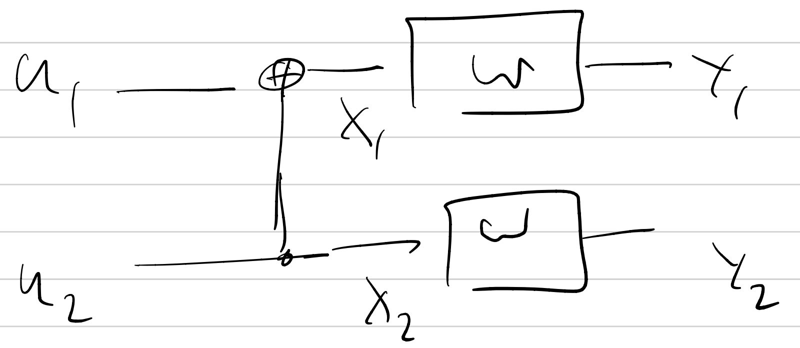
Information Theory & Coding

Dec 1st, 2020

Yesterday: we discussed polar coding.



$W^-: u_1 \to Y_1 Y_2$

$W^+: u_2 \to Y_1 Y_2 U_1$

$$W = BEC(p) \Rightarrow \begin{cases} W^+ = BEC(p^2) \\ W^- = BEC(2p-p^2) \end{cases}$$

$$W^-(y_1 y_2 | u_1) = \sum_{u_2 \in \{0,1\}} \frac{1}{2} W(y_1 | u_1 \oplus u_2) W(y_2 | u_2)$$

$$\frac{W^-(y_1 y_2 | 0)}{W^-(y_1 y_2 | 1)} = \frac{W(y_1|0) W(y_2|0) + W(y_1|1) W(y_2|1)}{W(y_1|0) W(y_2|1) + W(y_1|1) W(y_2|0)}$$

$$= \frac{\cancel{W(y_1|1) W(y_2|1)} \left[1 + \frac{W(y_1|0)}{W(y_1|1)} \cdot \frac{W(y_2|0)}{W(y_2|1)} \right]}{\cancel{W(y_1|1) W(y_2|1)} \left(\frac{W(y_1|0)}{W(y_1|1)} + \frac{W(y_2|0)}{W(y_2|1)} \right)}$$

