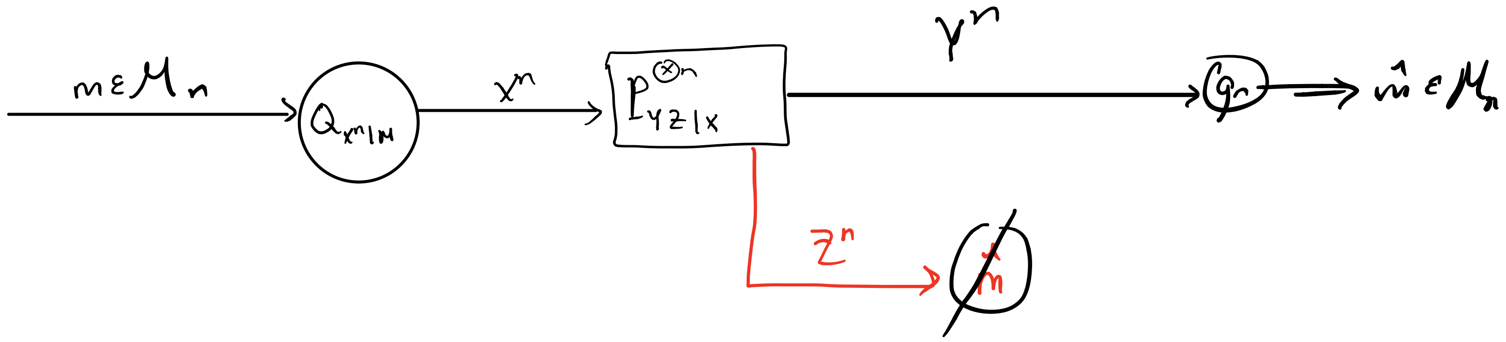
Recap

Wiretap Channel



WT code $\quad C_n = (Q_{X^n|M}, g_n)$

Reliability w.r.t $e_{avg}(C_n)$ or $e_{max}(C_n)$

Security w.r.t. $l_{avg}(C_n)$ or $l_{max}(C_n)$

Secrecy Capacity as sup over all R achievable rates

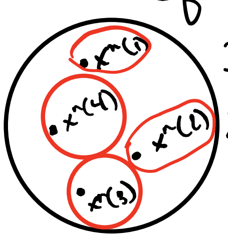
Theorem:

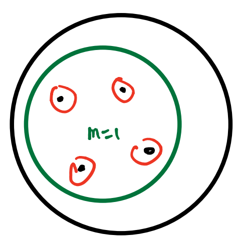
$$C_{WTC}(\underbrace{P_{YZ|X}}_{\text{degraded}}) = \max_{P_X} I(X;Y) - I(X;Z)$$

for any degraded WTC $P_{YZ|X}$ $\quad (\forall P_X,\ P_X P_{YZ|X} \quad X \leftrightarrow Y \leftrightarrow Z)$

Proof Outline

[I] **Achievability**: If $R < \max_{P_X} \overbrace{I(X;Y) - I(X;Z)}^{I(X;Y|Z) \text{ via } X \leftrightarrow Y \leftrightarrow Z}$ then it is achievable, i.e we can find asymptoticall reliable + secure sequence of wiretap codes of rate R.





