder $\Pr(X = x|Q = q) = F(x|q)$;
  Decoder $\Pr(\hat{Q} = \hat{q}|Y = y) = G(\hat{q}|y)$.
- $M_\epsilon(\mathcal{E}^n)$:=max M such that $\exists$ code with
  $\Pr(Q \neq \hat{Q}|\mathcal{E}^n, F, G) \leq \epsilon$ (hard to compute exactly).

Classical data over classical channels



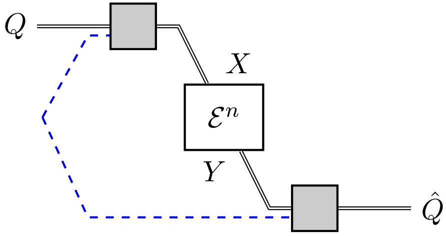
- Correlated Encoder/Decoder:
  $\Pr(X = x, \hat{Q} = \hat{q} | Q = q, Y = y) = Z(x, \hat{q} | q, y)$

Classical data over classical channels



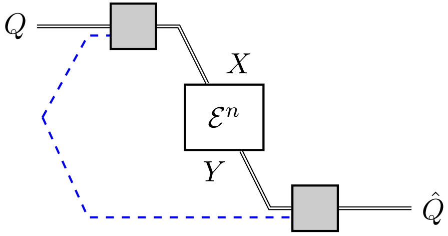
- Correlated Encoder/Decoder:
  $\Pr(X = x, \hat{Q} = \hat{q} | Q = q, Y = y) = Z(x, \hat{q} | q, y)$
- Entanglement assisted: $Z(x, \hat{q}|q, y) = \operatorname{Tr} F_x^{(q)} \otimes G_{\hat{q}}^{(y)} \rho_{AB}$

Classical data over classical channels



- Correlated Encoder/Decoder:
  $\Pr(X = x, \hat{Q} = \hat{q} | Q = q, Y = y) = Z(x, \hat{q} | q, y)$
- Entanglement assisted: $Z(x, \hat{q}|q, y) = \operatorname{Tr} F_x^{(q)} \otimes G_{\hat{q}}^{(y)} \rho_{AB}$
- Non-signalling assisted: $Z(x, \hat{q}|q, y)$ is non-signalling.

Classical data over classical channels



- Correlated Encoder/Decoder:
  $\Pr(X = x, \hat{Q} = \hat{q} | Q = q, Y = y) = Z(x, \hat{q}|q, y)$
- Entanglement assisted: $Z(x, \hat{q}|q, y) = \mathrm{Tr}\, F_x^{(q)} \otimes G_{\hat{q}}^{(y)} \rho_{AB}$
- Non-signalling assisted: $Z(x, \hat{q}|q, y)$ is non-signalling.
- $M_\epsilon^{\mathrm{E}}(\mathcal{E}^n)$:=max M such that $\exists$ entanglement assisted code with $\Pr(Q \neq \hat{Q}|\mathcal{E}^n, Z) \leq \epsilon$.

Capacity

- $C_\epsilon(\mathcal{E}) := \lim_{n\to\infty} \frac{1}{n} \log M_\epsilon(\mathcal{E}^n)$, $C(\mathcal{E}) := \lim_{\epsilon\to 0} C_\epsilon^\Omega(\mathcal{E})$

Capacity

- $C_\epsilon(\mathcal{E}) := \lim_{n\to\infty} \frac{1}{n} \log M_\epsilon(\mathcal{E}^n)$, $C(\mathcal{E}) := \lim_{\epsilon\to 0} C_\epsilon^\Omega(\mathcal{E})$
- In general, *zero-error* capacity $C_0(\mathcal{E}) \neq C(\mathcal{E})$.

Capacity

- $C_\epsilon(\mathcal{E}) := \lim_{n\to\infty} \frac{1}{n} \log M_\epsilon(\mathcal{E}^n)$, $C(\mathcal{E}) := \lim_{\epsilon\to 0} C_\epsilon^\Omega(\mathcal{E})$
- In general, *zero-error* capacity $C_0(\mathcal{E}) \neq C(\mathcal{E})$.
- Bennett, Shor, Smolin, Thapliyal (2001):
  For all DMCs: $C^{\mathrm{E}}(\mathcal{E}) = C(\mathcal{E})$ (quant-ph/0106052).

