On the Duality Between the BSC and Quantum PSC

Narayanan Rengaswamy
The University of Arizona

Joint Work: Henry D. Pfister
Duke University

ISIT 2021

CODE AND CHANNEL DUALITY

- Binary linear code $C \subseteq \mathbb{F}_2^n$

  $\Rightarrow$ Dual code $C^\perp = \{ x \in \mathbb{F}_2^n \mid xy^T = 0 \ \forall y \in C \}$

Duality based on linear algebra

– Hartmann-Rudolph [IT '76]

$$\sum_{x \in C} \prod_{j=1}^{n} \mu_j(x_j) = 2^{k-\frac{n}{2}} \sum_{\hat{x} \in C^\perp} \prod_{j=1}^{n} \underbrace{\hat{\mu}_j(\hat{x}_j)}_{\text{FT of } \mu_j}$$

Code and Channel Duality

- Binary linear code $C \subseteq \mathbb{F}_2^n$
  $\Rightarrow$ Dual code $C^{\perp} = \{ x \in \mathbb{F}_2^n \mid x y^T = 0 \ \forall y \in C \}$

Duality based on linear algebra

— Hartmann-Rudolph [IT '76]

$$\sum_{x \in C} \prod_{j=1}^{n} \mu_j(x_j) = 2^{k-\frac{n}{2}} \sum_{\hat{x} \in C^{\perp}} \prod_{j=1}^{n} \underbrace{\hat{\mu}_j(\hat{x}_j)}_{\text{FT of } \mu_j}$$

- Is there a theory of duality for channels?

BINARY ERASURE CHANNEL (BEC)

- Capacity: $\underbrace{I(\mathrm{BEC}(\varepsilon))}_{=1-\varepsilon} + \underbrace{I(\mathrm{BEC}(1-\varepsilon))}_{=\varepsilon} = 1$

- Performance of C on $\mathrm{BEC}(\varepsilon)$ completely characterized by performance of $C^\perp$ on $\mathrm{BEC}(1-\varepsilon)$

$x \in C \longrightarrow$ Erased indices $\mathcal{E} \longrightarrow$

$y \in C^\perp \longrightarrow$ Erased indices $\mathcal{E}^c \longrightarrow$

BINARY ERASURE CHANNEL (BEC)

- **Capacity**: $\underbrace{I(BEC(\varepsilon))}_{=1-\varepsilon} + \underbrace{I(BEC(1-\varepsilon))}_{=\varepsilon} = 1$

- Performance of C on $BEC(\varepsilon)$ completely characterized by performance of $C^{\perp}$ on $BEC(1-\varepsilon)$

$x \in C \longrightarrow$ Erased indices $\mathcal{E} \longrightarrow$ i^{th} bit can't be recovered

IF AND ONLY IF

$y \in C^{\perp} \longrightarrow$ Erased indices $\mathcal{E}^c \longrightarrow$ i^{th} bit can be recovered

EXTEND CHANNEL DUALITY BEYOND BEC?

CQ $\Rightarrow$ classical input quantum output

Renes [IT'18] proposed a dual CQ channel

Entropic Duality: $H(W) + H^{\perp}(W^{\perp}) = \log d$ ← dim. of inp

Shannon Entropy : $H^{\perp} = H$ → input uncertainty given output

Dual Entropies - See "Quantum Information Processing with Finite Resources" by Marco Tomamichel

EXTEND CHANNEL DUALITY BEYOND BEC?

CQ ⇒ classical input quantum output

Renes [IT'18] proposed a dual CQ channel

Entropic Duality: $H(W) + H^{\perp}(W^{\perp}) = \log d$ ← dim. of inp

Shannon Entropy : $H^{\perp} = H$ → input uncertainty given output

Coding (block error rate) and Secrecy (input decoupling):

$$H = H_{min},\ H^{\perp} = H_{max} \Rightarrow P(W) = 2^{-H_{min}(W)} = \frac{1}{d} 2^{H_{max}(W^{\perp})} = Q(W^{\perp})$$

TALK AGENDA

Consider $W = PSC(\theta)$, $W^{\perp} = BSC\left(p = \frac{1-\cos\theta}{2}\right)$

Prove $P(W) = B(\text{posterior}, \text{uniform})^2 = Q(W^{\perp})$

coding on PSC
(block success rate)

