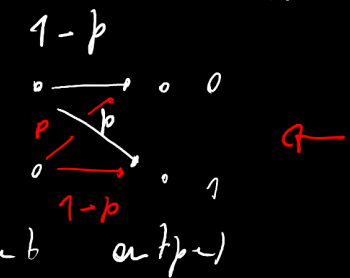
Random Code Ensemble

$$m \xrightarrow{\text{encoding}} \underline{x} \xrightarrow{\text{channel}} \underline{y} \xrightarrow{\text{decoding}} \underline{x}^d \longrightarrow m'$$

$m, m' \in \{0,1\}^M$; $\underline{x}, \underline{x}^d \in \{0,1\}^N$ $\quad R = M/N$

$\underline{y} \in \mathcal{Y}^N$ — in general

— Binary Symmetric Channels $\quad \underline{y} \in \{0,1\}^N$



$2^{N 2^M}$ possible codes ; $R < C$ — uniform prob. distribution across codes

Distance Enumerator

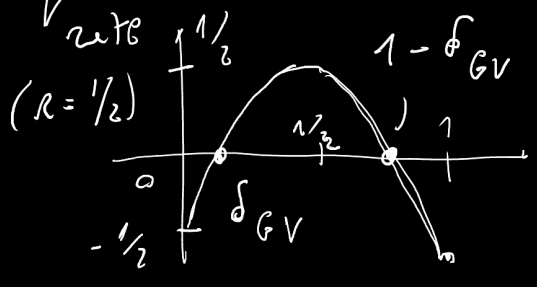
$N_{\underline{x}_0}(d)$ $\quad \underline{x}_0$ codeword $\in$ the Hamming space $\{0,1\}^N$ (2^M codewords)

$$\mathbb{E}\, N_{\underline{x}_0}(d) = \frac{2^M - 1}{2^N} \binom{N}{d}$$

$$\mathbb{E}\, N_{\underline{x}_0}(d) \underset{N \gg 1}{\simeq} 2^{N\left[R - 1 + \mathcal{H}_2(\delta)\right]} \qquad \delta = d/N$$

growth rate

$0 \le \delta \le 1$



$\delta_{GV} \;/\; \mathcal{H}_2(\delta_{GV}) = 1 - R$

(Gilbert-Varshamov distance

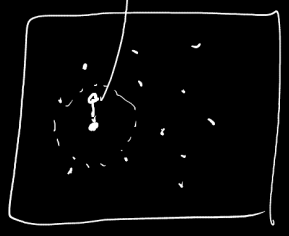
$\delta_{GV}(R = 1/2) \approx 0.11$ (on a déjà vu ça $-\varepsilon^*$ in RETM)

(1) $\delta < \delta_{GV}(R)$ ⇒ negative growth rate

average # of codewords found at a distance $d = \delta N$ vanishes exponentially (with N)

(2) $\delta_{GV}(R) < \delta < 1 - \delta_{GV}(R)$ ⇒ positive growth rate

⇒ average # of codewords at distance d is exponentially large in N



(1) ⟶ successfull decoding

(2) ⟶ unsuccessfull decoding

The lower R, the higher δ_{GV} if $\delta < \delta_{GV}$ no other codeword is found at a distance $d = N\delta$

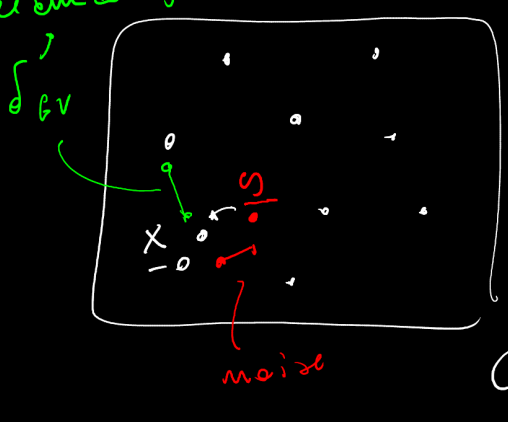
Direct statement of the channel coding theorem:

$\underline{x}_0$ is the codeword transmitted through the channel

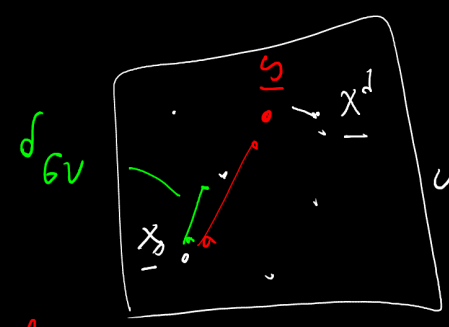
channel output is $\underline{y}$ (most typically $\underline{y} \notin \mathcal{C}_N$)

($\underline{y} \neq \underline{x}_0$ due to channel noise)

Decoding: $\underline{x}^1$ such that $d(\underline{x}^1, \underline{y})$ is minimum



successfull decoding ($\underline{x}^1 = \underline{x}_0$)



$\underline{x}^1 \neq \underline{x}_0$ unsuccessfull decoding

channel noise ⟶ p (spin flip prob.)

