UTS:QSI
CENTRE FOR QUANTUM SOFTWARE AND INFORMATION
Hao-Chung Cheng, Min-Hsiu Hsieh

Operational Duality between Classical Source Coding with QSI and C-Q Channel Coding

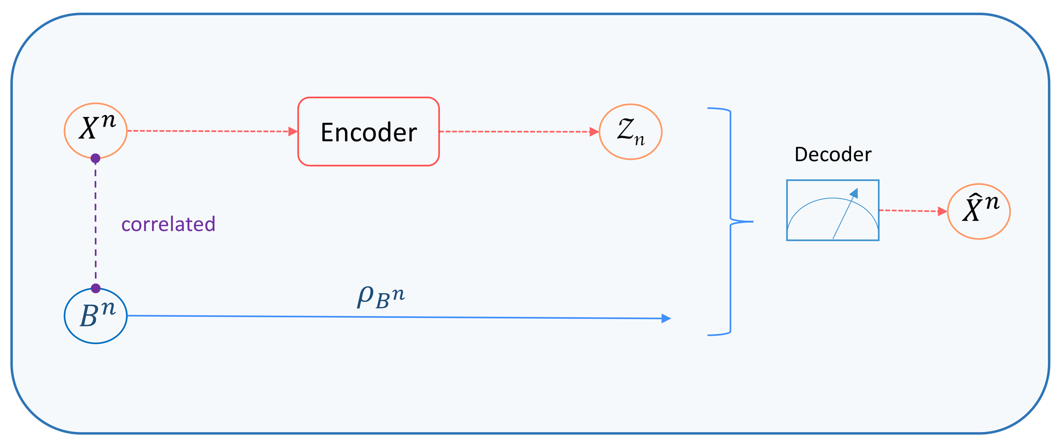
Entropic bounds: arXiv/1803.07505; operational duality: in preparation.

UNIVERSITY OF CAMBRIDGE
Eric P. Hanson, Nilanjana Datta

Quantum Information Protocols

Classical-quantum Slepian-Wolf source coding for blocklength n

$$\rho_{XB} = \sum_{x\in\mathcal{X}} P_X(x)\,|x\rangle\langle x| \otimes \rho_B^x$$



Decoder: a POVM on B^n for each $z \in \mathcal{Z}_n$.
Entropic bounds:

$$E_r^{\downarrow}(R) \lessapprox e_s(n,R) \lessapprox E_{sp}(R)$$

where

$$E_r^{\downarrow}(R) := \sup_{\frac{1}{2}\le\alpha\le1} \frac{1-\alpha}{\alpha}\left(R - H^{\downarrow}_{2-\frac{1}{\alpha}}(X|B)_\rho\right),$$

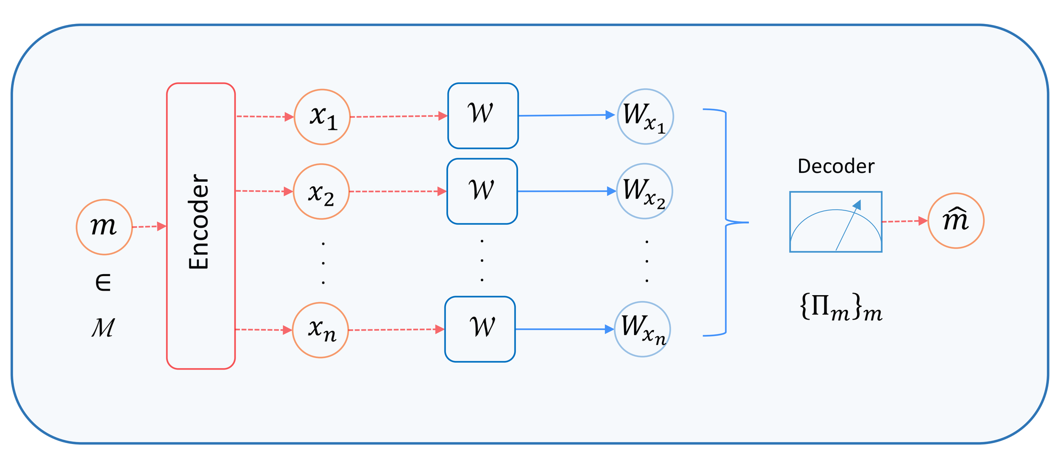
$$E_{sp}(R) := \sup_{0\le\alpha\le1} \frac{1-\alpha}{\alpha}\left(R - H^{\uparrow}_{\alpha}(X|B)_\rho\right).$$