Secrecy on BSC
(distance between eavesdropper's posterior on secret message and uniform distribution)

TALK AGENDA

Consider $W = PSC(\theta)$, $W^{\perp} = BSC\left(p = \frac{1-\cos\theta}{2}\right)$

Prove $P(W) = B(\text{posterior}, \text{uniform})^2 = Q(W^{\perp})$

coding on PSC
(block success rate)

Secrecy on BSC
(distance between eavesdropper's posterior on secret message and uniform distribution)

OUTLINE:

1. BEC duality via entropies
2. Extend entropic approach to PSC-BSC
3. Factor graph duality to prove $P(W) = Q(W^{\perp})$

BEC Coding – Secrecy Duality

Coding/secrecy with code C: (generator G)

$$A = \begin{array}{c} \overbrace{}^{n} \\ \begin{bmatrix} G \\ F \end{bmatrix} \end{array} \begin{array}{l} \}\,k \\ \}\,n-k \end{array} : \quad X = [\,\overset{k}{U} \;\; \overset{n-k}{S}\,]A = UG + SF$$

UG: information; SF: coset selector

Coding/secrecy with code $C^\perp$: (generator H)

$$B = \begin{array}{c} \overbrace{}^{n} \\ \begin{bmatrix} E \\ H \end{bmatrix} \end{array} \begin{array}{l} \}\,k \\ \}\,n-k \end{array} : \quad X = [\,\underset{k}{S'} \;\; \underset{n-k}{U'}\,]B = S'E + U'H$$

$S'E$: coset selector; $U'H$: information

BEC Coding-Secrecy Duality

Coding/secrecy with code C: (generator G)

$$A = \begin{array}{c} n \\ \begin{bmatrix} G \\ F \end{bmatrix} \end{array} \begin{array}{l} \}k \\ \}n-k \end{array} : \quad X = \begin{array}{cc} k & n-k \\ [U & S] \end{array} A = \underbrace{UG}_{\text{information}} + \underbrace{SF}_{\text{coset selector}}$$

Coding/secrecy with code $C^\perp$: (generator H)

$$B = \begin{array}{c} n \\ \begin{bmatrix} E \\ H \end{bmatrix} \end{array} \begin{array}{l} \}k \\ \}n-k \end{array} : \quad X = \begin{array}{cc} [S' & U'] \\ k & n-k \end{array} B = \underbrace{S'E}_{\text{coset selector}} + \underbrace{U'H}_{\text{information}}$$

$$\underbrace{H(U \mid \mathcal{E}, X_{\mathcal{E}^c}, S)}_{\text{coding with } C \text{ on BEC}(\mathcal{E})} + \underbrace{H(S' \mid \mathcal{E}, X'_{\mathcal{E}})}_{\text{secrecy with cosets of } C^\perp \text{ on BEC}(\mathcal{E}^c)} = k$$

Message perfectly recovered $\Rightarrow$ maximal secrecy

Pure-State Channel (PSC)

$$\mathrm{PSC}(\theta): \quad x \in \{0,1\} \longmapsto |(-1)^x \theta\rangle := \begin{bmatrix} \cos\frac{\theta}{2} \\ (-1)^x \sin\frac{\theta}{2} \end{bmatrix} \quad \text{(qubit)}$$

Symmetry: $Z|\theta\rangle = |-\theta\rangle, \; Z|-\theta\rangle = |\theta\rangle \; ; \; Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

$$\Rightarrow \quad c \in \mathbb{F}_2^n \longrightarrow \boxed{\mathrm{PSC}(\theta)^{\otimes n}} \longrightarrow Z(c)\,|\theta\rangle^{\otimes n} \; ; \; Z(c) = \bigotimes_{i=1}^{n} Z^{c_i}$$

Pure-State Channel (PSC)

$PSC(\theta)$: $x \in \{0,1\} \longmapsto |(-1)^x \theta\rangle := \begin{bmatrix} \cos\frac{\theta}{2} \\ (-1)^x \sin\frac{\theta}{2} \end{bmatrix}$ (qubit)

Symmetry: $Z|\theta\rangle = |-\theta\rangle$, $Z|-\theta\rangle = |\theta\rangle$; $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

$\Rightarrow$ $c \in \mathbb{F}_2^n \longrightarrow \boxed{PSC(\theta)^{\otimes n}} \longrightarrow Z(c)|\theta\rangle^{\otimes n}$; $Z(c) = \bigotimes_{i=1}^{n} Z^{c_i}$