$d(\underline{x}_0, \underline{y}) \underset{N \gg 1}{\simeq} Np$ (sum of N Bernoulli processes)

The other $2^n - 1$ codewords are not correlated with $\underline{x}_0$ (and not with $\underline{y}$)

$\Rightarrow$ $\{\underline{y}, \underline{x}_1, \dots, \underline{x}_{2^n}\}$ is a set of 2^n random points in Hamming space

(1) if $p = \frac{d(\underline{x}_0, \underline{y})}{N} < \delta_{GV}$ more of the other codewords is closer to $\underline{y}$ than $\underline{x}_0$
($\Rightarrow$ successfull decoding)

(2) if $p = \frac{d(\underline{x}_0, \underline{y})}{N} > \delta_{GV}$ exponentially many other codewords are closer to $\underline{y}$ than $\underline{x}_0$
$\rightarrow$ unsuccessfull decoding

[$\underline{x}^d$ chosen / $d(\underline{x}^d, \underline{y}) = N\delta_{GV}$ — the number of such codewords increases with N even than exponent.]

δ_{GV} / $R - 1 + \mathcal{H}_2(\delta_{GV}) = 0$

(1) $\rightarrow$ $p < \delta_{GV} \Leftrightarrow R < 1 - \mathcal{H}_2(p)$

($\mathcal{H}_2(p) < \mathcal{H}_2(\delta_{GV})$ if $p < 1/2$)

$C = 1 - \mathcal{H}_2(p)$ — channel capacity for BST

$R < C$

$$C = \max_{p(x)} I_{X,Y} = \max_{p(x)} \left[H_Y - H_{Y/X} \right]$$

$$= \max_{p(x)} H_Y - \mathcal{H}_2(p)$$

$$\overset{\text{uniform } p(y)}{\underset{\text{(for uniform } p(x))}{}} = 1 - \mathcal{H}_2(p)$$

Different decoding strategies (in a Bayesian framework)

word MAP, symbol MAP encoding

MAP = Max. A Posteriori prob.

$$\underbrace{P(\underline{x} \mid \underline{y})}_{\text{decoding probability for } \underline{x} \text{ given channel output } \underline{y}} = \frac{1}{Z(\underline{y})} \underbrace{\prod_{i=1}^{N} Q(y_i \mid x_i) \Pi(x_i)}_{\text{BAYES THEOREM}}$$

"a priori" prob. for the input message

$$Z(\underline{y}) = \sum_{\underline{x}} Q(\underline{y} \mid \underline{x}) \Pi(\underline{x})$$

$\underline{x}$ = model parameter $\quad \left(\Rightarrow \sum_{\underline{x}} P(\underline{x} \mid \underline{y}) = 1 \right)$

$\underline{y}$ = observed data

$Q(\underline{y} \mid \underline{x})$ = likelihood

uniform prior $\Pi(\underline{x}) = \dfrac{1}{|\mathcal{C}_N|} \mathbb{I}(\underline{x} \in \mathcal{C}_N)$ $\quad \sim 2^n$

(MAP = maximum likelihood

Word MAP: maximize $\mu_y(\underline{x}) = \frac{1}{Z(\underline{y})} \prod_i Q(y_i|x_i)\mu_0(\underline{x})$ (posterior for the codeword)

Symbol MAP: maximize the posterior marginals separately for each bit

uniform prior p

$$\mu_y^{(i)}(x_i) = \sum_{\underline{x}\setminus i} \mu_y(\underline{x})$$

Formally: WORD MAP: $\underline{x}^d(\underline{y}) = \arg\max_{\underline{x}} \mu_y(\underline{x})$

