Joseph M. Renes, ETH Zürich

BIID 10, 2022-09-29

$$E_r(R) = \max_{0\le\rho\le 1} \max_{\mathbf{Q}} [E_o(\rho,\mathbf{Q}) - \rho R] \qquad (5.6.16)$$

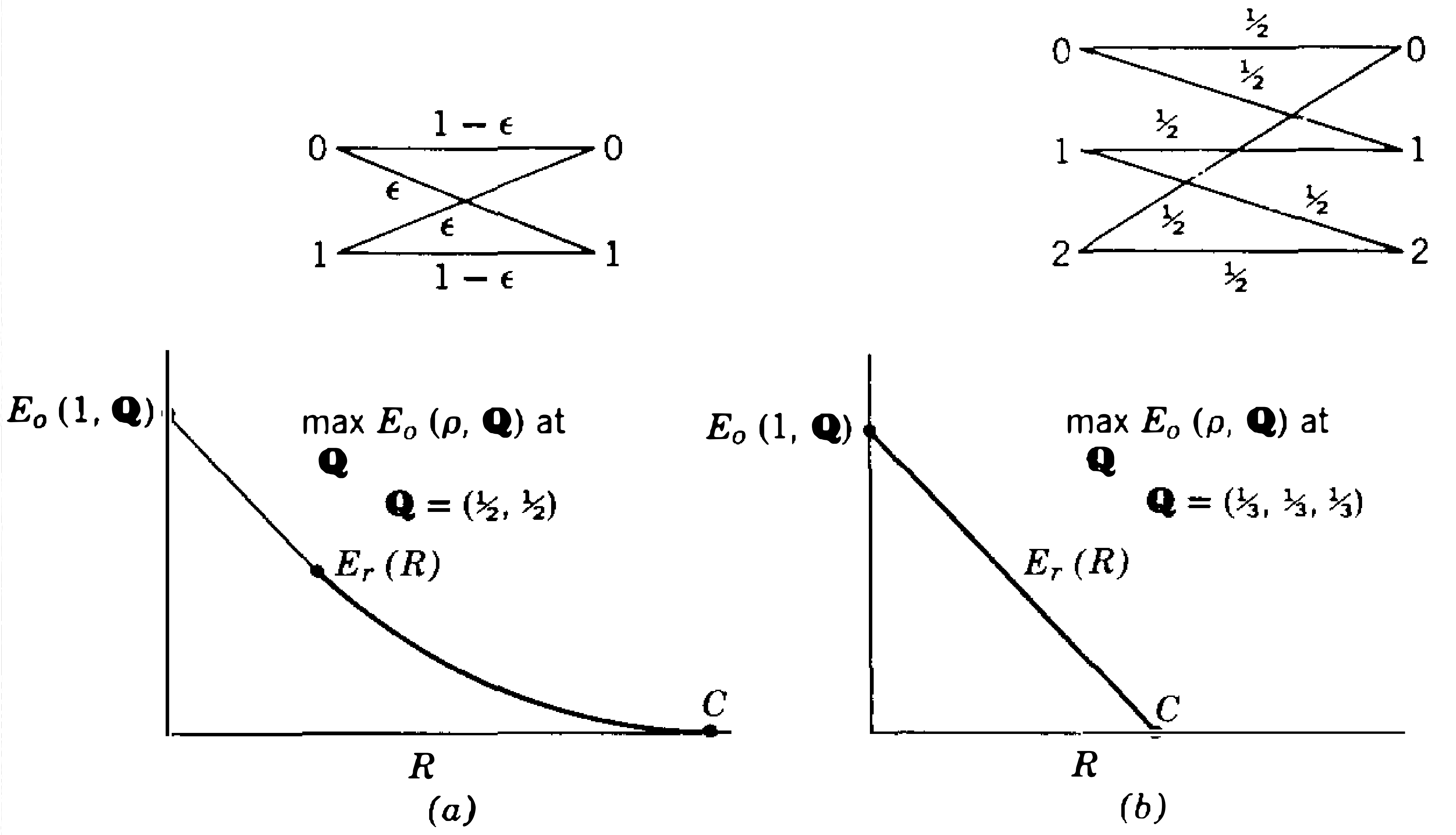


Figure 5.6.1. Random-coding exponent, $E_r(R)$, for two channels. (a) Typical behavior. (b) Special case where $\partial^2 E_o/\partial\rho^2 = 0$.