- Compression rate
  - fixed-length coding: $R := \frac{1}{n}\log|\mathcal{Z}_n|$
  - variable-length coding: $\bar{R} := \frac{1}{n}\mathbb{E}\left[\mathsf{length}(\mathcal{E}(X^n))\right]$
- Sources
  - iid sources: $\Pr[X^n] = \Pi_{i=1}^n P_X(x_i)$
  - type class $T_Q^n := \{x^n : Q(x) = \frac{1}{n}\sum_{i=1}^n 1_{\{x_i = x\}}\}$
  - source of type Q: $\Pr[X^n] = \frac{1}{|T_Q^n|} 1_{\{X^n \in T_Q^n\}}$
- Error probability for a code $\mathcal{C} = (\mathcal{E},\mathcal{D})$

$$\mathrm{P_e}(\mathcal{C}) := \Pr\left[\hat{X} \ne X\right] = 1 - \sum_{x^n\in\mathcal{X}^n} \Pr[x^n]\,\mathrm{Tr}\left[\rho_{B^n}^{x^n} \Pi_{x^n}^{(\mathcal{E}(x^n))}\right]$$

where $\rho_{B^n}^{x^n} = \rho_B^{x_1} \otimes\cdots\otimes \rho_B^{x_n}$ for $x^n = (x_1,\dots,x_n)$.
  - optimal error prob. for iid source $\rho_{XB}^{\otimes n}$: $P_e^\star(n,R)$
  - optimal error prob. for source of type Q: $P_e^\star(n,R,Q)$
- Error exponents
  - fixed-length & iid: $e_s(n,R) := -\frac{1}{n}\log P_e^\star(n,R)$
  - fixed-length & of type Q: $e_s(n,R,Q) := -\frac{1}{n}\log P_e^\star(n,R,Q)$
  - variable-length & iid: $e_v(n,\bar{R}) := -\frac{1}{n}\log P_e^\star(n,\bar{R})$

Classical-quantum channel coding for blocklength n



$$E^{\downarrow}_{r,ch}(R,Q) \lessapprox e_c(n,R,Q) \lessapprox E_{sp,ch}(R,Q)$$

$$E^{\downarrow}_{r,ch}(R,Q) := \sup_{\frac{1}{2}\le\alpha\le1} \frac{1-\alpha}{\alpha}\left(I^{\downarrow}_{2-\frac{1}{\alpha}}(Q,\mathcal{W}) - R\right)$$

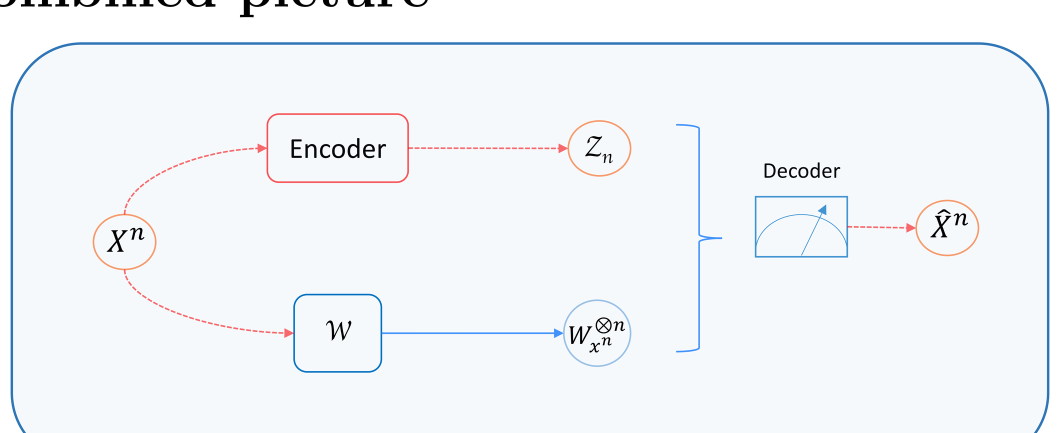
$$E_{sp,ch}(R,Q) := \sup_{0\le\alpha\le1} \frac{1-\alpha}{\alpha}\left(I^{\uparrow}_{\alpha}(Q,\mathcal{W}) - R\right)$$

- Transmission rate: $R := \frac{1}{n}\log|\mathcal{M}|$
- Codes with fixed type: $\{x^n(m)\}_{m\in\mathcal{M}} \subset T_Q^n$
- Error probability:

$$\mathrm{P_e} := \Pr[\hat{m} \ne m] = 1 - \frac{1}{|\mathcal{M}|}\sum_{m\in\mathcal{M}} \mathrm{Tr}\left[W_{x^n(m)}^{\otimes n}\Pi_m\right]$$

  - Optimal error probability over all codes with fixed type Q and rate R: $P_e^\star(n,R,Q)$
- Error exponent:
  $e_c(n,R,Q) := -\frac{1}{n}\log P_e^\star(n,R,Q)$

Combined picture



- Source of type Q has $\approx nH(Q)$ bits of info.
- Source encoder provides nR bits to decoder
- QSI induces a c-q channel $\mathcal{W} : x \mapsto W_x := \rho_B^x$
- The decoder needs $n(H(Q) - R)$ bits from the c-q channel to recover the source
  - ⇝ A c-q channel code of rate $H(Q) - R$ solves the source coding task
  - ⇝ Solving the source coding task at rate R implicitly solves the c-q channel coding task