Construct matrix $\Phi_{2^n \times 2^k}$: columns are $Z(c)|\theta\rangle^{\otimes n}$, $c \in C$

$\underbrace{2^{-k}\,\Phi\Phi^\dagger}$: density matrix at channel output = equal mixture of all codewords

$\hookrightarrow$ Von Neumann entropy = Shannon entropy of eigenvalues

ENTROPIC VIEW OF PSC-BSC DUALITY

Lemma: $\Gamma = 2^{-k} \Phi^\dagger \Phi$ diagonalized by the Fourier transform on $\mathbb{Z}_2^k$. The eigenvalues of Γ and $e^{Y,S=0} = 2^{-k} \Phi \Phi^\dagger$ are $\{2^{-k/2} \hat{s}(h), h \in \mathbb{Z}_2^k\}$.

$$H(Y|S=0)_{e^{Y,S=0}} = \sum_{h \in \mathbb{Z}_2^k} \underbrace{2^{-k/2} \hat{s}(h)}_{\text{posterior for secrecy on BSC with } C^\perp!} \log \frac{1}{2^{-k/2} \hat{s}(h)} = H(S'|Y)$$

ENTROPIC VIEW OF PSC-BSC DUALITY

Lemma: $\Gamma = 2^{-k}\Phi^{\dagger}\Phi$ diagonalized by the Fourier transform on $\mathbb{Z}_2^k$. The eigenvalues of Γ and $e^{Y,S=0} = 2^{-k}\Phi\Phi^{\dagger}$ are $\{2^{-k/2}\hat{s}(h),\ h\in\mathbb{Z}_2^k\}$.

$$H(Y|S=0)_{\rho^{Y,S=0}} = \sum_{h\in\mathbb{Z}_2^k} \underbrace{2^{-k/2}\hat{s}(h)}_{\text{posterior for secrecy on BSC with } C^{\perp}!} \log\frac{1}{2^{-k/2}\hat{s}(h)} = H(S'|Y')$$

$$H(U|Y,S=0)_{\rho^{UY,S=0}} = H(U|S=0) + H(Y|U,S=0)_{\rho^{UY,S=0}} - H(Y|S=0)_{\rho^{Y,S=0}}$$

$$= k + 0 - H(S'|Y')$$

BEC: $H(U|\mathcal{E},X_{\mathcal{E}^c},S) + H(S'|\mathcal{E},X'_{\mathcal{E}}) = k$

PROOF OF $P(W) = Q(W^{\perp})$ FOR PSC-BSC

SQUARE ROOT MEASUREMENT: $\Psi := \Phi\left[(\Phi^{\dagger}\Phi)^{1/2}\right]^{-1}$
(SRM)

→ columns $\{|\psi_j\rangle, j \in [2^k]\}$ of Ψ define rank-1 projectors

→ optimal for decoding binary linear codes on PSC

$$1 - P(W) = \text{Prob.}[\text{block error}] = \frac{1}{2^k} \sum_{j \in \mathbb{Z}_2^k} \sum_{\substack{i \in \mathbb{Z}_2^k \\ i \neq j}} |\langle \psi_j | \phi_i \rangle|^2$$

need to compute

PROOF OF $P(W) = Q(W^{\perp})$ FOR PSC-BSC

SQUARE ROOT MEASUREMENT (SRM): $\Psi := \Phi\left[(\Phi^{\dagger}\Phi)^{1/2}\right]^{-1}$

→ columns $\{|\psi_j\rangle, j \in [2^k]\}$ of Ψ define rank-1 projectors

→ optimal for decoding binary linear codes on PSC

$$1 - P(W) = \text{Prob.}[\text{block error}] = \frac{1}{2^k} \sum_{j \in \mathbb{Z}_2^k} \sum_{\substack{i \in \mathbb{Z}_2^k \\ i \neq j}} \underbrace{|\langle \psi_j | \phi_i \rangle|^2}_{\text{need to compute}}$$

Eldar-Forney '01: $\Psi^{\dagger}\Phi = \mathcal{F}\Sigma\mathcal{F}^{\dagger}$, $\Sigma = \text{diag}(\{\sigma(h), h \in \mathbb{Z}_2^k\})$

$\mathcal{F}$ → Fourier transform on $\mathbb{Z}_2^k$.