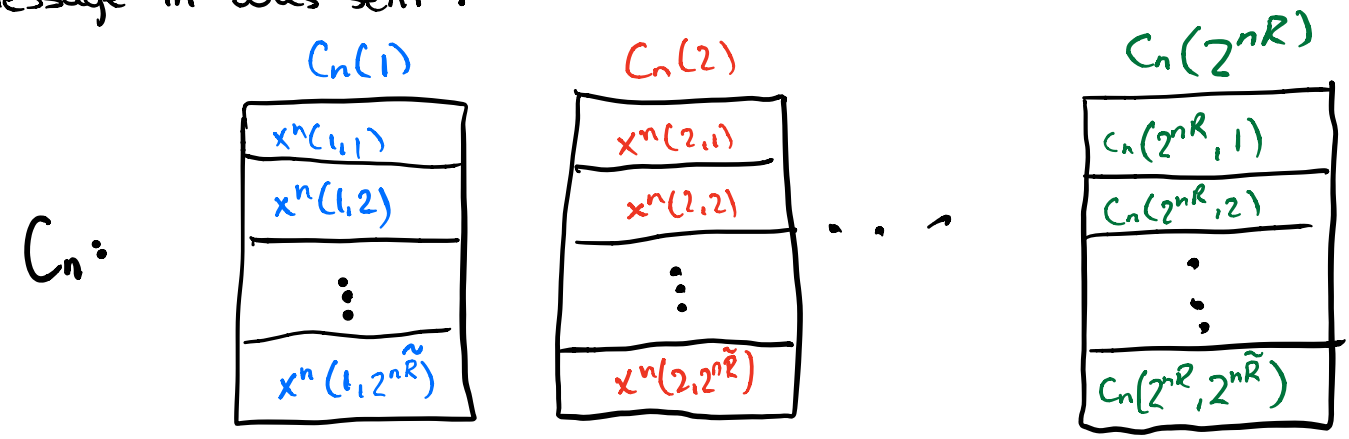
Random Code Design

$\mathcal{M}_n = \{1, \ldots, 2^{nR}\}$ and define $\mathcal{W}_n = \{1, \ldots, 2^{n\tilde{R}}\}$, $\tilde{R} > 0$

↑ message set ↑ auxiliary index set

- The wiretap code comprises $2^{n(R+\tilde{R})}$ codewords iid according to $P^{\otimes n}$ of length n, i.e., $C_n = \{X(m,w)\}_{(m,w) \in \mathcal{M}_n \times \mathcal{W}_n}$.

Thus, for each $m \in \mathcal{M}_n$ there is a sub-codebook $C_n(m) = \{X(m,w)\}_{w \in \mathcal{W}_n}$ associated with it. Any codeword in $C_n(m)$ conveys the same information: "message m was sent".



Encoding & Decoding

Fix a WT code $\mathcal{C}_n = \{x^n(m,w)\}_{(m,w) \in \mathcal{M}_n \times \mathcal{W}_n}$ by drawing C_n.

① Encoding: To send $m \in \mathcal{M}_n$, draw $W \sim \text{Unif}(\mathcal{W}_n)$ and let $w \in \mathcal{W}_n$ be the realization of W. The sequence $x^n(m,w)$ is transmitted over the wiretap channel

$$Q_{X^n|M}(x^n|m) = 2^{-n\tilde{R}} \sum_{w \in \mathcal{W}_n} \mathbb{1}_{\{x^n = x^n(m,w)\}} \quad \forall\, m \in \mathcal{M}_n,\ x^n \in \mathcal{X}^n$$

② Decoding: Upon observing $Y^n \sim P_{Y|X}^{\otimes n}(y^n | x^n(m,w))$, we will use joint typicality decoding to estimate both m and w!

$\Rightarrow$ The decoder searches for a unique pair $(\hat{m}, \hat{w}) \in \mathcal{M}_n \times \mathcal{W}_n$ such that

$$(x^n(\hat{m}, \hat{w}), Y^n) \in \mathcal{T}_\eta^{(n)}(P_{XY})$$

$P_{XY} = P_X P_{Y|X}$

$P_Y = \sum_z P_{YZ|X}(\cdot, z|\cdot)$

Reliability Analysis

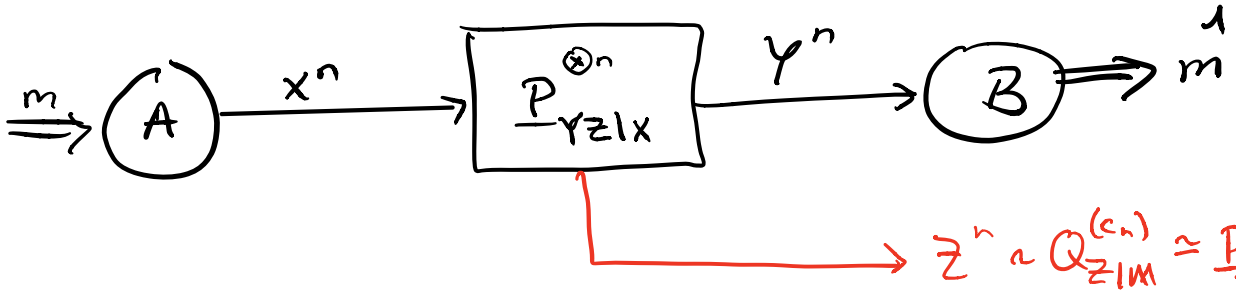
Observe that our goal is to decode (M,W) from Y^n where each pair $(m,w) \in \mathcal{M}_n \times \mathcal{W}_n$ is associated with a unique codeword $X^n(m,w)$. Then the reliability analysis reduces to classic P2P reliability analysis but for a codebook of rate $R + \tilde{R}$ (instead of R in the classic case).

