

Intro remarks: Joseph M. Renes : A Theory of Information (?)

00

1. Physicists are sorta lazy: witness the principle of least action!
2. but really what this means is that we want simple, coherent, powerful theories of physical phenomena. Such as
 - a. Maxwell's equations (second Wrangler; also at Trinity)
 - b. Newton's Laws (since we're in Cambridge)
 - c. if we have to mention it: general relativity

One-shot framework invites us to ~~think~~ consider a "theory of information" not just "information theory", by which I mean whatever results you can manage to find regarding information transmission & processing, but rather the logic behind the whole thing.

One-shot language allows us to see and to express this structure.

Because:

1. it allows us to build up more complicated protocols from simple primitives in a transparent way

2. ~~it makes sense of the entropy measures~~
~~motivates or explains~~

it allows us to see the relationships between protocols by looking at their entropic characterization

Outline

- Primitives
- Entropies
- Protocols
 - channel coding
 - channel simulation
 - quantum: $PA = IR$

Primitives

I'll argue that the two primitives are:

- Privacy Amplification
- Information Reconciliation (Data Compression / Slepian-Wolf)

For experts: these are "state" versions of resolvability ϵ , \rightarrow or prob. distribution channel coding

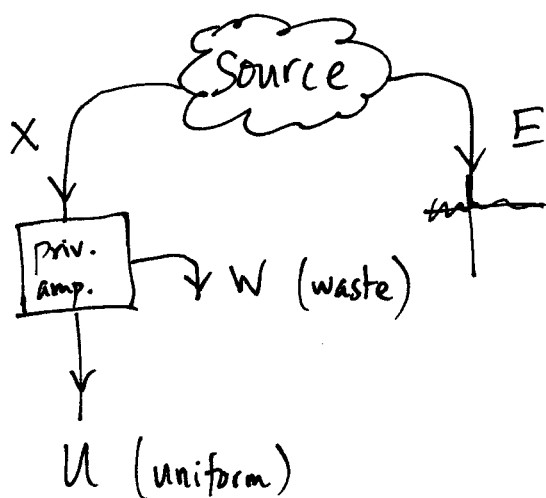
[They will prove more convenient to work with.] (covering) (packing)

~~PA~~ By "state" problem, I mean we're trying to transform a given (probability distribution) random variable / quantum state into a desired form: (It's always a bipartite RV)

PA: remove correlations

IR: ~~create~~ perfect correlations

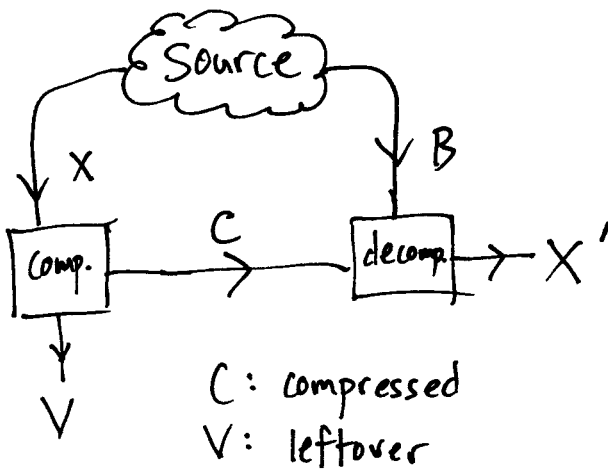
PA



U is uniform, uncorrelated with E

$$\frac{1}{2} \| \rho_{UE} - \pi_U \otimes \rho_E \|_1 \leq \epsilon$$

IR



C: compressed
V: leftover

X' is essentially identical to X

~~$X' = \text{Dec}(C, B)$~~

$X' = \text{Dec}(C, B)$

$\Pr[X \neq X'] \leq \epsilon$

$\frac{1}{2} \| p_{XX'} - p_{X \otimes X'} \| \leq \epsilon$

Entropies: $p_{XB} = \sum_x p_x [x] \otimes \psi_x$ $D_{\max}(p \| \sigma) = \min \{ \lambda \in \mathbb{R} : p \leq 2^{\lambda} \sigma \}$

