Converse of the Noisy Coding Theorem (NOT in MacKay)

"If $R > C(Q)$: $\exists \delta > 0$ $\exists N_0\ \forall N \geq N_0$: $\nexists$ code with $\frac{K}{N} \geq R$ & $p_B \leq \delta$"

Tools: ① Data Processing Inequality (DPI) for $A \to B \to C$ Markov chain:

$$I(A:B) \geq I(A:C) \quad \& \quad H(A|B) \leq H(A|C)$$

i.e. $P(a,b,c) = P(a)P(b|a)P(c|b)$

② If X^N arbitrary and Y^N channel output: ← i.e. $P(x^N, y^N) = P(x^N) Q(y_1|x_1)\cdots Q(y_N|x_N)$

$$I(X^N : Y^N) \leq \sum_{i=1}^{N} I(X_i : Y_i) \leq N \cdot C(Q)$$

HW 5

③ Fano's inequality for $S \to T \to \hat{S}$ Markov chain, $p = \Pr(S \neq \hat{S})$

$$\boxed{H(\{p, 1-p\}) + p \cdot \log \#A_S \geq H(S|\hat{S}) \geq H(S|T)}$$

Proof of the Converse:

Consider (N,K)-code with $\frac{K}{N} \geq R > C$. Let $S \in \{1, \ldots, 2^K\}$ uniform. Then:

$$* \ H(S|Y^N) = H(S) - I(S:Y^N) \overset{\text{DPI ①}}{\geq} H(S) - I(X^N;Y^N) \overset{②}{\geq} K - N\cdot C$$

$S \to X^N \to Y^N$ Markov chain

$$* \ H(S|Y^N) \overset{\text{Fano ③}}{\leq} 1 + \Pr(\hat{S} \neq S) \cdot \log \#A_S = 1 + p_B \cdot K$$

$S \to Y^N \to \hat{S}$ Markov chain

$$\Rightarrow \ K - N\cdot C \leq 1 + p_B \cdot K$$

$$\Rightarrow \ p_B \geq \frac{1}{K}(K - N\cdot C - 1) = 1 - \frac{N\cdot C}{K} - \frac{1}{K} \geq \underbrace{1 - \frac{C}{R}}_{>0} - \underbrace{\frac{1}{NR}}_{\to 0} \qquad \square$$

Can never go below this for large enough N

Are we happy? What questions does Shannon's theorem leave unaddressed? algorithmics, large N, ... how to even compute C?

Shannon's Theorem vs. Practice (§11)

- Need large block size N for joint typicality vs. fixed packet size
- Codebook $x^N(1), \dots, x^N(2^k)$ exponentially large in N (if $R>0$) → HW 5
- Random codes vs predictable performance

A family of codes is "very good" if $\frac{k}{N} \to C$ & $p_B \to 0$

"good" if $\frac{k}{N} \geq R > 0$ & $p_B \to 0$

"bad" otherwise

... and practical if ∃ efficient encoder + decoder

Often run in embedded devices (cell phone, satellite, TV, ...)!

In practice:

do you know what this means?

* most codes are linear (x^N linear function of s^k)

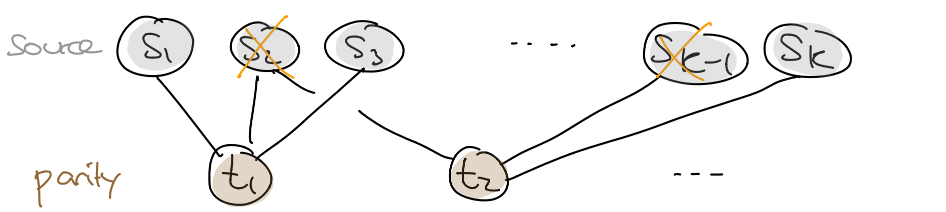
* "easy" to come up with "plausible" encoders — but optimal decoding is in general (NP) hard! ← unlike for compression!