with

$$L_W(y) = \frac{W(y|0)}{W(y|1)}$$ we see

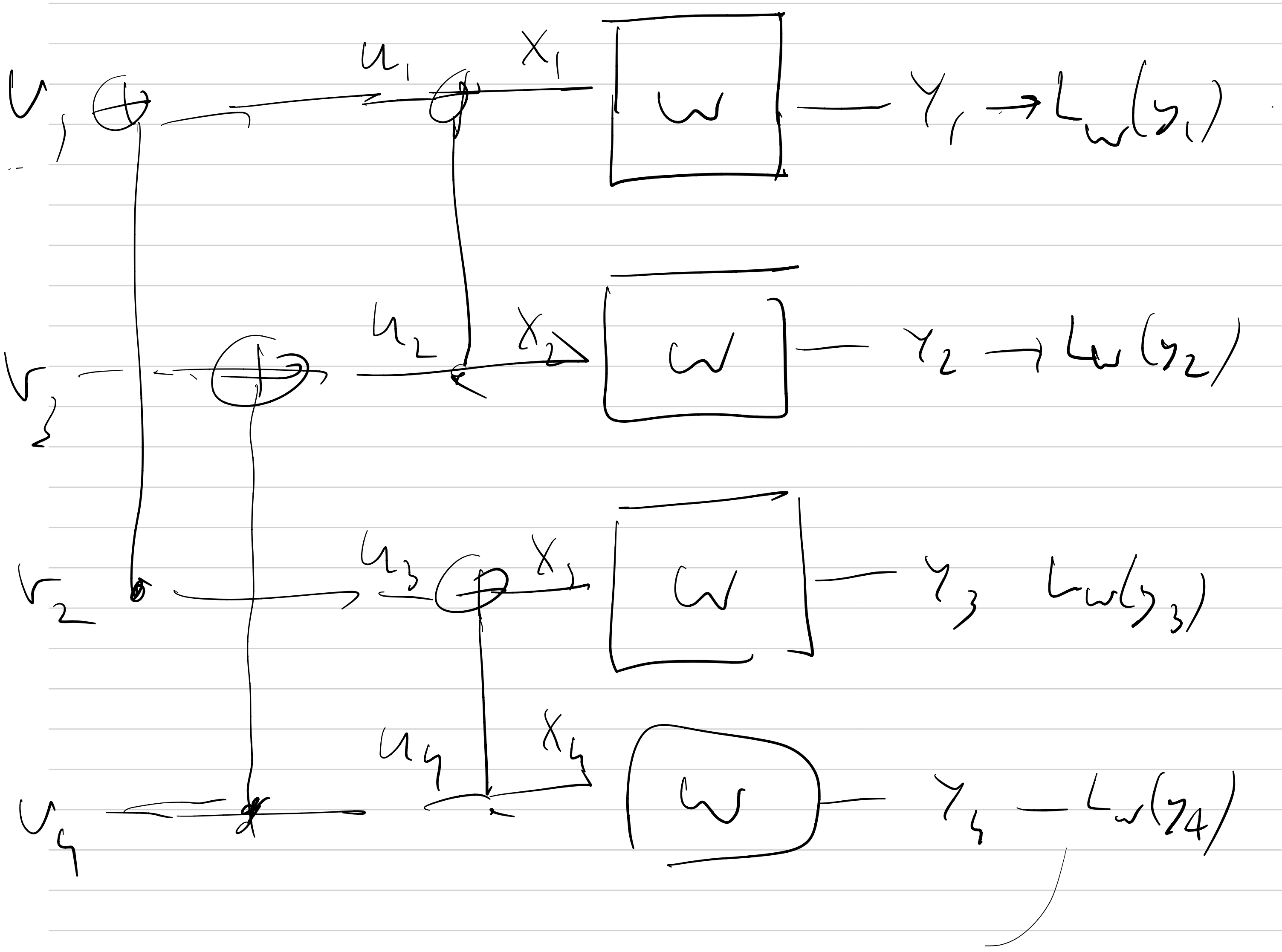
$$L_{W^-}(y_1 y_2) = \frac{1 + L_W(y_1) L_W(y_2)}{L_W(y_1) + L_W(y_2)}$$

$$W^+(y_1 y_2 u_1 | 0) = \frac{1}{2} W(y_1|u_1)\, W(y_2|0)$$

$$W^+(y_1 y_2 u_1 | 1) = \frac{1}{2} W(y_1|u_1 \oplus 1)\, W(y_2|1)$$

$$L_{W^+}(y_1 y_2 u_1) = \begin{cases} L_W(y_2)\, L_W(y_1) & u_1 = 0 \\ L_W(y_2) / L_W(y_1) & u_1 = 1 \end{cases}$$