Capacity

- $C_\epsilon(\mathcal{E}) := \lim_{n\to\infty} \frac{1}{n} \log M_\epsilon(\mathcal{E}^n)$, $C(\mathcal{E}) := \lim_{\epsilon\to 0} C_\epsilon^\Omega(\mathcal{E})$
- In general, *zero-error* capacity $C_0(\mathcal{E}) \neq C(\mathcal{E})$.
- Bennett, Shor, Smolin, Thapliyal (2001):
  For all DMCs: $C^{\mathrm{E}}(\mathcal{E}) = C(\mathcal{E})$ (quant-ph/0106052).
  Entanglement doesn't change capacity. But..

Capacity

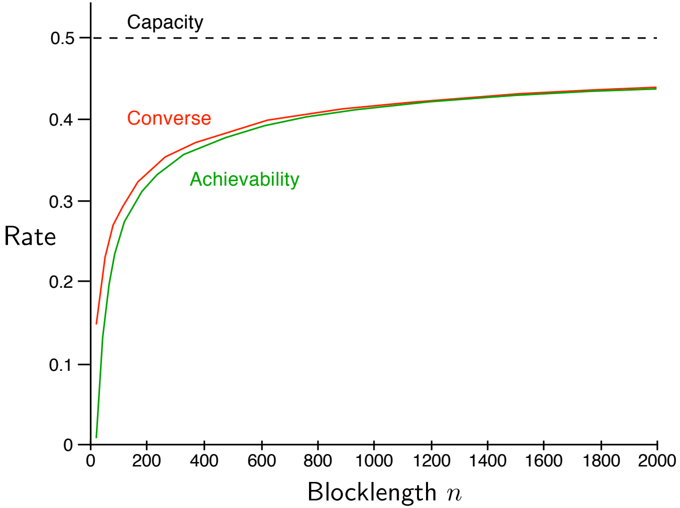
- $C_\epsilon(\mathcal{E}) := \lim_{n\to\infty} \frac{1}{n} \log M_\epsilon(\mathcal{E}^n)$, $C(\mathcal{E}) := \lim_{\epsilon\to 0} C_\epsilon^\Omega(\mathcal{E})$
- In general, *zero-error* capacity $C_0(\mathcal{E}) \neq C(\mathcal{E})$.
- Bennett, Shor, Smolin, Thapliyal (2001):
  For all DMCs: $C^{\mathrm{E}}(\mathcal{E}) = C(\mathcal{E})$ (quant-ph/0106052).
  Entanglement doesn't change capacity. But..
- Entanglement can increase rate for fixed n and ϵ / reduce error prob. for fixed rate and n
  Cubitt, Leung, W.M., Winter: (0911.5300 and 1003.3195)
  Demonstration by Resch group at IQC (1010.2566)

Capacity

- $C_\epsilon(\mathcal{E}) := \lim_{n\to\infty} \frac{1}{n} \log M_\epsilon(\mathcal{E}^n)$, $C(\mathcal{E}) := \lim_{\epsilon\to 0} C_\epsilon^\Omega(\mathcal{E})$
- In general, *zero-error* capacity $C_0(\mathcal{E}) \neq C(\mathcal{E})$.
- Bennett, Shor, Smolin, Thapliyal (2001):
  For all DMCs: $C^{\mathrm{E}}(\mathcal{E}) = C(\mathcal{E})$ (quant-ph/0106052).
  Entanglement doesn't change capacity. But..
- Entanglement can increase rate for fixed n and ϵ / reduce error prob. for fixed rate and n
  Cubitt, Leung, W.M., Winter: (0911.5300 and 1003.3195)
  Demonstration by Resch group at IQC (1010.2566)
- Leung, Mancinska, W.M., Ozols, Roy (1009.1195):
  Example of DMC with $C(\mathcal{E}) = C_0^{\mathrm{E}}(\mathcal{E}) > C_0(\mathcal{E})$.

Motivation: Beyond Capacity

Converse and achievability bounds on the rate $\frac{1}{n}\log M_\epsilon(\mathcal{E}^n)$ when $\epsilon = 1/1000$ and $\mathcal{E}$ is the BSC with $\Pr(\text{bit flip}) = 0.11$[1].



[1] Polyanskiy, Poor, Verdú. IEEE Trans. Inf. T., 56, 2307-2359

Motivation: Beyond Capacity

Asymptotics of rate as function of n for DMCs:

$$\frac{1}{n}\log M_\epsilon(\mathcal{E}^{\otimes n}) = C(\mathcal{E}) - Q^{-1}(\epsilon)\sqrt{\frac{V(\mathcal{E})}{n}} + O(\log n)/n$$

By Polyanskiy, Poor, Verdú (PPV converse) converse and achievability results for classical codes which match up to $O(\log n)/n$.