1. $H_{\min}(X|B)_p := - \min_{\sigma_B} D_{\max}(p_{XB} \| \mathbb{1}_X \otimes \sigma_B)$ (∞ norm $\sigma_p^{-1/2} \sigma^{-1/2}$)

\Rightarrow guessing probability $p_{\text{guess}}(X|B)_p = 2^{-H_{\min}(X|B)_p}$

2. $H_{\max}(X|B)_p := \max_{\sigma} \log \| \sqrt{p_{XB}} \sqrt{\mathbb{1}_X \otimes \sigma_B} \|_1^2$ (1-norm)

\Rightarrow proximity to uniform, uncorrelated state

$H_{\max}(X|B)_p = \max_{\sigma} \log \| |X| F(p_{XB}, \mathbb{1}_X \otimes \sigma_B) \|^2$ (eqn after 4.8 in MT omits the 2)

3. Smoothing: minimize H_{\max} , maximize H_{\min} by looking in ϵ -neighborhood of actual state

in quantum case, best to use purified distance

Entropic Characterizations of Protocols

PA target output: $H_{\max}(U|E) \approx 0 \Rightarrow H_{\max}^\epsilon(U|E) = 0$
 "rate": $\log|U| \approx H_{\min}^\epsilon(X|E)$ \leftarrow should be $\log|U|$ \nearrow

IR target output $H_{\min}^\epsilon(X|X') = 0$
 "rate" $\log|C| \approx H_{\max}^\epsilon(X|B)$

Proofs: ϵ universal hashing $\frac{1}{2}$ leftover hash lemma PA
 pretty good measurement IR

A unifying entropy hypothesis-testing entropy

also used by
 Wang/Renner
 Tomamichel/Hayashi
 Buscemi/Datta
 Brandão/Datta

$$2^{-D_H^\epsilon(\rho \parallel \sigma)} = \min_{\substack{Q \geq 0 \\ \text{tr} Q \rho \geq \epsilon}} \frac{1}{\epsilon} \text{tr} Q \sigma = \max_{\substack{R \geq 0 \\ \mu \rho \leq \sigma + R}} \mu - \frac{1}{\epsilon} \text{tr} R$$

$$\begin{aligned} &\text{tr} Q \rho \geq \epsilon \\ &0 \leq Q \leq \mathbb{1} \end{aligned} \qquad \begin{aligned} &\mu \rho \leq \sigma + R \\ &R \geq 0 \end{aligned}$$

\leftarrow already looks a bit like D_{\max}

$$H_H^\epsilon(X|B)_\rho = \min_{\sigma} -D_H^\epsilon(\rho_{XB} \parallel \mathbb{1}_X \otimes \sigma_B)$$

~~vs~~

Point being: $H_H^\epsilon(X|B)_\rho \approx H_{\min}^\epsilon(X|B)_\rho$
 $H_H^{1-\epsilon}(X|B)_\rho \approx H_{\max}^\epsilon(X|B)_\rho$

Protocols

Renes / Renner

1012.4814

TIT 57, 7377 (2011)

Noisy channel coding $X \rightarrow [N] \rightarrow B$

~~example~~: $M \rightarrow [Enc] \rightarrow [N] \rightarrow [Dec] \rightarrow M'$ M uniform