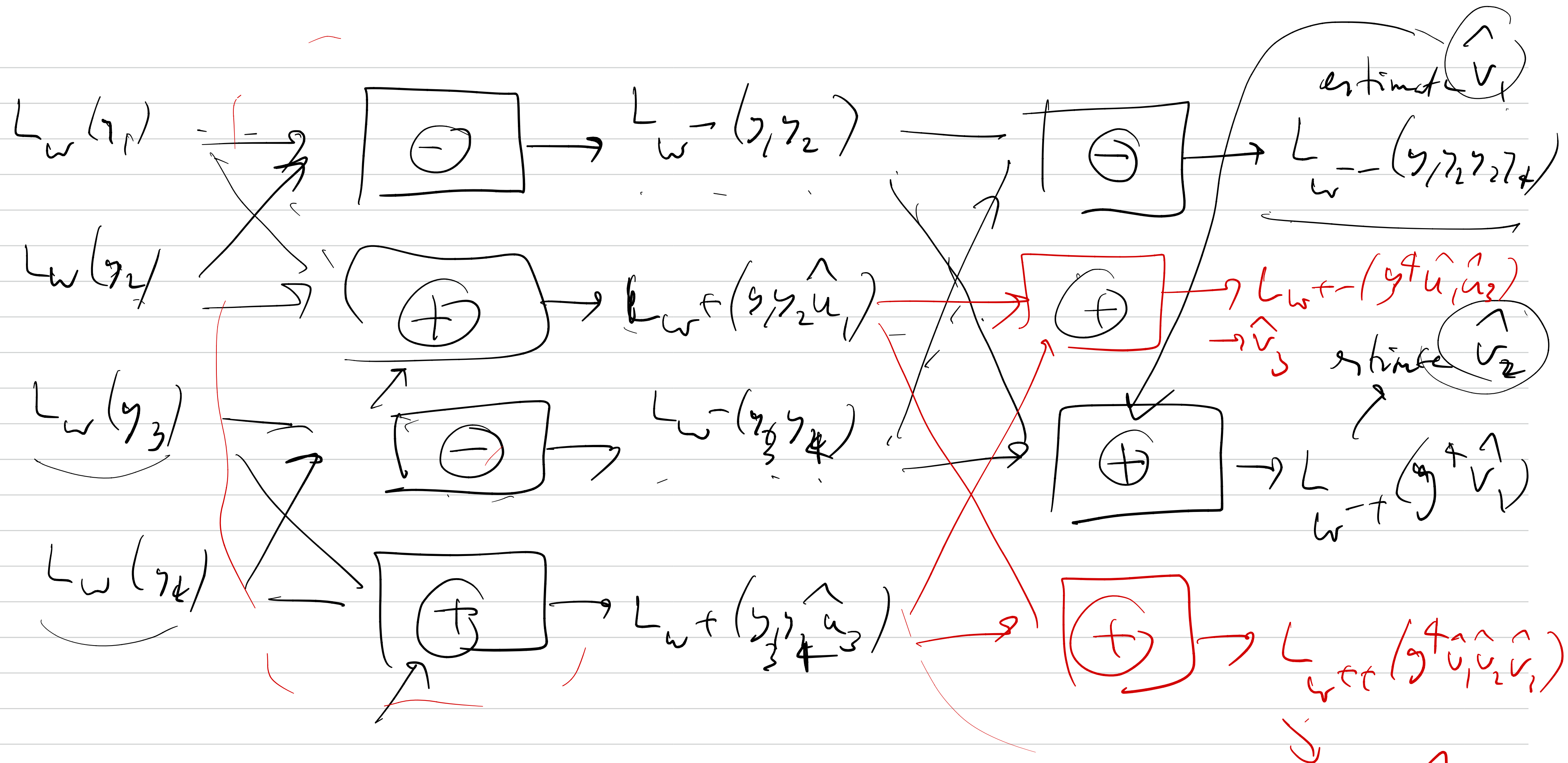
How to communicate:



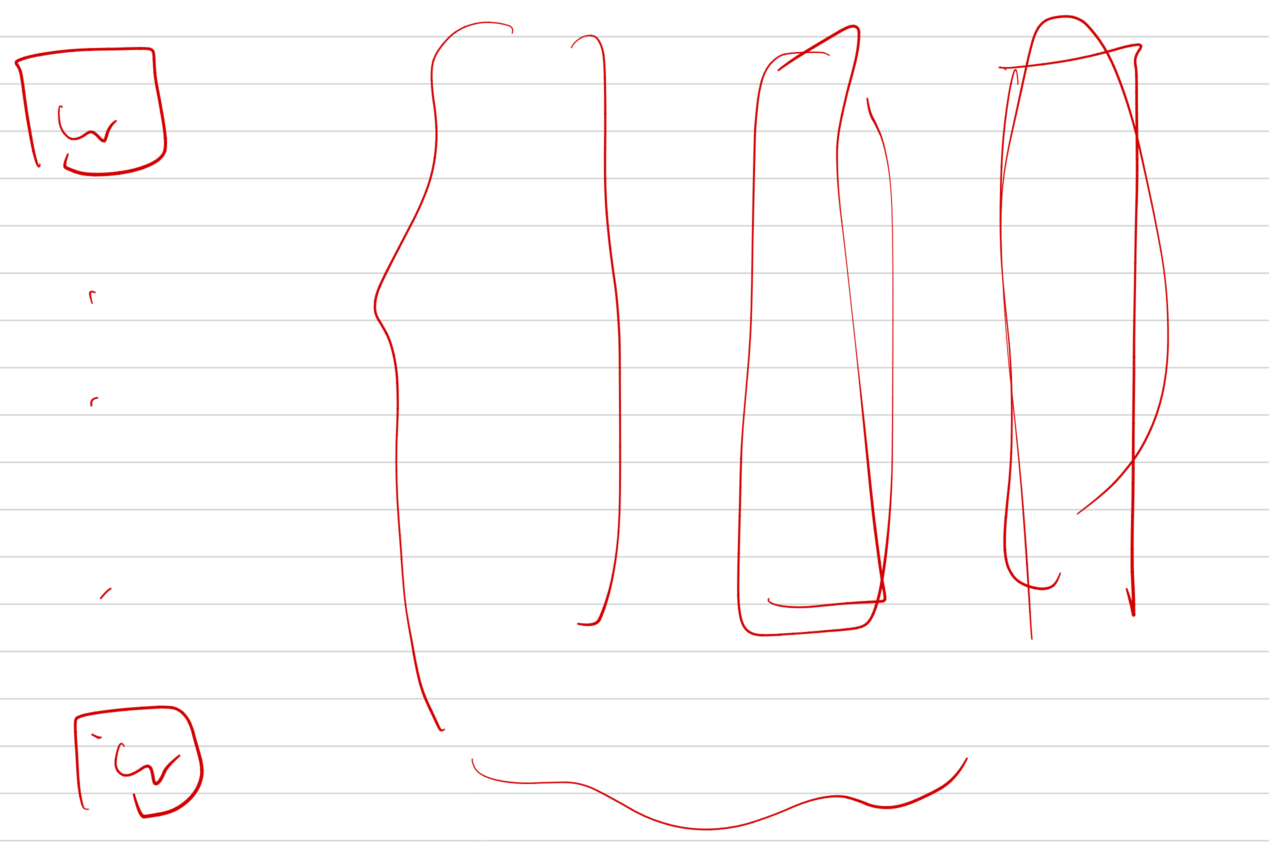
encoding takes t stages each stage has 2^t $\oplus$ operations