Motivation: Beyond Capacity

Asymptotics of rate as function of n for DMCs:

$$\frac{1}{n}\log M_\epsilon(\mathcal{E}^{\otimes n}) = C(\mathcal{E}) - Q^{-1}(\epsilon)\sqrt{\frac{V(\mathcal{E})}{n}} + O(\log n)/n$$

By Polyanskiy, Poor, Verdú (PPV converse) converse and achievability results for classical codes which match up to $O(\log n)/n$.

- Use of entanglement can't change capacity but can give striking qualitative changes to error behaviour below capacity.

Motivation: Beyond Capacity

Asymptotics of rate as function of n for DMCs:

$$\frac{1}{n}\log M_\epsilon(\mathcal{E}^{\otimes n}) = C(\mathcal{E}) - Q^{-1}(\epsilon)\sqrt{\frac{V(\mathcal{E})}{n}} + O(\log n)/n$$

By Polyanskiy, Poor, Verdú (PPV converse) converse and achievability results for classical codes which match up to $O(\log n)/n$.

- Use of entanglement can't change capacity but can give striking qualitative changes to error behaviour below capacity.
- Goal: Looking beyond zero-error, *quantify* the extent to which entanglement improves coding.

Motivation: Beyond Capacity

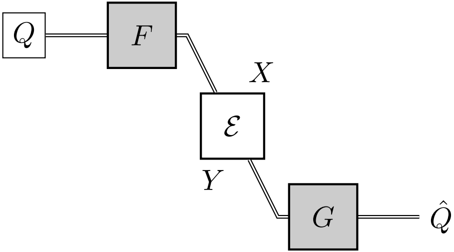
Asymptotics of rate as function of n for DMCs:

$$\frac{1}{n}\log M_\epsilon(\mathcal{E}^{\otimes n}) = C(\mathcal{E}) - Q^{-1}(\epsilon)\sqrt{\frac{V(\mathcal{E})}{n}} + O(\log n)/n$$

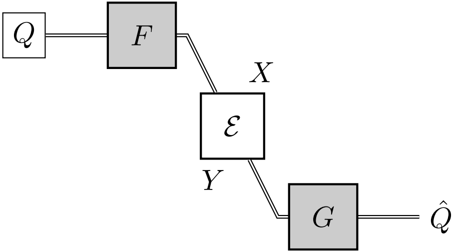
By Polyanskiy, Poor, Verdú (PPV converse) converse and achievability results for classical codes which match up to $O(\log n)/n$.

- Use of entanglement can't change capacity but can give striking qualitative changes to error behaviour below capacity.
- Goal: Looking beyond zero-error, *quantify* the extent to which entanglement improves coding.
- E.g. what does the asymptotic expansion of rate as a function of n look like after the capacity term with entanglement assistance?

PPV converse

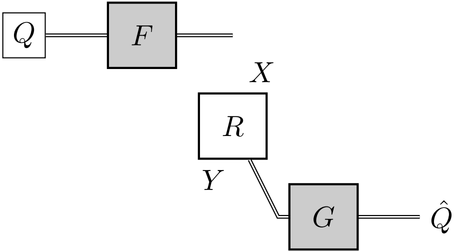


PPV converse



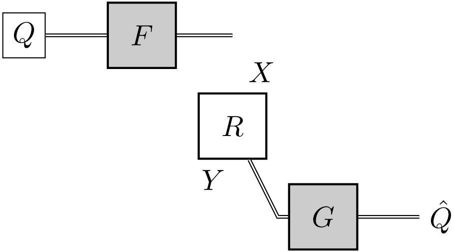
- P_{XY}: $\Pr(X = a) = \frac{1}{M} \sum_q F(x|q) =: p_x$, $\Pr(Y = y|X = x) = \mathcal{E}(y|x)$.

PPV converse



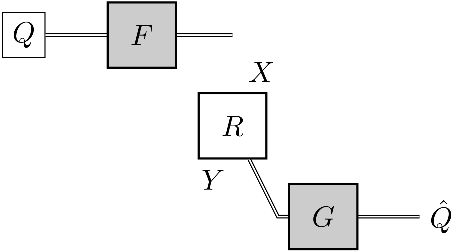
- P_{XY}: $\Pr(X=a) = \frac{1}{M}\sum_q F(x|q) =: p_x$,
  $\Pr(Y=y|X=x) = \mathcal{E}(y|x)$.
- $P_X \times R_Y$: $\Pr(X=a) = p_x$, $\Pr(Y=y|X=x) = r_y$.