$\Rightarrow$ We have $\mathbb{E}_{C_n}[e_{av}(C_n)] \xrightarrow{n\to\infty} 0$ exponentially fast provided $R + \tilde{R} < I(X;Y)$

Security Analysis

We will use the approximate distribution simulation result.

How is it related?



When we are sending $m \in \mathcal{M}_n$, the output at Eve's end is distributed according to $Z^n \sim Q_{Z^n|M}^{(c_n)}(\cdot|m)$

We will see how to make $Q_{Z|M}^{(c_n)}(\cdot|m) \approx P_Z^{\otimes n}$ for any $m \in \mathcal{M}_n$

In particular, doing so make Z^n asymptotically independent of M.

$$\ell_{avg}(c_n) = I_{Q^{(c_n)}}(M; Z^n) \overset{\text{KL divergence chain rule}}{=} D_{KL}\left(Q_{Z^n|M}^{(c_n)} \,\|\, Q_{Z^n}^{(c_n)} \,|\, \text{Unif}(\mathcal{M}_n)\right)$$

$$\overset{\forall\, P_Z \in \mathcal{P}(\mathcal{Z})}{=} D_{KL}\left(Q_{Z^n|M}^{(c_n)} \,\|\, P_Z^{\otimes n} \,|\, \text{Unif}(\mathcal{M}_n)\right) - \underbrace{D_{KL}\left(Q_{Z^n}^{(c_n)} \,\|\, P_Z^{\otimes n}\right)}_{\geq 0}$$

$$\leq D_{KL}\left(Q_{Z|M}^{(c_n)} \,\|\, P_Z^{\otimes n} \,|\, \text{Unif}(\mathcal{M}_n)\right)$$

$$\Rightarrow \mathbb{E}_{C_n}[\ell_{avg}(C_n)] \le \mathbb{E}_{C_n}\left[D_{KL}\left(Q_{Z|M}^{(C_n)} \,\|\, P_Z^{\otimes n} \,|\, Unif(\mathcal{M})\right)\right]$$

$$= \frac{1}{|\mathcal{M}_n|}\sum_{m\in\mathcal{M}_n} \mathbb{E}_{C_n}\left[D_{KL}\left(Q_{Z|M}^{(C_n)}(\cdot|m) \,\|\, P_Z^{\otimes n}\right)\right]$$

(the $\frac{1}{|\mathcal{M}_n|}\sum_{m}$ term $\to 1$)

symmetry: "same across different indices"

$$\equiv \mathbb{E}_{C_n(1)}\left[D_{KL}\left(Q_{Z^n|M}(\cdot|1) \,\|\, P_Z^{\otimes n}\right)\right]$$

$$Q_{Z^n|M}(\cdot|1) = \frac{1}{|\mathcal{W}_n|}\sum_{\omega\in\mathcal{W}_n} P_{Z|X}^{\otimes n}(z^n|x^n(1,\omega))$$

exponentially fast provided that $\tilde{R} > I(X;Z)$

Combined Rate conditions: We've seen that for our scheme to work it suffices that $R + \tilde{R} < I(X;Y)$ (Reliability), $\tilde{R} > I(X;Z)$ (security via distribution approximation).

Note that $\tilde{R}$ is not part of the problem definition and we only need to show that if $R < I(X;Y) - I(X;Z)$ then a pair $(R, \tilde{R})$ as above can be found.

Clearly this is the case: If $R < I(X;Y) - I(X;Z)$, then $\exists \delta > 0$ s.t. $R = I(X;Y) - I(X;Z) - \delta$

Take

$$\tilde{R} = I(X;Z) + \delta > I(X;Z).$$

We also get

$$R + \tilde{R} = I(X;Y) - 2\delta < I(X;Y)$$

$\Rightarrow$ $R < I(X;Y) - I(X;Z)$ is a sufficient condition for our performance guarantees to hold, as is the goal in the achievability proof.

Remark: From here we need to use Markov's inequality to prove that a deterministic (non-random) sequence of asymptotically reliable & secure WT codes exists (codes w/ rate R). Afterwards, we can further prune the extracted codebooks to attain small **maximal** error probability and information leakage.