$\Rightarrow$ encoding effort is $t 2^t$ to encode $2^t = n$

data bits $\Rightarrow$ encoding takes $O(n \log_2 n)$ effort.



$\hat{u}_1, \hat{u}_2 = (\hat{v}_1 + \hat{v}_2, \hat{v}_2)$



2^t copies

t computation stages, each with 2^t ⊕ ⊖

$\Rightarrow$ total computational effort for decoding:

$t \cdot 2^t \cdot C(n, t)$

- In terms of the blocklength $n = 2^t$, the decoding effort is $(\text{const}) \cdot n(\log_2 n)$

We should note the following: data bits

$(u_1, \dots, u_n)$ $\quad n = 2^t$ travel over the synthetic channels $\{W^s : s \in \{+,-\}^t\}$, e.g.

$$u_1 \to \boxed{W^{--\cdots-}} \to$$

$$u_n \to \boxed{W^{++\cdots+}} \to$$

if W^s is a "good" channel $I(W^s) \approx 1$

so estimate of its input u_i will be most likely correct

if W^s is "not good" $\Rightarrow$ estimate will be wrong.

So: to use this polar enc/dec for reliable communication we should send data only on the indices i s.t. corresponding W^s is good. The remaining u_i's should be frozen to a known value, e.g. 0.

What we will show: among the 2^t

$\{W^s : s \in \{+,-\}^t\}$, we will have:

$$\boxed{\frac{1}{2^t} \sum_{s \in \{+,-\}^t} \mathbb{1}\{I(W^s) \geq 1-\varepsilon\} \xrightarrow[t \to \infty]{} I(W)}$$

$\Rightarrow$ when $R < I(W)$ we can find

$nR = (2^t R)$ good channels among the

$\{W^s : s \in \{+,-\}^t\}$ to send our data.

Yesterday, based on the numerical experiments, we had conjectured:

<u>Thm</u>: given $W = BEC(p)$, construct

$$\{W^s : s \in \{+,-\}^t\}, \quad W^s = BEC(p(s))$$

$$p(+) = p^2, \quad p(-) = 2p - p^2, \quad p(++) = (p^2)^2$$

$$p(+-) = 2p^2 - (p^2)^2, \ldots \text{etc.}$$ For any $\varepsilon > 0$.

$$\lim_{t \to \infty} \frac{1}{2^t} \sum_{s \in \{+,-\}^t} \mathbb{1}\{\varepsilon \leq p(s) \leq 1-\varepsilon\} \to 0$$ as t gets large

Corollary: the 2^t synthetic channels W^s will be of 3-types:

1. s for which $p(s) \in [\varepsilon, 1-\varepsilon]$ (ε-ugly).
2. s for which $p(s) < \varepsilon$ (ε-good).
3. " " " $p(s) > 1-\varepsilon$ (ε-bad).

$$\frac{1}{2^t} \sum_{s \in \{+,-\}^t} p(s) = p \qquad \text{for every } t.$$

together with fraction of ε-ugly channels $\simeq 0$

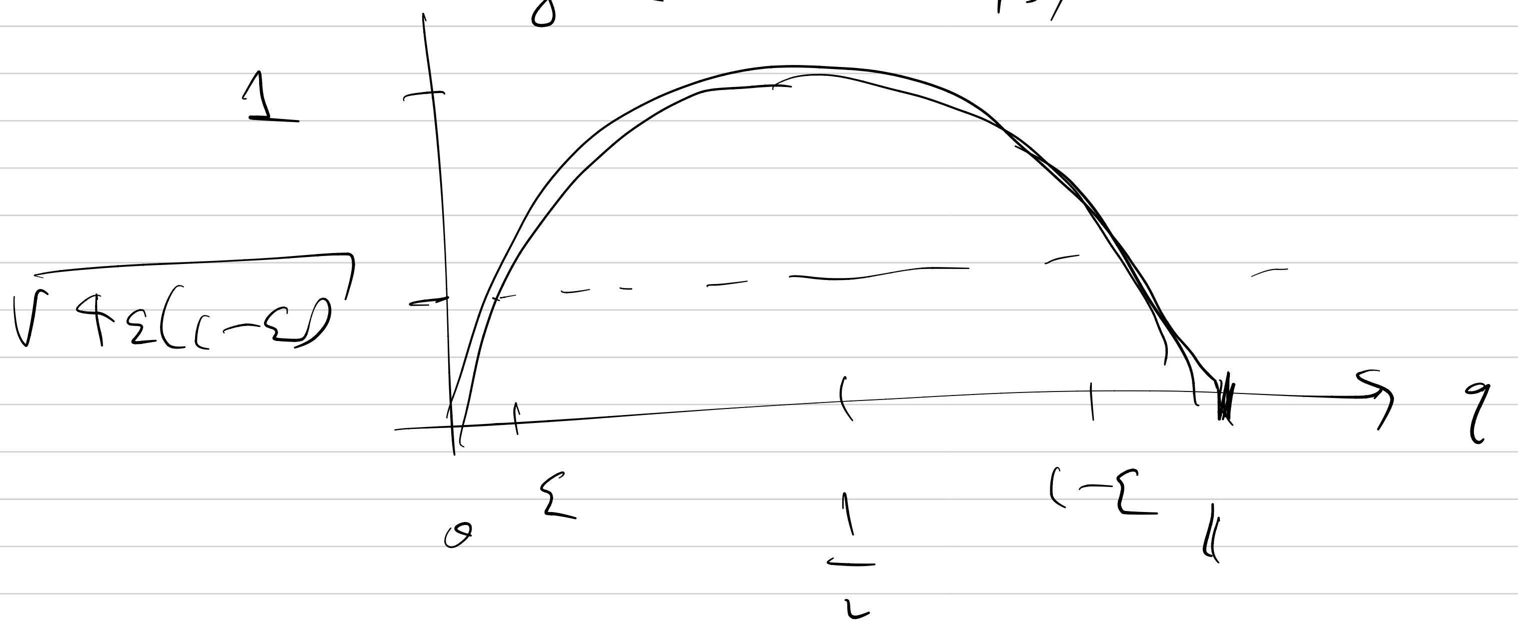
$\Rightarrow$ fraction of ε-good channels $\simeq 1-p$

fract of ε-bad " $\simeq p$.