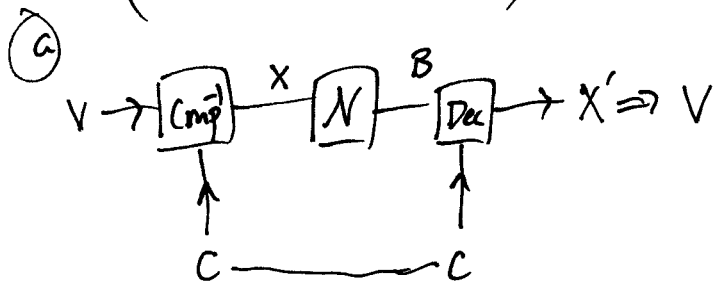
can show $\Pr[M \neq M'] \leq \epsilon$

$$\log |M| \approx \underset{\substack{\uparrow \\ \max \\ X}}{H_{\min}^{\epsilon}(X)} - H_{\max}^{\epsilon}(X|B)$$

expurgate to get worst-case, i.e. identity channel simul.

Yet another coding thm proof!

① (examine case $X=U$) use IR to simulate state



③ imagine. Cmp is linear, then if X is uniform, so are C, V

$$\Rightarrow |V| \cdot |C| = |X| \Rightarrow |V| = \frac{|X|}{|C|} \Rightarrow \log |V| = \log |X| - \log |C|$$

$$\Rightarrow \log |V| \approx \log |X| - H_{\max}^{\epsilon}(X|B)$$

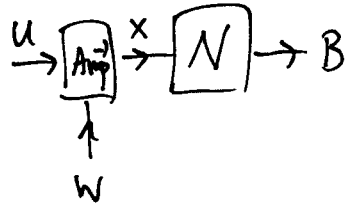
④ derandomize C by taking best value

⑤ that only gives "symmetric capacity".

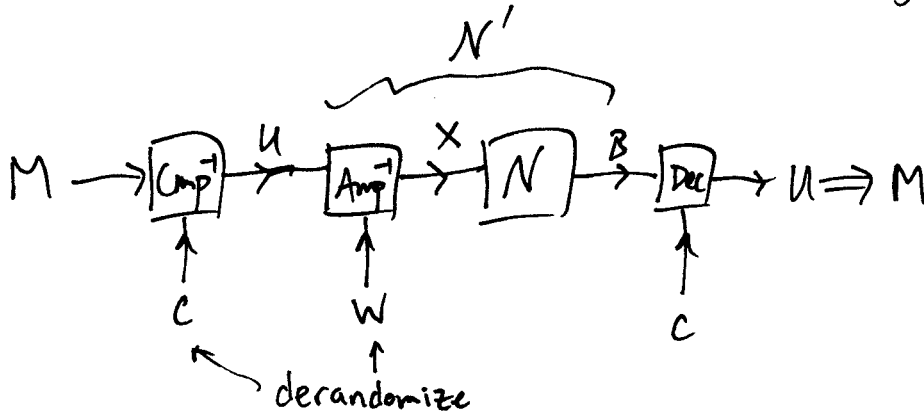
for the actual capacity, prefix the channel with PA

⑥

Protocols 2



Again, assume Amp is linear. We don't need to worry about correlations.



rate: $\log |M| \approx \log |U| - H_{\max}^{\epsilon}(U|B)_{N'}$

$\approx H_{\min}^{\epsilon}(X) - H_{\max}^{\epsilon}(U|B)$

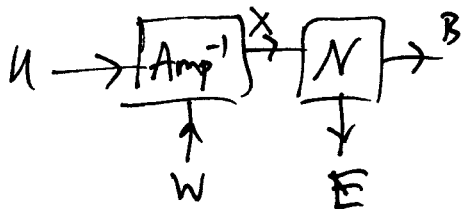
$\approx H_{\min}^{\epsilon}(X) - H_{\max}^{\epsilon}(X|B)$

U is a function of X via Amp (5.11)

can show converse (cf. Ligong/Renner)