$$\boxed{\sigma_{opt}(y^N) = \underset{\hat{s}}{\operatorname{argmax}}\ P(\hat{s} \mid y^N)}$$

Why? If $P(s)$ arbitrary prior, want to choose σ to maximize $\Pr(\hat{S}=S)$

$= \underbrace{\sum_{y^N} \Pr(S=\sigma(y^N), Y^N=y^N)}_{\text{choose } s=\sigma(y^N) \text{ that maximizes } P(s,y^N) \propto P(s \mid y^N)}$

e.g. imagine the following (LDPC) code:



e.g. 4 bits per parity constraint, each bit in 3 parity constraints

For erasure channel:

$s_1 \oplus \cancel{s_2} \oplus s_3 \oplus t_1 = 0$

$s_2 \oplus \dots \oplus \cancel{s_{k-1}} \oplus t_2 = 0$

...

* types of decoders: "algebraic" vs. "iterative"

Types of codes:

* block codes: e.g. Hamming, Reed–Solomon, LDPC codes

  Reed–Solomon: storage, bar codes, sat comm — TODAY

  LDPC codes: WiFi, DVB, ...

* Convolutional: e.g. turbo codes (3G/4G/LTE, sat. comm.) — NEXT WEEK

  ≈ linear streaming codes

Reed-Solomon Codes

e.g. PDF417 bar code
$q = 929,\ \alpha = 3,\ T = 4$

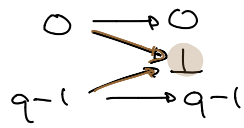
Alphabet: $\mathcal{A} = \mathbb{F}_q$ for q prime ← prime power ok, too

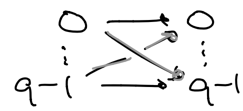
↳ $\{0, \ldots, q-1\}$ with $+$ and $\cdot$ modulo q
(finite field with q elements)

Parameters: $K < N \leq q$ and $\alpha \in \mathbb{F}_q$

* overhead: $T := N - K$
* Can correct up to T erasures (= known error locations)

  or up to $\frac{T}{2}$ errors (= at unknown locations)





* α should be a "generator": $\mathbb{F}_q = \{0, \alpha, \alpha^2, \ldots, \alpha^{q-1} = 1\}$ any nonzero element is power of α

  always exists! e.g. $\mathbb{F}_3 = \{0, 2, 2^2 = 1\}$ $\mathbb{F}_7 = \{0, 3, 3^2 \equiv 2, 3^3 \equiv 6, 3^4 \equiv 4, \ldots\}$

↳ generator polynomial: $G = (X - \alpha) \cdots (X - \alpha^T)$

variables of the polynomial

Encoder: Input: $s^K \in \mathcal{A}^K$

* $P \leftarrow s_1 + s_2 X + \ldots + s_K X^{K-1}$
* $R \leftarrow P \cdot X^T \bmod G$ ← degree $< T$ (remainder of poly division)
* $M \leftarrow P \cdot X^T - R$ ← degree $N-1$ & leading coeffs $s_K, \ldots, s_1$
* $x^N \leftarrow$ coefficients of M ← i.e. $M = x_1 + x_2 X + \ldots + x_N X^{N-1}$

By construction:

M is multiple of G

$\Rightarrow \boxed{M(\alpha) = 0}$ & ... & $\boxed{M(\alpha^T) = 0}$

These are our "parity checks".

$\boxed{\text{ex:}}$ $k=1$, $N=3$, $q=3$ and $\alpha=2$

$\hookrightarrow T=2$ & $G=(X-2)(X-1)=X^2-1$

To <u>encode</u> $s \in \mathbb{F}_q$:

* $P \leftarrow s$
* $R \leftarrow s \cdot X^2 \bmod G = s \cdot X^2 - s \cdot G = s$
* $M \leftarrow s \cdot X^2 - R = s \cdot G$
* $x^N \leftarrow [-s, 0, s]$

$\boxed{\text{How to decode?}}$