To prove this theorem, let us define for BEC's a quantity:

$$\mathrm{ugl}(BEC(q)) = \sqrt{4q(1-q)}.$$

$\mathrm{ugl}(W = BEC(q))$



if $BEC(q)$ is ε-ugly then

$$\mathrm{ugl}(BEC(q)) \geq \sqrt{4\varepsilon(1-\varepsilon)}.$$

$$\equiv \quad \mathbb{1}\{BEC(q) \text{ is } \varepsilon\text{-ugly}\} \leq \frac{\mathrm{ugl}(BEC(q))}{\sqrt{4\varepsilon(1-\varepsilon)}}$$

$W = BEC(q)$

$$\mathrm{ugl}(W^-) = \sqrt{4q(2-q)(1-q(2-q))} = \mathrm{ugl}(W)\sqrt{(2-q)(1-q)}$$

$$\mathrm{ugl}(W^+) = \sqrt{4q^2(1-q^2)} = \mathrm{ugl}(W)\sqrt{q(1+q)}$$

$$\frac{1}{2}\mathrm{ugl}(W^-) + \frac{1}{2}\mathrm{ugl}(W^+)$$

$$= \mathrm{ugl}(W)\left(\frac{1}{2}\sqrt{q(1+q)} + \frac{1}{2}\sqrt{(2-q)(1-q)}\right)$$

$$\leq \mathrm{ugl}(W)\left(\frac{1}{2}\sqrt{\frac{1}{2}\cdot\frac{3}{2}} + \frac{1}{2}\sqrt{\frac{3}{2}\cdot\frac{1}{2}}\right)$$

$$= \mathrm{ugl}(W)\cdot\sqrt{\frac{3}{4}} < \mathrm{ugl}(W)$$

$$\Rightarrow \underbrace{\frac{1}{2^t} \sum_{s \in \{+,-\}^t} \mathrm{ugl}(W^s)} \le \left(\sqrt{\frac{3}{4}}\right)^t \cdot \mathrm{ugl}(W) \searrow 0$$

as $t \nearrow \infty$

$$\Rightarrow \frac{1}{2^t} \sum_{s \in \{+,-\}^t} \mathbb{1}\{W^s \text{ is } \varepsilon\text{-ugly}\}$$

$$\le \frac{1}{2^t} \sum_{s \in \{+,-\}^t} \mathrm{ugl}(W^s) / \sqrt{4\varepsilon(1-\varepsilon)}$$

$$\le \frac{1}{\sqrt{4\varepsilon(1-\varepsilon)}} \cdot \left(\sqrt{\frac{3}{4}}\right)^t \searrow 0 \quad \text{as } t \nearrow \infty.$$

Based on this let us try to bound the error probability of our communication system:

$n = 2^t$ we have $(U_1 .. U_n)$

$\rightarrow (X_1 .. X_n) \rightarrow W \rightarrow (Y_1 .. Y_n)$

$\rightarrow (\hat{U}_1 .. \hat{U}_n)$.

U_i = data if U_i travels on a good channel

$U_i = 0$ " " " not good channel

$$\Pr(\hat{U}_i \neq U_i) = \frac{1}{2} p(s) \quad \text{if } W^s \text{ is the channel}$$
on which U_i is sent.

$$\Rightarrow \Pr(\text{error}) \leq \sum_{\substack{s \in \{+,-\}^t : \\ W^s \text{ is } \varepsilon\text{-good}}} \Pr(\hat{U}_i \neq U_i)$$

$$= \frac{1}{2} \sum_{\substack{s \in \{+,-\}^t : \\ W^s \text{ } \varepsilon\text{-good}}} p(s) \leq \frac{\varepsilon}{2} \cdot \sum_{\substack{s \in \{+,-\}^t \\ W^s \text{ is } \varepsilon\text{-good}}} 1$$

$$\leq \frac{\varepsilon}{2} \cdot 2^t$$

So, the theorem we have shown is not strong enough to show that $P(\text{error})$ is small.

To show that we have a reliable communication system we need to show:

$$\frac{1}{2^t} \sum_{s \in \{+,-\}^t} \mathbb{1}\{p(s) : p(s) \leq \varepsilon_t\} \to 1 - p$$

with $\varepsilon_t \ll \frac{1}{2^t}$

if we can show:

$$\frac{1}{2^t}\sum_{s\in\{+,-\}^t} \mathbb{1}\{w^s \text{ is } \varepsilon_t\text{-ugly}\} \longrightarrow 0$$

with some $\varepsilon_t \ll \frac{1}{2^t}$

we will be done.