Private Coding

Great thing is we can immediately do private coding



$p_{UE} \approx \pi_U \otimes p_E$

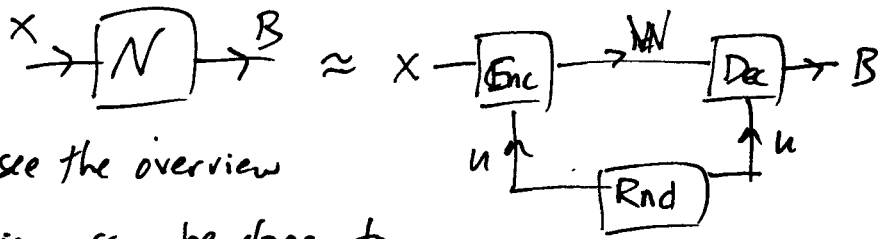
\Rightarrow rate ~~is~~

$\log |M| \approx H_{\min}^{\epsilon}(X|E) - H_{\max}^{\epsilon}(X|B)$

Csiszar Körner

Protocols 3

Arb. Channel Simulation
for fixed state



- specialize to classical to see the overview
- measurement compression can be done, too
- to get universal simulation, use post-selection
for iid

from PA of $Y|X$: $P_{YX} \rightarrow P_{UWX} \rightarrow P_{W|UX}$

$$(U, W) = \text{Amp}(Y)$$

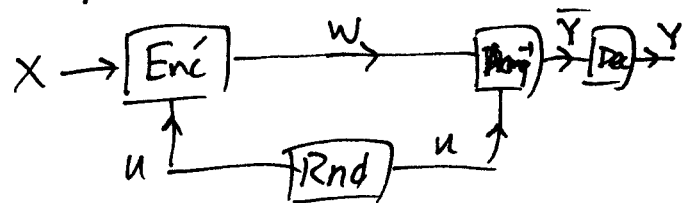
Enc: generate W from UX using $P_{W|UX}$

Dec: recreate Y from (U, W) $\text{Dec} = \text{Amp}^{-1}$

rate? $C = \log|W| = \log|Y| - \log|U| = \log|Y| - H_{\min}^{\epsilon}(Y|X)$
 $S = \log|U| = H_{\min}^{\epsilon}(Y|X)$

improve by compressing Y first, to \bar{Y}

$$\Rightarrow \log|\bar{Y}| = H_{\max}^{\epsilon}(Y)$$



rate of channel sim:

$$C = \log|\bar{Y}| - H_{\min}^{\epsilon}(\bar{Y}|X)$$

$$S = H_{\min}^{\epsilon}(\bar{Y})$$

$$\Rightarrow C \approx H_{\max}^{\epsilon}(Y) - H_{\min}^{\epsilon}(Y|X)$$

$$S \approx H_{\min}^{\epsilon}(Y)$$

$$H_{\min}^{\epsilon}(\bar{Y}|X) \leq H_{\min}^{\epsilon}(Y|X) \quad \bar{Y} \text{ function of } Y$$