Error exponents

Information reconciliation and symmetric CQ channel coding

arXiv:2207.08899 [quant-ph]

Error probability for a good code C of rate R, blocklength n, and channel W:

$$P_{\text{err}} \approx 2^{-nE(W,R)} \quad \text{for} \quad n \to \infty$$

For classical channels and rates below capacity:

$$E(W,R) \geq \max_{s\in[0,1]} \left(E_0(s,W) - sR\right)$$

Fano, Gallager, …

$$E(W,R) \leq \sup_{s\geq 0} \left(E_0(s,W) - sR\right)$$

Shannon, Gallager, Berlekamp

$$E_0(s,W) = \max_{P_Z} s\, \bar{I}^{\uparrow}_{1/1+s}(Z:B)$$

Error probability for a good code C of rate R, blocklength n, and channel W:

$$P_{\text{err}} \approx 2^{-nE(W,R)} \quad \text{for} \quad n \to \infty$$

For classical-quantum channels and rates below capacity:

$$E(W,R) \geq \max_{s\in[0,1]} \left(E_0(s,W) - sR\right)$$

Pure state channels: Burnashev & Holevo

$$E(W,R) \leq \sup_{s\geq 0} \left(E_0(s,W) - sR\right)$$

Dalai, Winter

$$E_0(s,W) = \max_{P_Z} s\, \bar{I}^{\uparrow}_{1/1+s}(Z:B)$$

Error probability for a good code C of rate R, blocklength n, and channel W:

$$P_{\mathrm{err}} \approx 2^{-nE(W,R)} \quad \text{for} \quad n \to \infty$$

For classical-quantum channels and rates below capacity:

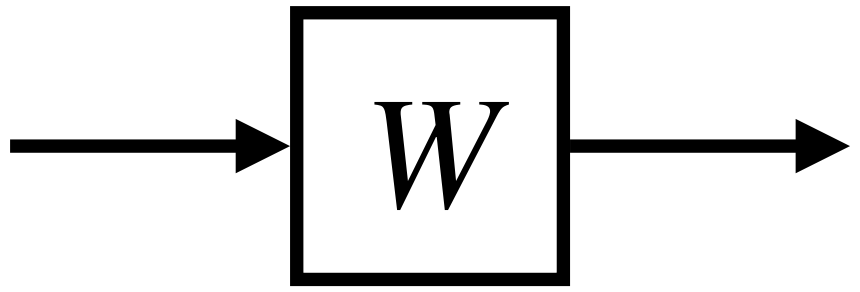
$$E(W,R) \geq \max_{s\in[0,1]} \left(E_0(s,W) - sR\right)$$

arXiv:2207.08899 [quant-ph]

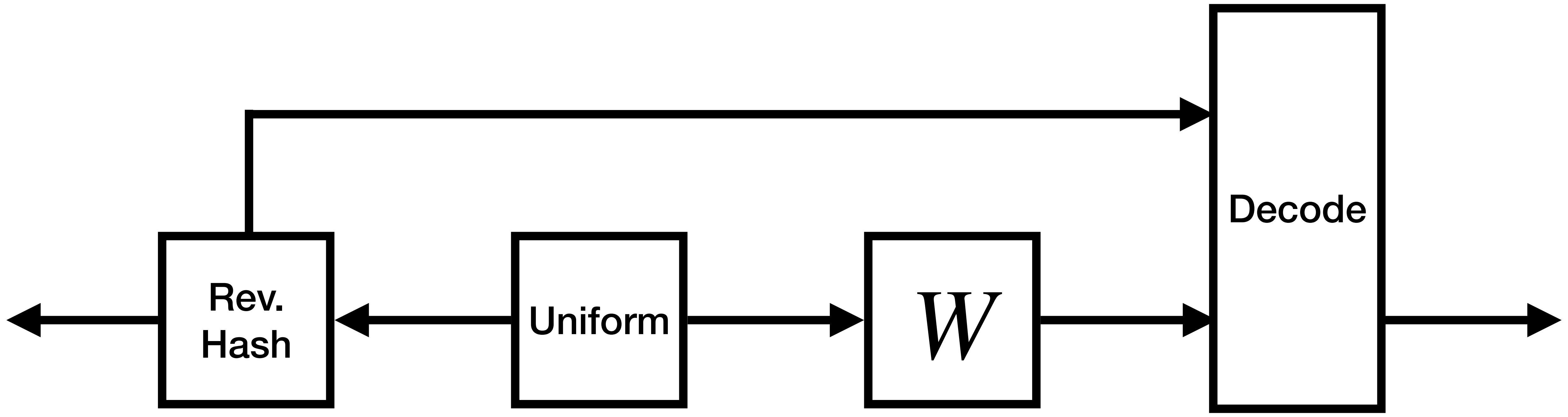
This talk: extend the achievability result to symmetric channels using duality