PPV converse



- P_{XY}: $\Pr(X = a) = \frac{1}{M}\sum_q F(x|q) =: p_x$,
  $\Pr(Y = y|X = x) = \mathcal{E}(y|x)$.
- $P_X \times R_Y$: $\Pr(X = a) = p_x$, $\Pr(Y = y|X = x) = r_y$.
- Test T for P_{XY}: Specifies $\Pr(\text{pass } T|X = x, Y = y)$.

PPV converse



- P_{XY}: $\Pr(X = a) = \frac{1}{M}\sum_q F(x|q) =: p_x$,
  $\Pr(Y = y|X = x) = \mathcal{E}(y|x)$.
- $P_X \times R_Y$: $\Pr(X = a) = p_x$, $\Pr(Y = y|X = x) = r_y$.
- Test T for P_{XY}: Specifies $\Pr($pass $T|X = x, Y = y)$.
- $\beta_\epsilon(P_{XY}, P_X \times R_Y)$: Minimum $\Pr($pass $T|P_X \times R_Y)$ for all T with $\Pr($pass $T|P_{XY}) \geq 1 - \epsilon$.

PPV converse

Given (M, ϵ) code for $\mathcal{E}$ with input distribution P_X, construct test T for P_{XY} (vs. $P_X \times R_Y$):

$$\Pr(\text{pass } T|X = x, Y = y) = T_{xy} := \sum_{q \in [M]} G(q|y) \Pr(Q = q|X = x, F).$$

PPV converse

Given (M, ϵ) code for $\mathcal{E}$ with input distribution P_X, construct test T for P_{XY} (vs. $P_X \times R_Y$):

$$\Pr(\text{pass } T|X=x, Y=y) = T_{xy} := \sum_{q \in [M]} G(q|y) \Pr(Q=q|X=x, F).$$

For P_{XY}: $\Pr(X=x, Y=y) = p_x \mathcal{E}(y|x)$, the probability of passing the test is

$$\begin{aligned}
\sum_{x,y} T_{xy} p_x \mathcal{E}(y|x) &= \sum_{x,y,q} G(q|y)\mathcal{E}(y|x) p_x \Pr(Q=q|X=x, F) \\
&= \sum_{x,y,q} G(q|y)\mathcal{E}(y|x) \Pr(Q=q \wedge X=x|F) \\
&= \frac{1}{M} \sum_{x,y,q} G(q|y)\mathcal{E}(y|x) F(x|q) \\
&= 1-\epsilon.
\end{aligned}$$

PPV converse

Given (M, ϵ) code for $\mathcal{E}$ with input distribution P_X, construct test T for P_{XY} (vs. $P_X \times R_Y$):

$$\Pr(\text{pass } T|X = x, Y = y) = T_{xy} := \sum_{q \in [M]} G(q|y) \Pr(Q = q|X = x, F).$$

For $P_X \times R_Y$: $\Pr(X = x, Y = y) = p_x r_y$, the probability of passing the test is

$$\begin{aligned}
\sum_{x,y} T_{xy} p_x r_y &= \sum_{x,y,q} G(q|y) r_y p_x \Pr(Q = q|X = x, F) \\
&= \sum_{x,y,q} G(q|y) r_y \Pr(Q = q \wedge X = x|F) \\
&= \frac{1}{M} \sum_{x,y,q} G(q|y) r_y F(x|q) \\
&= \frac{1}{M} \sum_{y,q} G(q|y) r_y \\
&= 1/M.
\end{aligned}$$

PPV converse

If there exists a code of size M with distribution P_X for channel input X, and error prob. ϵ, then for all distributions R_Y on Y:

$$\beta_\epsilon(P_{XY}, P_X \times R_Y) \leq \frac{1}{M}.$$

PPV converse

If there exists a code of size M with distribution P_X for channel input X, and error prob. ϵ, then for all distributions R_Y on Y:

$$\beta_\epsilon(P_{XY}, P_X \times R_Y) \leq \frac{1}{M}.$$

For *all* codes of size M and error prob. ϵ

$$\min_{P_X} \max_{R_Y} \beta_\epsilon(P_{XY}, P_X \times R_Y) \leq \frac{1}{M}.$$

PPV converse

If there exists a code of size M with distribution P_X for channel input X, and error prob. ϵ, then for all distributions R_Y on Y:

$$\beta_\epsilon(P_{XY}, P_X \times R_Y) \le \frac{1}{M}.$$

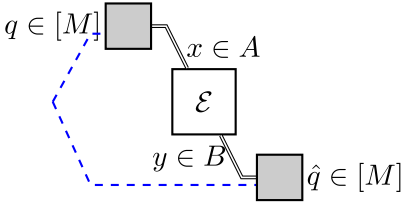
For *all* codes of size M and error prob. ϵ

$$\min_{P_X} \max_{R_Y} \beta_\epsilon(P_{XY}, P_X \times R_Y) \le \frac{1}{M}.$$