Main Results

Operational duality of error exponents:

$$e_s(n,R,Q) \approx e_c(n, H(Q) - R, Q)$$

$$e_s(n,R) \approx \min_Q \{e_c(n, H(Q)-R, Q) + D(Q\|P_X)\}$$

$$e_v(n,R) \approx e_c(n, H(P_X) - R, P_X)$$

Entropic duality of error exponents:

$$E_r^{\downarrow}(R,Q) = E^{\downarrow}_{r,ch}(H(Q)-R, Q)$$

$$E_{sp}(R,Q) = E_{sp,ch}(H(Q)-R,Q)$$

$$E_r^{\downarrow}(R) = \min_Q\left\{E_r^{\downarrow}(R,Q) + D(Q\|P_X)\right\}$$

$$E_{sp}(R) = \min_Q\left\{E_{sp}(R,Q) + D(Q\|P_X)\right\}$$

Type decomposition of the iid source

$$(\rho_{XB})^{\otimes n} \overset{\text{iid}}{=} \sum_{x^n\in\mathcal{X}^n} \Pr[x^n]\,|x^n\rangle\langle x^n| \otimes \rho_{B^n}^{x^n} = \sum_{Q\in\mathcal{P}_n(\mathcal{X}^n)} \Pr[x^n \in T_Q^n]\,\rho_{X^nB^n}^{(Q)}. \qquad (\star)$$

where $\rho_{X^nB^n}^{(Q)} := \frac{1}{|T_Q^n|}\sum_{x^n\in T_Q^n} |x^n\rangle\langle x^n| \otimes \rho_{B^n}^{x^n}$.

Entropic quantities

- (Petz)-Rényi relative entropy

$$D_\alpha(\rho\|\sigma) := \frac{1}{\alpha-1}\log\mathrm{tr}\left[\rho^\alpha\sigma^{1-\alpha}\right]$$

- Rényi conditional entropies

$$H_\alpha^{\downarrow}(X|B)_\rho := -D_\alpha(\rho_{XB}\|\mathbb{1}_X \otimes \rho_B)$$

$$H_\alpha^{\uparrow}(X|B)_\rho := \max_{\sigma_B} -D_\alpha(\rho_{XB}\|\mathbb{1}_X \otimes \sigma_B)$$

- Rényi mutual informations

$$I_\alpha^{\downarrow}(Q,\mathcal{W}) := \sum_{x\in\mathcal{X}} Q(x) D_\alpha(W_x\|\textstyle\sum_y Q(y)W_y)$$

$$I_\alpha^{\uparrow}(Q,\mathcal{W}) := \inf_\sigma \sum_{x\in\mathcal{X}} Q(x) D_\alpha(W_x\|\sigma)$$

Proof Ideas

Building source codes from channel codes

Ahlswede's type covering lemma (1980): For any nonempty subset $\mathcal{U} \subset T_Q^n$, there exist a set of L permutations $\pi_1,\dots,\pi_L$ such that

$$\bigcup_{i=1}^{\Lambda} \pi_i\mathcal{U} = T_Q^n,$$

$$L := \lceil |\mathcal{U}|^{-1}|T_Q^n|\log|T_Q^n|\rceil,$$

where $\pi_i\mathcal{U} := \{\pi_i\mathbf{u} : \mathbf{u}\in\mathcal{U}\}$.

- Optimal channel code with rate $H(Q) - R$ has a codebook $\mathcal{U} \subset T_Q^n$ and decoder $\{\Lambda_m\}_{m\in\mathcal{M}}$
- Source encoder compresses $x^n \in T_Q^n$ by sending $i \in \{1,\dots,L\}$ such that $\pi_i^{-1}x^n \in \mathcal{U}$; note $L \approx 2^{nR}$.
- Source decoder rotates channel decoder using π_i and measures the QSI.
- The error probability of the constructed source code is controlled by the error of the optimal channel code, because we are using its encoder and decoder (up to permutations)

Building channel codes from source codes

- Source code $\mathcal{C} = (\mathcal{E},\mathcal{D})$ of rate $R = \frac{1}{n}\log|\mathcal{Z}|$.
- Using source encoder, define $S_z = \mathcal{E}^{-1}(z) \subset T_Q^n$ for $z \in \mathcal{Z}$. Each S_z is a possible codebook for the c-q channel $x \mapsto \rho_B^x$ (source decoder conditioned on z gives a channel decoder).
- Pigeonhole arguments: there exists $z \in \mathcal{Z}$ such that $|S_z| \ge \frac{1}{n+1}|T_Q^n|\cdot|\mathcal{Z}|^{-1} \approx \exp(n(H(Q) - R))$ and the average probability of channel coding error using this codebook is at most $\frac{n+1}{n}P_e(\mathcal{C})$.

Duality for iid source

- We simply combine $(\star)$, the estimate

$$\Pr[x^n \in T_Q^n] \approx \exp(-nD(Q\|P_X)),$$

and the duality $e_s(n,R,Q) \approx e_c(n,H(Q)-R,Q)$.

Variable length source coding

- Sequences with type $Q \not\approx P_X$: compress losslessly (does not contribute to the rate asymptotically)
- Sequences with type $Q \approx P_X$: encode using the constant type duality (contributes to the rate)