Specifically: convert a security exponent result from Hayashi 2015 to an information reconciliation error exponent, and from there to a channel coding result

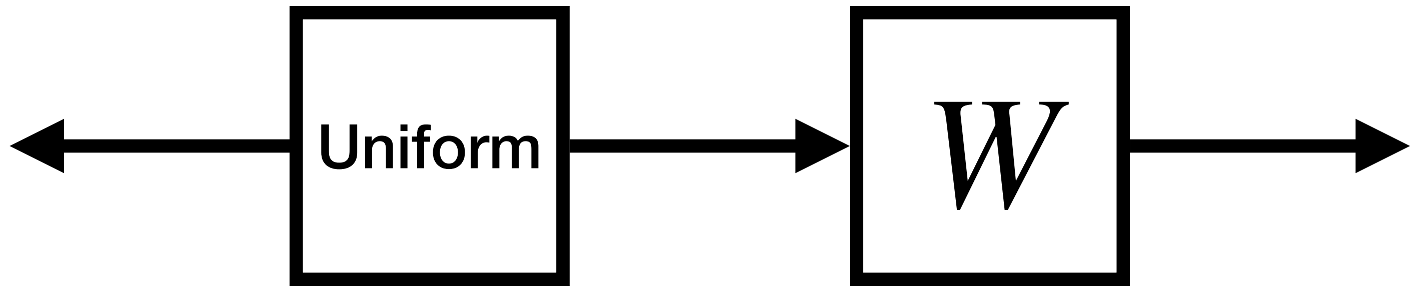
Reduction from reconciliation to channel coding



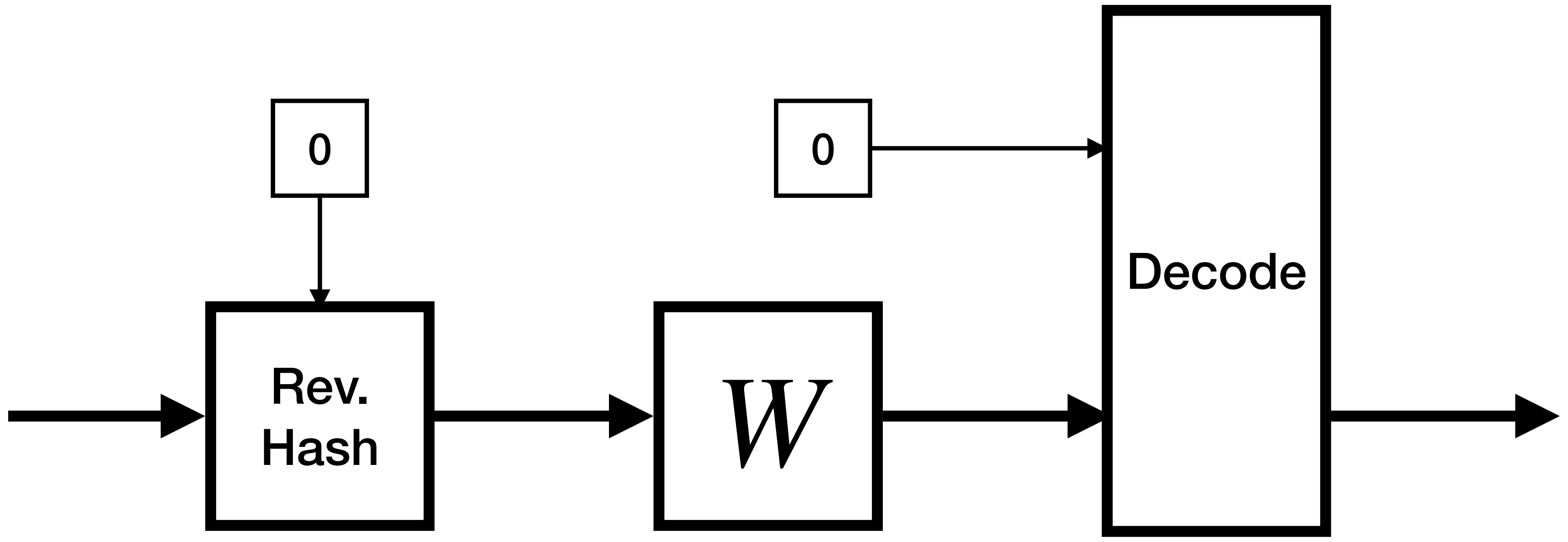
Channel (n-fold iid)