II Converse: Assume R is achievable, i.e., let $\{C_n\}_{n\in\mathbb{N}}$ be a reliable & secure sequence of WT codes of rate R, and prove $R \leq \max_{P_X} I(X;Y) - I(X;Z)$

It is sufficient to assume $\{C_n\}_{n\in\mathbb{N}}$ has average performance guarantees.

$$e_{avg}(C_n) = P_{Q^{(C_n)}}(\tilde{M} \neq M) \xrightarrow[n\to\infty]{} 0 \quad \left(\xrightarrow{n\to\infty} \varepsilon_n,\ H(M|Y^n) \le n\cdot\varepsilon_n\right)$$

$$l_{avg}(C_n) = I_{Q^{(C_n)}}(M; Z^n) \xrightarrow[n\to\infty]{} 0 \quad \left(\xrightarrow{n\to\infty} \varepsilon_n,\ I(M;Z^n) \le \varepsilon_n\right)$$

$M \sim \text{Unif}(\mathcal{M}_n)$

We have

$$nR = H(M) = H(M) - H(M|Y^n) + \underbrace{H(M|Y^n)}_{\le n\cdot\varepsilon_n} - I(M;Z^n) + \underbrace{I(M;Z^n)}_{\le \varepsilon_n}$$

$$= \underbrace{I(M;Y^n) - I(M;Z^n)}_{\text{channel is degraded}} - \underbrace{n\varepsilon_n + \varepsilon_n}_{:= n\delta_n \text{ where } \delta_n \xrightarrow{n\to\infty} 0}$$

$M \leftrightarrow Y^n \leftrightarrow Z^n$

$$= I(M;Y^n|Z^n) + n\delta_n$$

$$\le I(M, X^n; Y^n|Z^n) + n\delta_n$$

$$= \sum_{i=1}^{n} \underbrace{H(Y_i|Z^n Y^{i-1})}_{\le H(Y_i|Z_i)} - \underbrace{H(Y_i|M, X^n, Z^n, Y^{i-1})}_{Y_i - X_i - (M, Y^{i-1}, Z^n)} + n\delta_n$$