PPV converse:

$$M_\epsilon(W) \le M_\epsilon^\diamond(W) := \max_{P_X} \min_{R_Y} \frac{1}{\beta_\epsilon(P_{XY}, P_X \times R_Y)}$$

Non-signalling assisted codes: Minimum error LP



$$\epsilon^{\mathrm{NS}}(M,\mathcal{E}) := 1 - \max \frac{1}{M} \sum_{q\in[M]} \sum_{x\in A} \sum_{y \in B} Z(x,q|q,y)\mathcal{E}(y|x)$$

subject to

$$\forall \hat{q} \in [M], y \in B : \sum_{x,\hat{q}} Z(x,\hat{q}|q,y) = 1, Z \geq 0$$

$$\forall \hat{q}, y, q, q' : \sum_{x\in A} Z(x,\hat{q}|q,y) = \sum_{x \in A} Z(x,\hat{q}|q',y)$$

$$\forall x, q, y, y' : \sum_{\hat{q}\in[M]} Z(x,\hat{q}|q,y) = \sum_{\hat{q}\in[M]} Z(x,\hat{q}|q,y')$$

Simplified LP

Let $\pi(q)$ denote the image of $q \in [M]$ under permutation $\pi \in S_M$.

$$\bar{Z}(x, \hat{q}|q, y) = \frac{1}{M!} \sum_{\pi \in S_M} Z(x, \pi(\hat{q})|\pi(q), y)$$

Simplified LP

Let $\pi(q)$ denote the image of $q \in [M]$ under permutation $\pi \in S_M$.

$$\bar{Z}(x, \hat{q}|q, y) = \frac{1}{M!} \sum_{\pi \in S_M} Z(x, \pi(\hat{q})|\pi(q), y)$$

$\bar{Z}$ is still NS, yields same error prob. and it is symmetric under simultaneous permutation of q and $\hat{q}$.

Simplified LP

Let $\pi(q)$ denote the image of $q \in [M]$ under permutation $\pi \in S_M$.

$$\bar{Z}(x, \hat{q}|q, y) = \frac{1}{M!} \sum_{\pi \in S_M} Z(x, \pi(\hat{q})|\pi(q), y)$$

$\bar{Z}$ is still NS, yields same error prob. and it is symmetric under simultaneous permutation of q and $\hat{q}$.
This symmetry is equivalent to Z having the form:

$$\bar{Z}(x, \hat{q}|q, y) = \begin{cases} D_{xy} & \text{if } \hat{q} = q \\ W_{xy} & \text{if } \hat{q} \neq q. \end{cases}$$

Simplified LP

Let $\pi(q)$ denote the image of $q \in [M]$ under permutation $\pi \in S_M$.

$$\bar{Z}(x, \hat{q}|q, y) = \frac{1}{M!} \sum_{\pi \in S_M} Z(x, \pi(\hat{q})|\pi(q), y)$$

$\bar{Z}$ is still NS, yields same error prob. and it is symmetric under simultaneous permutation of q and $\hat{q}$.
This symmetry is equivalent to Z having the form:

$$\bar{Z}(x, \hat{q}|q, y) = \begin{cases} D_{xy} & \text{if } \hat{q} = q \\ W_{xy} & \text{if } \hat{q} \neq q. \end{cases}$$

Substitute this form into the LP for the error...

Simplified LP

$$\epsilon^{\mathrm{NS}}(M,\mathcal{E}) := 1 - \max \frac{1}{M} \sum_{q\in[M]} \sum_{x\in A} \sum_{y\in B} Z(x,q|q,y)\mathcal{E}(y|x)$$

$$\forall \hat{q} \in [M], y \in B : \sum_{x,\hat{q}} Z(x,\hat{q}|q,y) = 1$$

$$Z \geq 0$$

$$\forall \hat{q}, y, q, q' : \sum_{x\in A} Z(x,\hat{q}|q,y) = \sum_{x\in A} Z(x,\hat{q}|q',y)$$

$$\forall x, q, y, y' : \sum_{\hat{q}\in[M]} Z(x,\hat{q}|q,y) = \sum_{\hat{q}\in[M]} Z(x,\hat{q}|q,y')$$