Information reconciliation

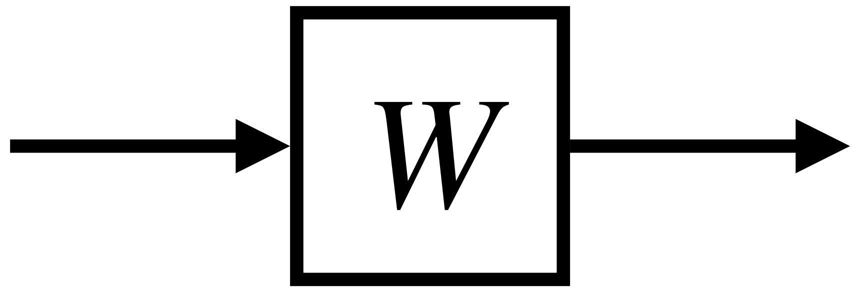


Bipartite source

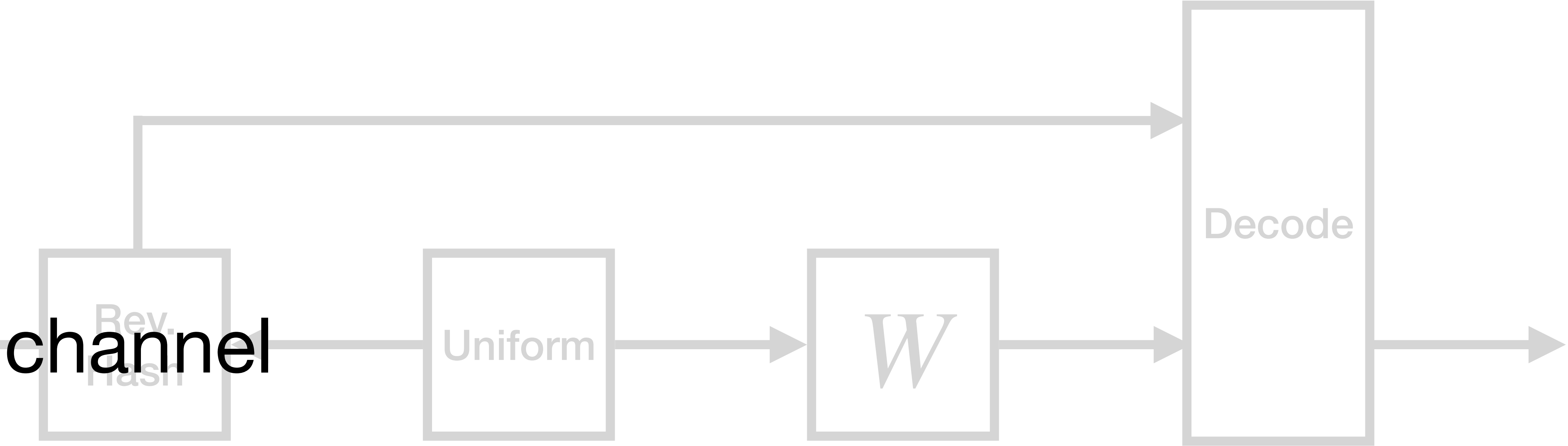


Channel coding

Reduction from reconciliation to channel coding



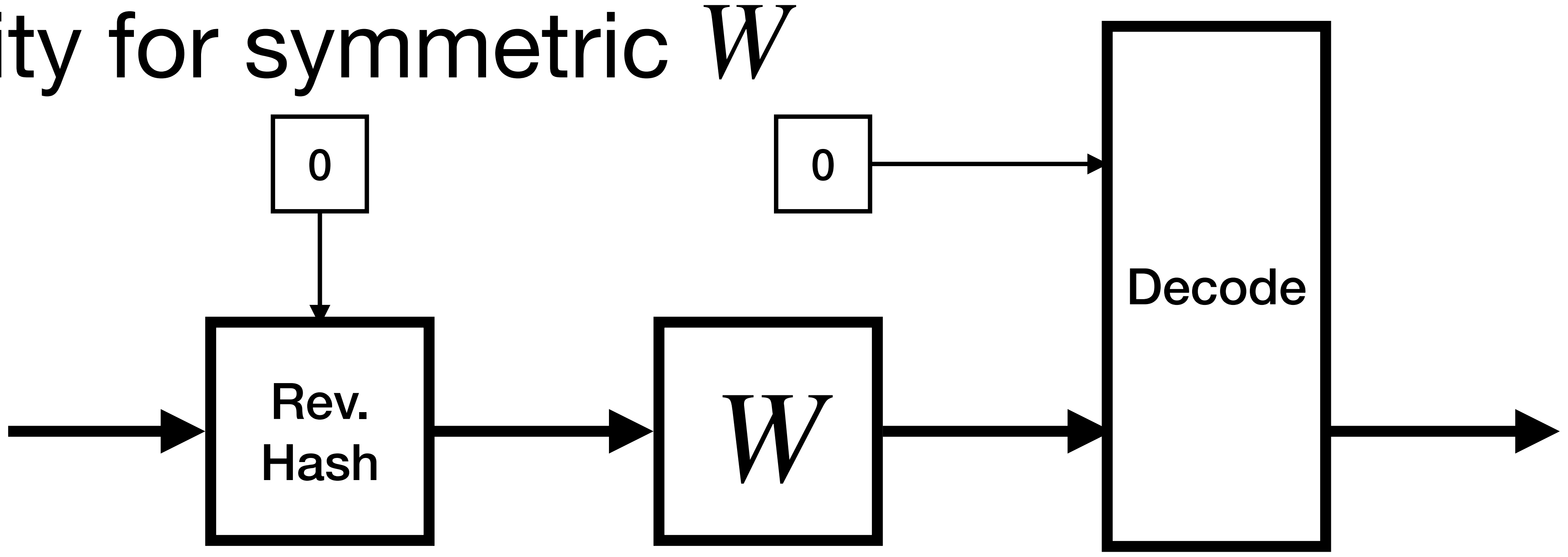
Channel



Information reconciliation

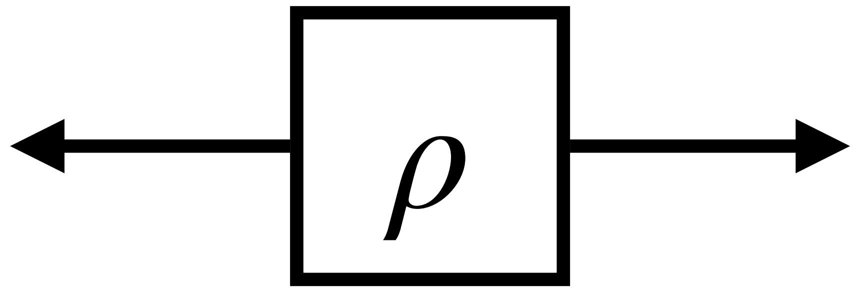
- Works for any channel
- Average error for coding $\leq$ IR error
- Rate is $\log d - R_{IR}$
- Achieves capacity for symmetric W