$|\psi_j\rangle$ is a function of $\{\sigma(h), h \in \mathbb{Z}_2^k\}$.

Factor Graph Duality to Compute $\sigma(h)$

Overlap Function: $s(g) := \langle \theta |^{\otimes n} Z(c_g) | \theta \rangle^{\otimes n} = (\cos\theta)^{w_H(c_g)}, g \in \mathbb{Z}_2^k$

Fourier transform: $\hat{s}(h) = \frac{1}{\sqrt{2^k}} \sum_{g \in \mathbb{Z}_2^k} (-1)^{gh^T} (\cos\theta)^{w_H(c_g)}$

Eldar-Forney '01: $\sigma(h) = 2^{k/4} \sqrt{\hat{s}(h)} \leftarrow$ to be computed

Factor Graph Duality to Compute $\sigma(h)$

Overlap Function: $s(g) := \langle\theta|^{\otimes n} Z(\varsigma_g)|\theta\rangle^{\otimes n} = (\cos\theta)^{w_H(\varsigma_g)}, \; g \in \mathbb{Z}_2^k$

Fourier transform: $\hat{s}(h) = \frac{1}{\sqrt{2^k}} \sum_{g \in \mathbb{Z}_2^k} (-1)^{gh^T} (\cos\theta)^{w_H(\varsigma_g)}$

Eldar-Forney '01: $\sigma(h) = 2^{k/4} \sqrt{\hat{s}(h)} \leftarrow$ to be computed

Embed in $\mathbb{Z}_2^n$: $\hat{s}'(y) = \frac{1}{\sqrt{2^n}} \sum_{x \in \mathbb{Z}_2^n} \mathbb{I}(x \in C)\, (-1)^{xy^T} (\cos\theta)^{w_H(x)}$

Factor graph Duality: $\sum_{x \in \mathbb{Z}_2^n} \mathbb{I}(x \in C) \prod_{j=1}^{n} \mu_j(x_j) = \sum_{\hat{x} \in \mathbb{Z}_2^n} 2^{k-n/2}\, \mathbb{I}(\hat{x} \in C^\perp) \prod_{j=1}^{n} \hat{\mu}_j(\hat{x}_j)$

Completing Proof of $P(W) = Q(W^{\perp})$

Lemma: Closed form expression for $\hat{s}(h)$

$\sigma(h) = 2^{k/4}\sqrt{\hat{s}(h)}$ and $|\psi_g\rangle$ a function of $\sigma(h)$

Lemma: $|\langle\psi_g|\phi_t\rangle|^2 = \hat{\sigma}(g \oplus t)^2 / 2^k$

COMPLETING PROOF OF $P(W) = Q(W^{\perp})$

Lemma: Closed form expression for $\hat{s}(h)$

$\sigma(h) = 2^{k/4}\sqrt{\hat{s}(h)}$ and $|\psi_g\rangle$ a function of $\sigma(h)$

Lemma: $|\langle \psi_g | \phi_t \rangle|^2 = \hat{\sigma}(g \oplus t)^2 / 2^k$

Theorem: $1 - P_e(W) = P(W) = B\left(\frac{\hat{s}}{2^{k/2}}, \frac{1}{2^k}\right)^2$ ← Bhattacharyya coefficient

$$= \left[\sum_{h \in \mathbb{Z}_2^k} \sqrt{\frac{\hat{s}(h)}{2^{k/2}}} \sqrt{\frac{1}{2^k}}\right]^2 \qquad \square$$

for secrecy on BSC with $C^{\perp}$, ↗
optimal decoupling of secret from intercepted information!

CONCLUSION

- Reviewed BEC duality (coding - secrecy)
- Channel duality : $W = PSC(\theta)$, $W^{\perp} = BSC\left(\frac{1-\cos\theta}{2}\right)$

  → Generalized BEC entropic relations

  → Proved $P(W) = Q(W^{\perp})$
  avoided more complicated quantum tools

- In arXiv: 2103.09225, discuss more and also about secrecy on PSC + coding on BSC

BEC CODING DUALITY

Consider coding on $\mathrm{BEC}(\mathcal{E})$ with code C
erased indices

Let $V = \{ z \in C \mid z_{\mathcal{E}^c} = y_{\mathcal{E}^c} \}$; y = received vector