This is what we will show next.

depth

0: W

1: w^+ $\quad$ w^-

2: w^{++} $\quad$ w^{+-} $\quad$ w^{-+} $\quad$ w^{--}

p

$p(+)$ $\quad$ $p(-)$

$p(++)$ $\quad$ $p(+-)$ $\quad$ $p(-+)$ $\quad$ $p(--)$

fix $0 < \varepsilon < \frac{1}{10}$. Recall

W^s is ε-good if $p(s) < \varepsilon$

is ε-bad if $p(s) > 1-\varepsilon$

is ε-ugly if $\varepsilon \le p(s) \le 1-\varepsilon$.

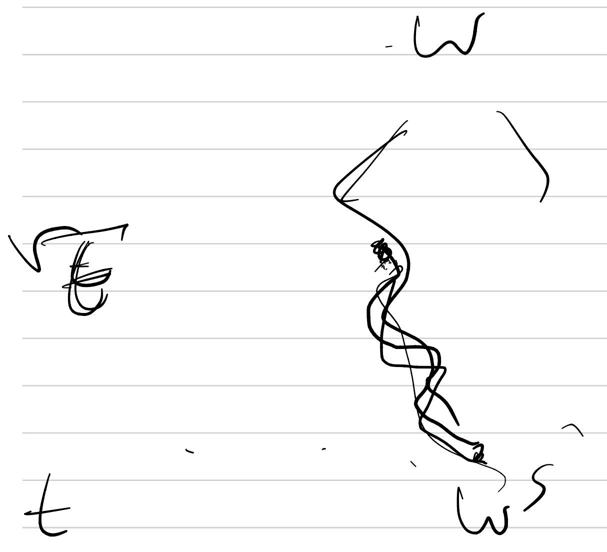
the fraction of ε-ugly channel at depth t

$\le c(\varepsilon) \left(\frac{3}{4}\right)^{t/2}$

Define a channel $W^{(s,t)}$ to be

ε- tainted if $\exists\ \sqrt{t} \le i \le t$ s.t

W^{s^i} is ε-ugly.



the fraction of channels at depth t that are

tainted $\le \sum_{i=\sqrt{t}}^{t}$ (fraction of ε-ugly channels at depth i)

$\le c(\varepsilon) \sum_{i=\sqrt{t}}^{t} \left(\sqrt{\frac{3}{4}}\right)^i \le c(\varepsilon) \sum_{i=\sqrt{t}}^{\infty} \left(\sqrt{\frac{3}{4}}\right)^i$

$$\leq c(\varepsilon)\left(\sqrt{3/4}\right)^{\sqrt{t}} \frac{1}{1-\sqrt{3/4}}$$

$$= c'(\varepsilon)\cdot\left(\sqrt{3/4}\right)^{\sqrt{t}} \searrow 0 \quad \text{as } t \text{ gets large}$$

$\Rightarrow$ fraction of tainted channels is ≈ 0 if t is large.

if W is ε-bad

$\Rightarrow$ W^+ is either ε-bad ε-ugly

W^- is ε-bad

if W is ε-good

W^+ is ε-good

W^- is ε-good or ε-ugly

if $W^{(s^t)}$ is ε-untainted & ε-good

$\Rightarrow$ then all $W^{(s^i)}$ for $\sqrt{t} \leq i \leq t$ are also

ε-good.

So far: among the channel

$\{W^s : s \in \{+,-\}^t\}$ there are $\approx (1-p)$ fraction ε-good channel

$\approx p$ fraction ε-bad chan

≈ 0 fraction ε-ugly chann

≈ 0 fraction ε-tainted channels

$\Rightarrow$ among these channels $\approx (1-p)$ fraction will be both ε-good and ε-untainted.

Def a channel W^{s^t} is said to be ε-lucky if

$$\underbrace{s^t = (s_1 \ldots s_t)} \text{ has } \leq \underbrace{\tfrac{t}{2}(1+\varepsilon)} \text{ "$-$" signs.}$$

$$\equiv \quad \geq \tfrac{t}{2}(1-\varepsilon) \text{ "$+$" signs}$$

the fraction of ε-unlucky channels $\to 0$ as $t \to \infty$.

$\Rightarrow$ the fraction of ε-good, ε-lucky, ε-untainted channels at depth t is $\approx (1-p)$.

Pick such a channel W^{s^t} and consider

$p(s^t)$, by analyzing the evolution

$$p(s^i) \to p(s^{i+1})$$

$$p(s^i) \to \begin{cases} p(s^i_+) = p(s^i)^2 \\ p(s^i_-) \leq 2p(s^i) \end{cases}$$