by $(Z^{n\setminus i}, Y^{i-1})$ being removed

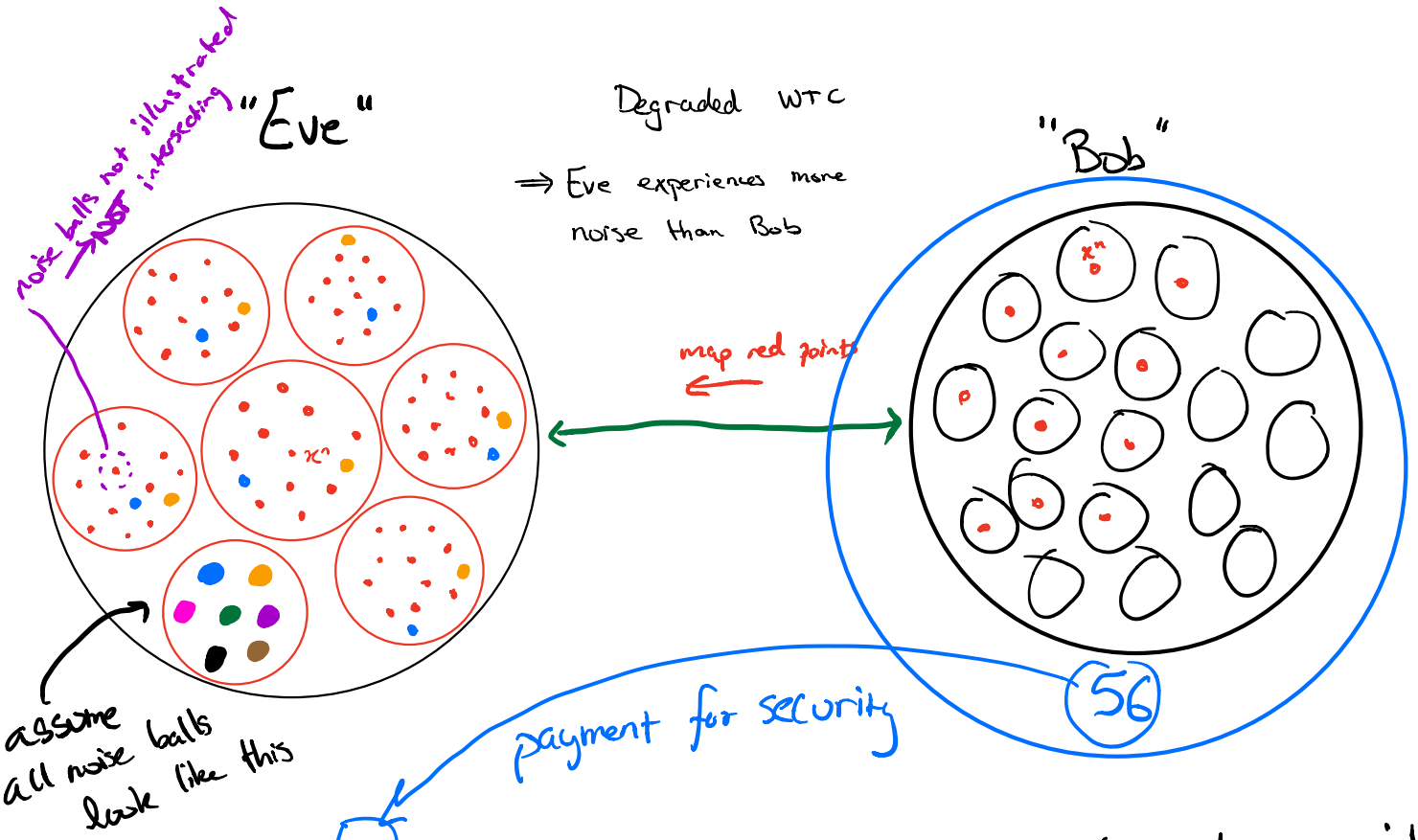
$$\Downarrow$$

$$Y_i \leftrightarrow (X_i, Z_i) \leftrightarrow (M, Y^{i-1}, Z^{n\setminus i})$$

$$= \sum_{i=1}^{n} \underbrace{I(X_i; Y_i|Z_i)}_{I(X_i;Y_i) - I(X_i;Z_i) = I(P_X; P_{Y|X}) - I(P_{X_i}; P_{Z|X})} + n\delta_n$$

$$\le \max_{P_X} I(P_X; P_{Y|X}) - I(P_X; P_{Z|X})$$

Discussion Section



Say we have 7 secret messages we want to transmit

↙ planting a codeword in space

$m=1$ •

$m=2$ • etc

Fix $c_n \in \mathcal{C}_n$

$$\ell_{max}(c_n) = \max_{P_M \in \mathcal{P}(\mathcal{M}_n)} I_{Q^{(c_n)}}(M; Z^n)$$

Fix $P_M \in \mathcal{P}(\mathcal{M}_n)$: $I(M; Z^n) \le D_{KL}\left(Q_{Z|M}^{(c_n)} \,\|\, P_Z^{\otimes n} \mid P_M\right)$

$$I(M;Z^n) \le D_{KL}\left(Q^{(c_n)}_{Z^n|M} \,\|\, P_Z^{\otimes n} \,|\, P_M\right)$$

$$= \sum_{m \in \mathcal{M}_n} P_M(m)\, D_{KL}\left(Q_{Z^n|M}(\cdot|m) \,\|\, P_Z^{\otimes n}(\cdot)\right)$$

$$\le \max_{m \in \mathcal{M}_n} D_{KL}\left(Q^{(c_n)}_{Z^n|M}(\cdot|m) \,\|\, P_Z^{\otimes n}(\cdot)\right)$$

Direct analysis for maximum information leakage

$$\mathbb{P}_{C_n}\left(\ell_{max}(c_n) > e^{-\gamma_n}\right) \le \mathbb{P}_{C_n}\left(\max_{m \in \mathcal{M}_n} D_n(m) > e^{-\gamma_m}\right)$$

$$= \mathbb{P}_{C_n}\left(\exists m \in \mathcal{M}_n \;\; D_n(m) > e^{-\gamma_m}\right)$$

$$= \mathbb{P}_{C_n}\left(\bigcup_{m \in \mathcal{M}_n} \{D_n(m) > e^{-\gamma_m}\}\right)$$

Union bound $\rightarrow$

$$\le \sum_{m \in \mathcal{M}_n} \mathbb{P}_{C_n}\left(D_n(m) > e^{-\gamma_m}\right)$$

$$= \sum_{m \in \mathcal{M}_n} \mathbb{P}_{C_n}\left(D_{KL}\left(Q^{(C_n(1))}_{Z^n|M}(\cdot|1) \,\|\, P_Z^{\otimes n}\right) > e^{-\gamma_n}\right)$$