$H_{\mathcal{E}} x_{\mathcal{E}}^T = H_{\mathcal{E}^c} x_{\mathcal{E}^c}^T \Rightarrow \dim(V) = H(X \mid X_{\mathcal{E}^c}) = |\mathcal{E}| - \operatorname{rank}(H_{\mathcal{E}})$

$u G_{\mathcal{E}^c} = x_{\mathcal{E}^c} \Rightarrow \dim(V) = H(X \mid X_{\mathcal{E}^c}) = k - \operatorname{rank}(G_{\mathcal{E}^c})$

Consider coding on $\mathrm{BEC}(\mathcal{E}^c)$ with code $C^{\perp}$
erased indices

$H(X' \mid X'_{\mathcal{E}}) = |\mathcal{E}^c| - \operatorname{rank}(H^{\perp}_{\mathcal{E}^c}) = |\mathcal{E}^c| - \operatorname{rank}(G_{\mathcal{E}^c})$

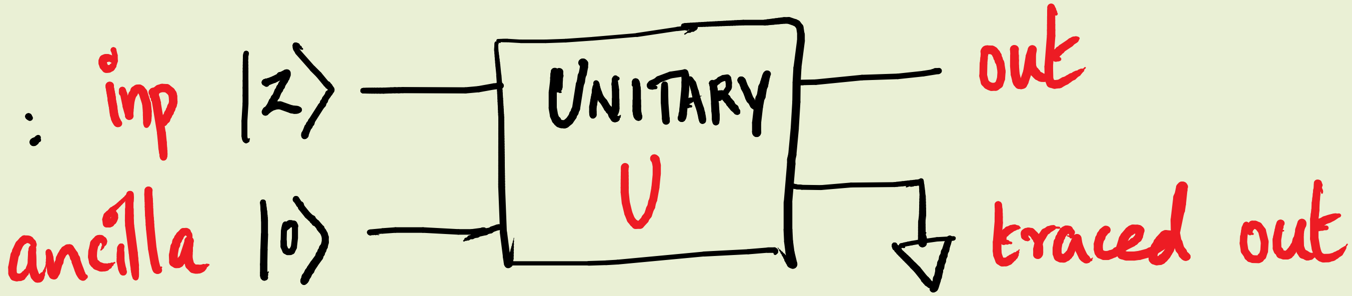
$\Rightarrow \quad H(X' \mid X'_{\mathcal{E}}) = H(X \mid X_{\mathcal{E}^c}) + |\mathcal{E}^c| - k$

EXTEND CHANNEL DUALITY BEYOND BEC?

CQ $\Rightarrow$ classical input quantum output

Renes [IT'18] proposed a dual CQ channel

<u>Primal</u> (W):



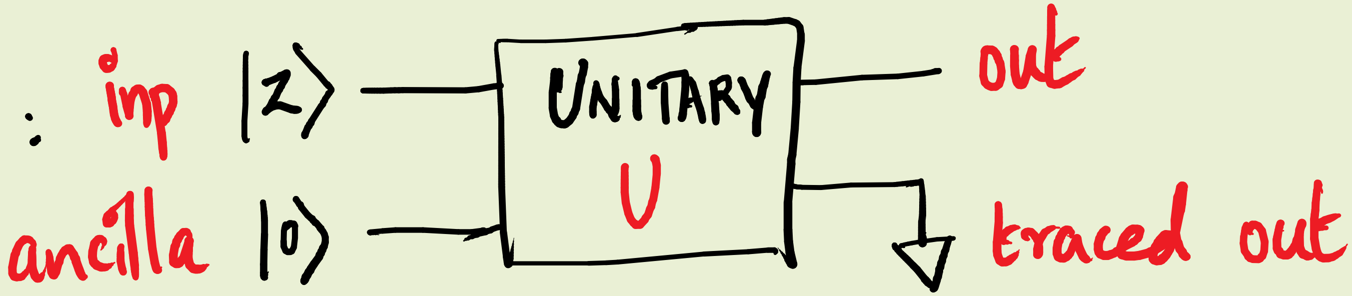
Stinespring's representation of quantum channels

EXTEND CHANNEL DUALITY BEYOND BEC?

CQ $\Rightarrow$ classical input quantum output

Renes [IT'18] proposed a dual CQ channel

Primal (W):



FT of $\{|z\rangle : z \in \mathbb{Z}_d\}$

Dual ($W^{\perp}$):