Bipartite source

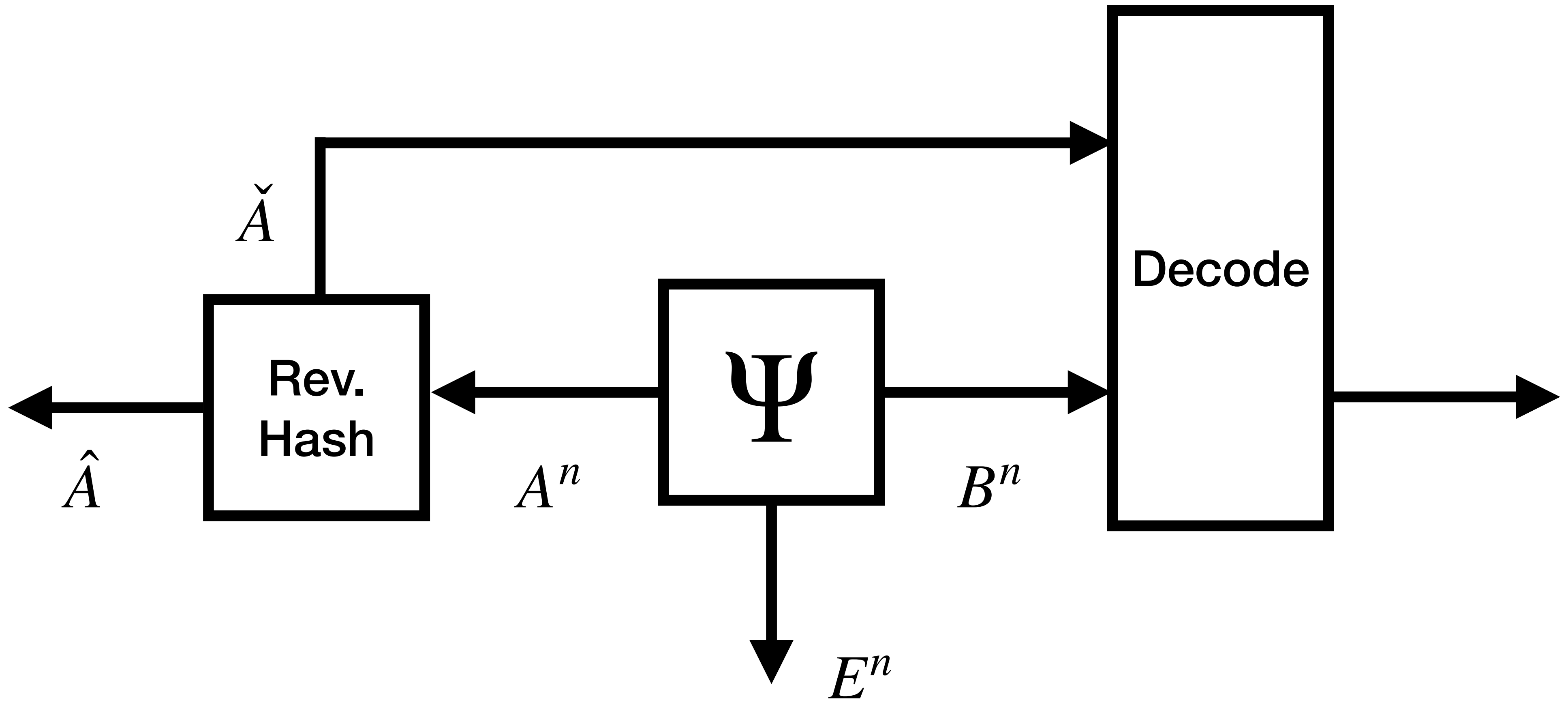


Channel coding

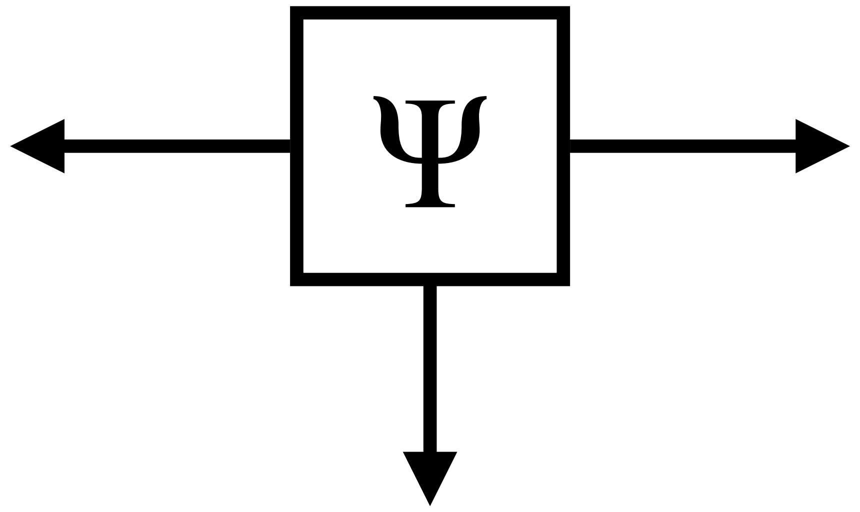
Connection between privacy amplification and reconciliation