SYMBOL MAP: $x_i^d(\underline{y}) = \arg\max_{x_i} \mu_y^{(i)}(x_i)$

BSC WORD MAP

$$\mu_y(\underline{x}) = \frac{1}{Z'(\underline{y})} p^{d(\underline{x},\underline{y})} (1-p)^{N-d(\underline{x},\underline{y})} \mathbb{I}(\underline{x}\in\mathcal{C}_N)$$

$$(Z'(\underline{y}) = Z(\underline{y})\,|\mathcal{C}_N|)$$

$$= \frac{1}{Z'(\underline{y})} (1-p)^N \cdot \left(\frac{p}{1-p}\right)^{d(\underline{x},\underline{y})} \mathbb{I}(\underline{x}\in\mathcal{C}_N)$$

$p < 1/2 \Rightarrow \frac{p}{1-p} < 1 \Rightarrow \arg\max_{\underline{x}} \mu_y(\underline{x})$

WORD MAP decoding = find the closest codeword to channel output $\arg\min_{\underline{x}} d(\underline{x},\underline{y})$

SYMBOL MAP decoding

$$\mu_y^{(i)}(x_i) = \sum_{\underline{x}\setminus i} \mu_y(\underline{x}) = \frac{1}{Z(y)} \sum_{\underline{x}\setminus i} \exp\left[-2\beta d(\underline{x},\underline{y})\right] \mathbb{I}(\underline{x}\underline{H}^T)$$

$$\beta \equiv \frac{1}{2}\log\left(\frac{1-p}{p}\right) > 0 \quad (p < 1/2)$$

$$Z(\underline{y}) = \sum_{\underline{x}} \exp\left(-2\beta d(\underline{x},\underline{y})\right)$$

contribution to $\mu_y^{(i)}(x_i)$ from all codewords weighted by the factor $\exp\left(-2\beta d(\underline{x},\underline{y})\right)$

$$Z(\underline{y}) = \underbrace{\exp\left(-2\beta d(\underline{x}^{(0)},\underline{y})\right)}_{Z_{corr}} + \left(\begin{array}{l}\underline{x}^{(0)} \text{ is the} \\ \text{correct} \\ \text{codeword}\end{array}\right)$$

$$+ \underbrace{\sum_0^N d\, \hat{N}_{\underline{y}}(d) \exp(-2\beta d)}_{Z_{err}}$$

$\hat{N}$ – distance enumerator for incorrect codewords

$$d(\underline{x}^{(0)},\underline{y}) \underset{N\gg 1}{\simeq} Np \Rightarrow Z_{corr} \simeq \exp(-2NB p)$$

for Z_{err} saddle point method $\sum_0^N d \to \int_0^1 d\delta$

$$Z_{err} \underset{N\gg 1}{\simeq} N \int_{\delta_{GV}}^{1-\delta_{GV}} \exp\left[N\left(\log_2(q-1) + \mathcal{H}(\delta) - 2\beta\delta\right)\right] d\delta \qquad \delta = d/N$$

$Z_{err} \underset{N\gg 1}{\simeq} \exp[N \phi_{err}]$ ϕ_{err} is the max of the $\log 2(R-1) + \mathcal{H}(\delta) - 2\beta\delta$ over δ in $(\delta_{GV}, 1-\delta_{GV}]$ (for $\delta = \delta^*$)

(2) $p \geq \delta^* > \delta_{GV}$ (but we need to check whether $\delta_{GV} < \delta^* < 1-\delta_{GV}$)

$\delta^* = p$

$\rightarrow \phi_{err} = \log 2(R-1) - \log(1-p)$

extremum condition

$\mathcal{H}'(\delta) = 2\beta = \log\left(\frac{1-p}{p}\right)$

$\| \quad \log\left(\frac{1-\delta}{\delta}\right)$

(1) $p < \delta_{GV}$; $\delta^* = \delta_{GV}$

$\rightarrow \phi_{err} = -\delta_{GV} \log\left(\frac{1-p}{p}\right)$

$$Z_{com}/Z_{err} \underset{N\gg 1}{\simeq} \begin{cases} \exp\left(-N \log\left(\frac{1-p}{p}\right)(p-\delta_{GV})\right) & p < \delta_{GV} \quad (1) \\ \exp\left[-N\left[\log 2(R-1) + \mathcal{H}(p)\right]\right] & p > \delta_{GV} \quad (2) \end{cases}$$

(1) $\rightarrow$ Z_{com} is the leading term $\rightarrow$ successful decoding

(2) $\underbrace{\log 2(R-1) + \mathcal{H}(p)}_{\text{growth rate}} > 0$ if $p > \delta_{GV}$

$\rightarrow$ Z_{err} is the leading term $\rightarrow$ unsuccessful decoding

!

Wrong codewords are selected at $\delta^* = p > \delta_{GV}$

(these are not the codewords closest to y)

There are exponentially many codewords at $\delta^* = p$