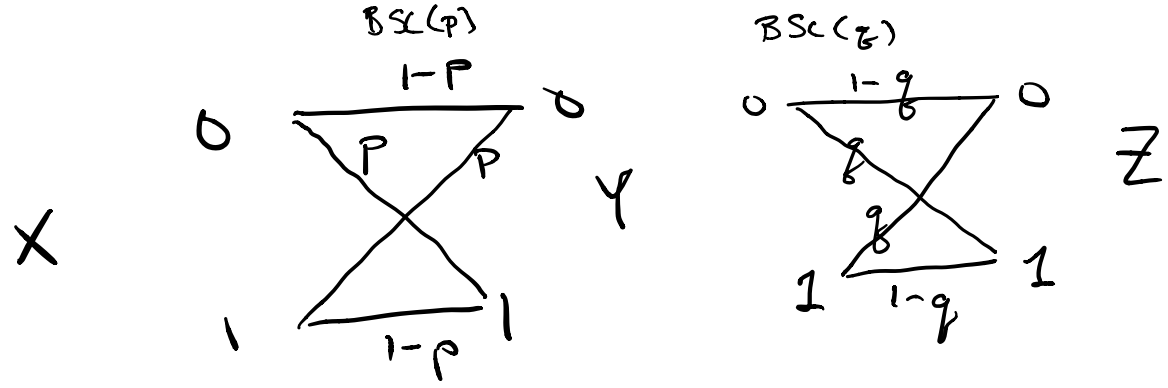
($\sum_{m \in \mathcal{M}_n}$: 2^{nR} terms)

$$\le e^{-e^{\gamma_{Z^n}}}$$

$$\le 2^{nR}\, e^{-e^{\gamma_n}} \xrightarrow[n \to \infty]{} 0$$

(strong-soft covering lemma)

Example: Consider the BSWT(p,q)



$Y = X \oplus N_1 \qquad N_1 \sim \text{Ber}(p)$

$Z = Y \oplus N_2 \qquad N_2 \sim \text{Ber}(q)$

$0 \le p, q \le \frac{1}{2}$

(things just flip otherwise)

What is the effective channel to Eve?

$$Z = X \oplus \tilde{N} \qquad \tilde{N} \sim \text{Ber}(\tilde{q})$$

$$P_{\tilde{N}}(1) = \mathbb{P}(\tilde{N}=1) = \mathbb{P}(N_1 \oplus N_2 = 1) = \mathbb{P}(N_1 \neq N_2) = (1-p)q + p(1-q)$$

$$= p * q$$

For $p, q \le \frac{1}{2}$, $\tilde{q} = p * q \ge \max\{p, q\}$ Prove this

We will show

$$C_{WT}^{(BSC)}(p,q) = H_b(\tilde{q}) - H_b(p) = \underbrace{1 - H_b(p)}_{C^{BSC}(p)} - \underbrace{(1 - H_b(\tilde{q}))}_{C^{BSC}(\tilde{q})}$$

$$C_{WT}^{BSC}(p,q) = \max_{x \sim Ber(r)} I(X;Y) - I(X;Z)$$

Achievability

Choose $X \sim Ber(1/2)$

$$C_{WTC}^{(BSC)}(p,q) \geq H_b(\tilde{q}) - H_b(p)$$

Converse

For $r \leq \frac{1}{2}$, let $X \sim Ber(r)$

$$I(X;Y) - I(X;Z) = H_b(r*p) - H_b(p) - \left(H_b(r*\tilde{q}) - H_b(\tilde{q})\right)$$

$$= H_b(\tilde{q}) - H_b(p) - \left(H_b(r*\tilde{q}) - H_b(r*p)\right)$$

need ≥ 0

$$\leq H_b(\tilde{q}) - H_b(p)$$

Observe that for $r \leq \frac{1}{2}$, the function that maps $u \mapsto r*u$ is monotonically increasing in $u \in [0, 1/2]$

$$\Rightarrow H_b(r*\tilde{q}) \geq H_b(r*q)$$

$$\Rightarrow H_b(r*\tilde{q}) - H_b(r*q) \geq 0 \Rightarrow \text{Proof}$$

$$f_r(u) = r * u = r(1-u) + (1-r)u$$

$$= r + (1-2r)u \quad , \quad r < 1/2$$