Bipartite source



Purified tripartite source



Tripartite uncertainty relation R2018

$$P_{\text{guess}}(\hat{Z}|B^n\check{Z})_\Psi = \max_\sigma F(\Psi_{\hat{X}E^n}, \pi_{\hat{X}} \otimes \sigma_{E^n})^2$$

$\hat{Z}, \check{Z}$: measure $\hat{A}, \check{A}$ in standard basis
$\hat{X}$: measure $\hat{A}$ in Fourier conjugate basis

Security exponent of privacy amplification

Hayashi2015: Universal hashing for privacy amplification achieves:

$$\lim_{n\to\infty} \frac{-1}{n} \log D(\Psi_{\hat{X}E^n}, \pi_{\hat{X}} \otimes \Psi_{E^n}) \geq \max_{\alpha\in[1,2]} (\alpha - 1)\left(\tilde{H}^{\downarrow}_{\alpha}(X_A \,|\, E)_{\psi} - R_{PA}\right)$$

Security exponent of privacy amplification

Hayashi2015: Universal hashing for privacy amplification achieves:

$$\lim_{n\to\infty} \frac{-1}{n} \log D(\Psi_{\hat{X}E^n}, \pi_{\hat{X}} \otimes \Psi_{E^n}) \geq \max_{\alpha\in[1,2]} (\alpha - 1)\left(\tilde{H}^{\downarrow}_{\alpha}(X_A \mid E)_{\psi} - R_{PA}\right)$$

LHS: Bound D by F and use uncertainty relation to obtain

$$\lim_{n\to\infty} \frac{-1}{n} \log P_{\text{err}}(\hat{Z} \mid B^n \check{Z})_{\Psi} \geq \lim_{n\to\infty} \frac{-1}{n} \log D(\Psi_{\hat{X}E^n}, \pi_{\hat{X}} \otimes \Psi_{E^n})$$

Security exponent of privacy amplification

Hayashi2015: Universal hashing for privacy amplification achieves:

$$\lim_{n\to\infty} \frac{-1}{n} \log D(\Psi_{\hat{X}E^n}, \pi_{\hat{X}} \otimes \Psi_{E^n}) \geq \max_{\alpha\in[1,2]} (\alpha-1)\left(\tilde{H}^{\downarrow}_{\alpha}(X_A\,|\,E)_{\psi} - R_{PA}\right)$$

RHS: Another uncertainty relation & PA / IR rate relations:

$$\bar{H}^{\uparrow}_{1/\alpha}(Z_A\,|\,B)_{\psi} + \tilde{H}^{\downarrow}_{\alpha}(X_A\,|\,E)_{\psi} = \log d_A \qquad\qquad R_{PA} = \log d_A - R_{IR}$$

$$\begin{aligned}\max_{\alpha\in[1,2]} (\alpha-1)\left(\tilde{H}^{\downarrow}_{\alpha}(X_A\,|\,E)_{\psi} - R_{PA}\right) &= \max_{\alpha\in[1,2]} (\alpha-1)\left(R_{IR} - \bar{H}^{\uparrow}_{1/\alpha}(Z_A\,|\,B)_{\psi}\right)\\ &= \max_{\alpha\in[1/2,1]} \frac{1-\alpha}{\alpha}\left(R_{IR} - \bar{H}^{\uparrow}_{\alpha}(Z_A\,|\,B)_{\psi}\right)\end{aligned}$$