Simplified LP

$$\epsilon^{\mathrm{NS}}(M,\mathcal{E}) := 1 - \max \sum_{x\in A}\sum_{y\in B} D_{xy}\mathcal{E}(y|x)$$

$$\forall \hat{q} \in [M], y \in B : \sum_{x,\hat{q}} Z(x,\hat{q}|q,y) = 1$$

$$Z \geq 0$$

$$\forall \hat{q}, y, q, q' : \sum_{x\in A} Z(x,\hat{q}|q,y) = \sum_{x\in A} Z(x,\hat{q}|q',y)$$

$$\forall x, q, y, y' : \sum_{\hat{q}\in[M]} Z(x,\hat{q}|q,y) = \sum_{\hat{q}\in[M]} Z(x,\hat{q}|q,y')$$

Simplified LP

$$\epsilon^{\mathrm{NS}}(M,\mathcal{E}) := 1 - \max \sum_{x\in A}\sum_{y\in B} D_{xy}\mathcal{E}(y|x)$$

$$\forall y \in B : \sum_{x} D_{xy} + (M-1)W_{xy} = 1$$

$$R \geq 0, W \geq 0$$

$$\forall \hat{q}, y, q, q' : \sum_{x\in A} Z(x,\hat{q}|q,y) = \sum_{x\in A} Z(x,\hat{q}|q',y)$$

$$\forall x, q, y, y' : \sum_{\hat{q}\in[M]} Z(x,\hat{q}|q,y) = \sum_{\hat{q}\in[M]} Z(x,\hat{q}|q,y')$$

Simplified LP

$$\epsilon^{\mathrm{NS}}(M,\mathcal{E}) := 1 - \max \sum_{x\in A}\sum_{y\in B} D_{xy}\mathcal{E}(y|x)$$

$$\forall y \in B : \sum_{x} D_{xy} + (M-1)W_{xy} = 1$$

$$R \geq 0, W \geq 0$$

$$\forall y \in B : \sum_{x\in A} D_{xy} = \sum_{x\in A} W_{xy}$$

$$\forall x, q, y, y' : \sum_{\hat{q}\in[M]} Z(x,\hat{q}|q,y) = \sum_{\hat{q}\in[M]} Z(x,\hat{q}|q,y')$$

Simplified LP

$$\epsilon^{\mathrm{NS}}(M,\mathcal{E}) := 1 - \max \sum_{x\in A}\sum_{y\in B} D_{xy}\mathcal{E}(y|x)$$

$$\forall y \in B : \sum_{x} D_{xy} + (M-1)W_{xy} = 1$$

$$R \geq 0, W \geq 0$$

$$\forall y \in B : \sum_{x\in A} D_{xy} = \sum_{x\in A} W_{xy}$$

$$\forall x, y : D_{xy} + (M-1)W_{xy} = p_x$$

Simplified LP

$$\epsilon^{\mathrm{NS}}(M,\mathcal{E}) := 1 - \max \sum_{x\in A}\sum_{y\in B} D_{xy}\mathcal{E}(y|x)$$

subject to

$$\forall y \in B : \sum_{x\in A} D_{xy} = 1/M (= \gamma)$$

$$\sum_{x\in A} p_x = 1,$$

$$\forall x \in A, y \in B : D_{xy} \geq p_x,$$

$$\forall x \in A, y \in B : D_{xy} \geq 0.$$

LP for M_ϵ^{NS}

Can rewrite to find the smallest value of $1/M$ for a given ϵ:

$$M_\epsilon^{\mathrm{NS}}(\mathcal{E})^{-1} = \min \gamma$$
$$\forall x \in A, y \in B : D_{xy} \leq p_x$$
$$\forall y \in B : \sum_{x \in A} D_{xy} \leq \gamma$$
$$\sum_{x \in A} \sum_{y \in B} \mathcal{E}(y|x) D_{xy} \geq 1 - \epsilon$$
$$\sum_{x \in A} p_x = 1$$
$$\forall x \in A, y \in B : D_{xy} \geq 0, p_x \geq 0.$$

LP for M_ϵ^{NS}

Can rewrite to find the smallest value of $1/M$ for a given ϵ:

$$
\begin{aligned}
&M_\epsilon^{\mathrm{NS}}(\mathcal{E})^{-1} = \min \gamma \\
&\forall x \in A, y \in B : D_{xy} \leq p_x \\
&\forall y \in B : \sum_{x \in A} D_{xy} \leq \gamma \\
&\sum_{x \in A} \sum_{y \in B} \mathcal{E}(y|x) D_{xy} \geq 1 - \epsilon \\
&\sum_{x \in A} p_x = 1 \\
&\forall x \in A, y \in B : D_{xy} \geq 0, p_x \geq 0.
\end{aligned}
$$

Also gives a converse for classical codes: $M_\epsilon(\mathcal{E}) \leq M_\epsilon^{\mathrm{NS}}(\mathcal{E})$.