but $P_{\text{guess}}(\bar{Y}|X) \approx P_{\text{guess}}(Y|X)$

just guess \bar{Y} and decompress

$$\Rightarrow H_{\min}^{\epsilon}(\bar{Y}|X) \approx H_{\min}^{\epsilon}(Y|X)$$

Protocols 4

in the quantum world $PA \Leftrightarrow IR!$

it's all about the uncertainty principle

use von Neumann $H(X_A|B) + H(Z_A|E) \geq \log |X|$

start with a pure state (actually any state) $|\psi\rangle_{ABE}$

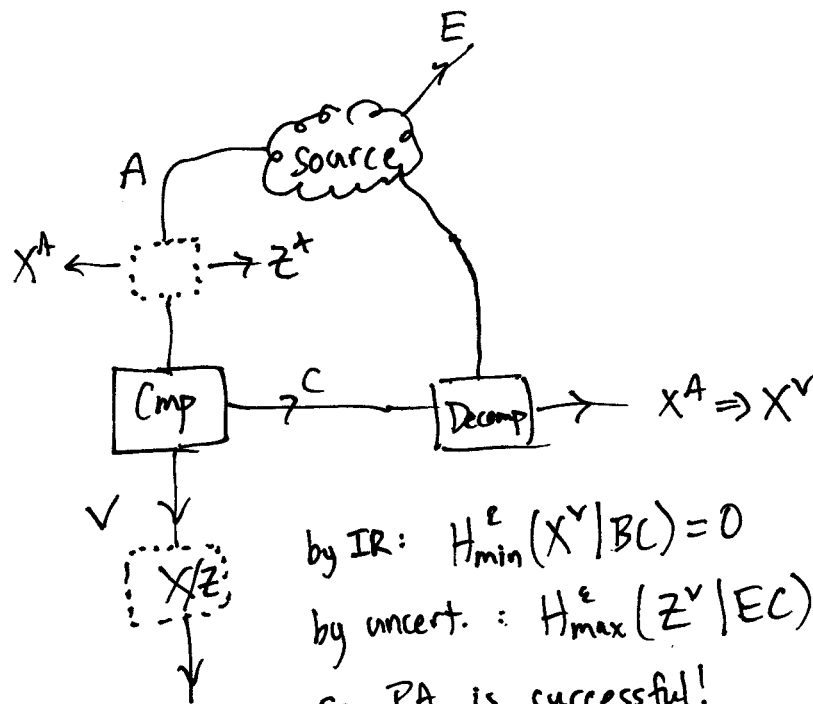
X arises from measurement in a given basis

Z arises from using the conjugate basis.

$$|z\rangle = \frac{1}{\sqrt{d}} \sum_x e^{2\pi i/d xz} |x\rangle$$

IR \Rightarrow PA

using a linear compressor, a map on X can also be viewed as a map on Z



rate: $\log |V| = \log d - \log |C| = \log d - H_{\max}^E(X^A|B)$
 (but $\leq H_{\min}^E(Z^A|E)$)

PA \Rightarrow IR

seems like it won't work, we need a certainty principle

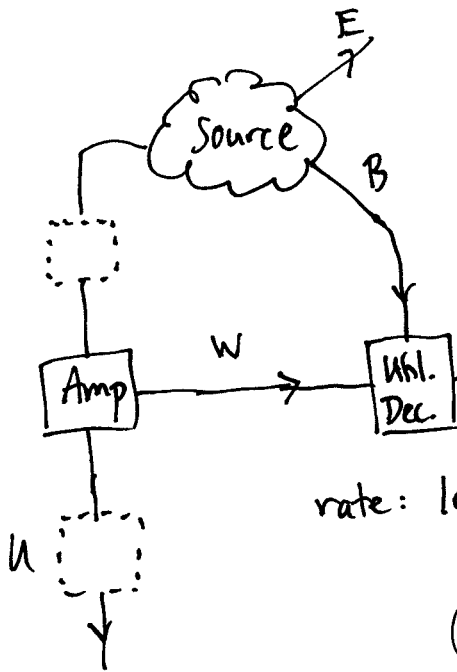
\Rightarrow we have that for certain states!

recall: $H(X^A|B) + H(Z^A|E) \geq \log d$

\hookrightarrow but if state pure and $H(X^A|E) = 0$ or $H(Z^A|B) = 0$
then equality

we could have assumed $H(Z^A|B) = 0$ in (IR $\stackrel{\text{PA}}{\Rightarrow}$ ~~$X^A|B$~~)

now assume $H(X^A|E) = 0$ for PA \Rightarrow IR



by PA $H_{\max}^e(Z^A|E) = \log d$

by max $\Rightarrow H_{\min}^e(X^A|WB) = 0$

can also say $H_{\max}^e(Z^A|EX^W) = \log d$

and therefore $H_{\min}^e(X^A|X^WB) = 0$

and hence $H_{\min}^e(X^A|B) = 0$

rate: $\log |W| = \log d - \log |U|$

$= \log d - H_{\min}^e(X^A|E)$

(but $\leq H_{\max}^e(X^A|B)$)

(10b)

(10a)