Error exponent of information reconciliation

We have the following achievability result:

$$\lim_{n\to\infty} \frac{-1}{n} \log P_{\mathsf{err}}(\hat{Z} | B^n \check{Z})_{\Psi} \geq \max_{\alpha \in [1/2,1]} \frac{1-\alpha}{\alpha} \left(R_{IR} - \bar{H}_{\alpha}^{\uparrow}(Z_A | B)_{\psi} \right)$$

Compare with the converse bound from Cheng, Hanson, Datta, Hsieh 2021

$$\lim_{n\to\infty} \frac{-1}{n} \log P_{\mathsf{err}}(\hat{Z} | B^n \check{Z})_{\Psi} \leq \sup_{\alpha \in [0,1]} \frac{1-\alpha}{\alpha} \left(R_{IR} - \bar{H}_{\alpha}^{\uparrow}(Z_A | B)_{\psi} \right)$$

Error exponent of channel coding

Uniform P_Z is optimal in $\max_{P_Z} \bar{I}^{\uparrow}_{\alpha}(Z_A : B)_{\psi}$ for symmetric channels, meaning

$$\max_{P_Z} \bar{I}^{\uparrow}_{\alpha}(Z_A : B)_{\psi} = \log d_A - \bar{H}^{\uparrow}_{\alpha}(Z_A \,|\, B)_{\psi}$$

By the IR→coding reduction, for which $R = \log d - R_{IR}$, we get

$$\lim_{n\to\infty} \frac{-1}{n} \log P_{\text{err}}(W) \geq \max_{\alpha\in[1/2,1]} \frac{1-\alpha}{\alpha} \left(\bar{I}^{\uparrow}_{\alpha}(Z_A : B)_{\psi} - R \right)$$

$$= \max_{s\in[0,1]} s\left(\bar{I}^{\uparrow}_{1/1+s}(Z_A : B)_{\psi} - R \right) ,$$

which is what we wanted to prove.

Apply IR bounds to PA: sphere-packing

Cheng, Hanson, Datta, Hsieh 2021 give polynomial prefactors
in their sphere-packing converse bound, which when applied to PA yields

$$-\frac{1}{n}\log P(\Psi'_{\hat{X}C^n}, \pi_{\hat{X}} \otimes \Psi'_{C^n}) \leq \frac{1}{2}E_{SP-PA}(R_{PA}) + \frac{1}{4}(1 + |E'_{SP-PA}(R_{PA})|)\frac{\log n}{n} + \frac{K}{n}\,.$$

$$E_{SP-PA}(R_{PA}) = \sup_{\alpha \geq 1}(\alpha - 1)(\tilde{H}^{\downarrow}_{\alpha}(X_A \,|\, C)_{\psi'} - R_{PA})$$

This sharpens a recent result by Li, Yao, and Hayashi 2022 (but only for linear extractors)

Apply IR bounds to PA: strong converse

Cheng, Hanson, Datta, Hsieh 2021 also find the strong converse exponent for IR

$$E_{SC-IR}(R_{IR}) = \sup_{\alpha \geq 1} \frac{1-\alpha}{\alpha}\left(R_{IR} - \tilde{H}^{\uparrow}_{\alpha}(Z_A \,|\, B)_{\psi}\right)$$

By the uncertainty relation, $\max_{\sigma} F(\Psi_{\hat{X}E^n}, \pi_{\hat{X}} \otimes \sigma_{E^n})^2$ will have the same exponent
(at least for linear extractors)

Now use yet another Renyi duality $\tilde{H}^{\uparrow}_{\alpha}(Z_A \,|\, B)_{\psi} + \tilde{H}^{\uparrow}_{\alpha/(2\alpha-1)}(X_A \,|\, E)_{\psi} = \log d_A$ to get

$$\lim_{n\to\infty} \frac{-1}{n} \log \max_{\sigma} F(\Psi_{\hat{X}E^n}, \pi_{\hat{X}} \otimes \sigma_{E^n})^2 = \sup_{\alpha \in [1/2,1]} \frac{1-\alpha}{\alpha}\left(R_{PA} - \tilde{H}^{\uparrow}_{\alpha}(X_A \,|\, E)_{\psi}\right)$$

This matches a recent result by Li and Yao 2022 (again, just for linear extractors)

Open questions

Can this duality be applied directly to channels?

Do we always have to use linear functions?