Equivalence to PPV converse

The PPV converse is

$$M_\epsilon^\diamond(\mathcal{E})^{-1} = \min_p \max_r \min_T \sum_{x\in A}\sum_{y\in B} T_{xy} p_x r_y$$

subject to

$$\sum_{x\in A}\sum_{y\in B} \mathcal{E}(y|x) T_{xy} p_x \geq 1-\epsilon$$

$$\sum_x p_x = 1, \sum_y r_y = 1$$

$$\forall x \in A, y \in B : p_x \geq 0, 0 \leq T_{xy} \leq 1, r_y \geq 0$$

Equivalence to PPV converse

The PPV converse is

$$M_\epsilon^\diamond(\mathcal{E})^{-1} = \min_p \min_T \max_r \sum_{x\in A} \sum_{y\in B} T_{xy} p_x r_y$$

subject to

$$\sum_{x\in A} \sum_{y\in B} \mathcal{E}(y|x) T_{xy} p_x \geq 1 - \epsilon$$

$$\sum_x p_x = 1, \sum_y r_y = 1$$

$$\forall x \in A, y \in B : p_x \geq 0, 0 \leq T_{xy} \leq 1, r_y \geq 0$$

By von Neumann's minimax theorem.

Equivalence to PPV converse

The PPV converse is

$$M_\epsilon^\diamond(\mathcal{E})^{-1} = \min_p \min_T \max_{y\in B} \sum_{x\in A} T_{xy} p_x$$

subject to

$$\sum_{x\in A} \sum_{y\in B} \mathcal{E}(y|x) T_{xy} p_x \geq 1 - \epsilon$$

$$\sum_x p_x = 1$$

$$\forall x \in A, y \in B : p_x \geq 0, 0 \leq T_{xy} \leq 1$$

By convexity of optimisation over r.

Equivalence to PPV converse

The PPV converse is

$$M_\epsilon^\diamond(\mathcal{E})^{-1} = \min_{D,p} \max_{y\in B} \sum_{x\in A} D_{xy}$$

subject to

$$\sum_{x\in A}\sum_{y\in B}\mathcal{E}(y|x)D_{xy} \geq 1-\epsilon$$

$$\sum_{x} p_x = 1$$

$$\forall x \in A, y \in B : p_x \geq 0, 0 \leq T_{xy} \leq 1$$

$$D_{xy} := T_{xy}p_x$$

Equivalence to PPV converse

The PPV converse is

$$M_\epsilon^\diamond(\mathcal{E})^{-1} = \min_{D,p} \max_{y \in B} \sum_{x \in A} D_{xy}$$

subject to

$$\sum_{x \in A} \sum_{y \in B} \mathcal{E}(y|x) D_{xy} \geq 1 - \epsilon$$

$$\sum_x p_x = 1$$

$$\forall x \in A, y \in B : p_x \geq 0, 0 \leq D_{xy} \leq p_x,$$

$$D_{xy} := T_{xy} p_x$$

Equivalence to PPV converse

The PPV converse is

$$M_\epsilon^\diamond(\mathcal{E})^{-1} = \min_{D,p} \gamma$$

subject to

$$\sum_{x\in A} \sum_{y\in B} \mathcal{E}(y|x) D_{xy} \geq 1 - \epsilon$$

$$\sum_x p_x = 1$$

$$\forall x \in A, y \in B : p_x \geq 0, 0 \leq D_{xy} \leq p_x,$$

$$y \in B : \gamma \geq \sum_{x\in A} D_{xy}$$

$$D_{xy} := T_{xy} p_x$$

Equivalence to PPV converse

The PPV converse is

$$M_\epsilon^\diamond(\mathcal{E})^{-1} = \min_{D,p} \gamma$$

subject to

$$\sum_{x\in A}\sum_{y\in B}\mathcal{E}(y|x)D_{xy} \geq 1-\epsilon$$

$$\sum_x p_x = 1$$

$$\forall x \in A, y \in B : p_x \geq 0, 0 \leq D_{xy} \leq p_x,$$

$$y \in B : \gamma \geq \sum_{x\in A} D_{xy}$$

$$M_\epsilon^\diamond(\mathcal{E}) = M_\epsilon^{\mathrm{NS}}(\mathcal{E})$$

Consequences

All converse results which can be derived from PPV converse apply to non-signalling and entanglement assisted codes too (for discrete channels):

Consequences

All converse results which can be derived from PPV converse apply to non-signalling and entanglement assisted codes too (for discrete channels):

- Non-signalling doesn't change capacity for completely general channels (using result of Verdú and Han).

Consequences

All converse results which can be derived from PPV converse apply to non-signalling and entanglement assisted codes too (for discrete channels):

- Non-signalling doesn't change capacity for completely general channels (using result of Verdú and Han).
- Asymptotic expansion of rate unchanged by NS/entanglement assistance up to $O(\log n)/n$.

Consequences

All converse results which can be derived from PPV converse apply to non-signalling and entanglement assisted codes too (for discrete channels):

- Non-signalling doesn't change capacity for completely general channels (using result of Verdú and Han).
- Asymptotic expansion of rate unchanged by NS/entanglement assistance up to $O(\log n)/n$.

Linear program formulation of the PPV converse:

Consequences

All converse results which can be derived from PPV converse apply to non-signalling and entanglement assisted codes too (for discrete channels):

- Non-signalling doesn't change capacity for completely general channels (using result of Verdú and Han).
- Asymptotic expansion of rate unchanged by NS/entanglement assistance up to $O(\log n)/n$.

Linear program formulation of the PPV converse:

- *Dual* formulation of LP gives a converse bound for any feasible point.

Consequences

All converse results which can be derived from PPV converse apply to non-signalling and entanglement assisted codes too (for discrete channels):

- Non-signalling doesn't change capacity for completely general channels (using result of Verdú and Han).
- Asymptotic expansion of rate unchanged by NS/entanglement assistance up to $O(\log n)/n$.

Linear program formulation of the PPV converse:

- *Dual* formulation of LP gives a converse bound for any feasible point.
- For channels with permutation covariance (e.g. DMCs), LP can be simplified to size poly(n).

Dispersionless channels

- Information density: $i(a;b) = \log \frac{\Pr(X=a, Y=b)}{\Pr(X=a)\Pr(Y=b)}$.

Dispersionless channels

- Information density: $i(a;b) = \log \frac{\Pr(X=a, Y=b)}{\Pr(X=a)\Pr(Y=b)}$.
- Capacity $C(\mathcal{E})$ is max. of expectation of information density over input distributions.

Dispersionless channels

- Information density: $i(a;b) = \log \frac{\Pr(X=a, Y=b)}{\Pr(X=a)\Pr(Y=b)}$.
- Capacity $C(\mathcal{E})$ is max. of expectation of information density over input distributions.
- Dispersion $V(\mathcal{E})$: Minimum variance of information density for capacity achieving input distributions.

Dispersionless channels

- Information density: $i(a;b) = \log \frac{\Pr(X{=}a, Y{=}b)}{\Pr(X{=}a)\Pr(Y{=}b)}$.
- Capacity $C(\mathcal{E})$ is max. of expectation of information density over input distributions.
- Dispersion $V(\mathcal{E})$: Minimum variance of information density for capacity achieving input distributions.

$$\frac{1}{n}\log M_\epsilon(\mathcal{E}^n) = C(\mathcal{E}) - Q^{-1}(\epsilon)\sqrt{\frac{V(\mathcal{E})}{n}} + O(\log n)/n$$

Dispersionless channels

- Information density: $i(a;b) = \log \frac{\Pr(X=a, Y=b)}{\Pr(X=a)\Pr(Y=b)}$.
- Capacity $C(\mathcal{E})$ is max. of expectation of information density over input distributions.
- Dispersion $V(\mathcal{E})$: Minimum variance of information density for capacity achieving input distributions.

$$\frac{1}{n} \log M_\epsilon(\mathcal{E}^n) = C(\mathcal{E}) - Q^{-1}(\epsilon)\sqrt{\frac{V(\mathcal{E})}{n}} + O(\log n)/n$$

For DMCs

$$C_0^{\text{NS}}(\mathcal{E}) = C(\mathcal{E}) \iff V(\mathcal{E}) = 0.$$

Future work

- Use dual LP formulation of converse to improve efficiently computable finite block length bounds for specific channels.

Future work

- Use dual LP formulation of converse to improve efficiently computable finite block length bounds for specific channels.
- Improved bounds for small block lengths by augmenting LP with certain families of Bell inequalities?

Future work

- Use dual LP formulation of converse to improve efficiently computable finite block length bounds for specific channels.
- Improved bounds for small block lengths by augmenting LP with certain families of Bell inequalities?
- Non-signalling converse generalises naturally to multi-terminal coding - investigate applications.

Future work

- Use dual LP formulation of converse to improve efficiently computable finite block length bounds for specific channels.
- Improved bounds for small block lengths by augmenting LP with certain families of Bell inequalities?
- Non-signalling converse generalises naturally to multi-terminal coding - investigate applications.