STO8 LECTURE 11 3/12/2008

Note Title 3/11/2008

TODAY: Decoding Concatenated Codes

- Simple Decoding
- Achieving Shannon Capacity on BSC.
- Decoding upto half the distance.

Recall Concatenation

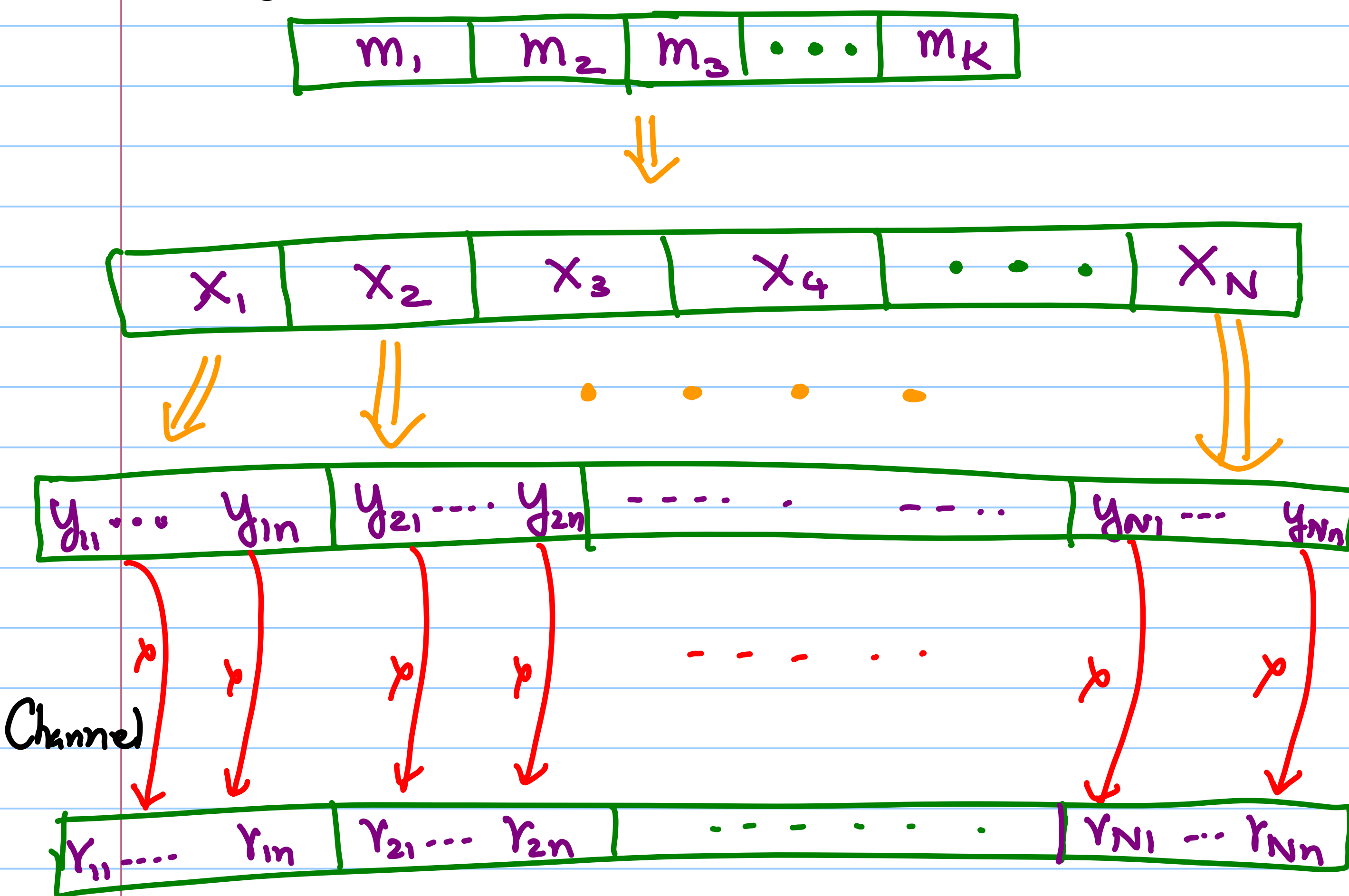
Outer Code: $[N, K, D]_Q$ (e.g. RS code)

Inner Code: $[n, k, d]_q$ (e.g. greedy code)

Composed Code:

$$[Nn, Kk, Dd]_q$$

Encoding



Decoding Problem: Compute $m_1 \dots m_K$ given

$Y_{11} \dots Y_{1n} \dots Y_{N1} \dots Y_{Nn}$

Simple Decoding

$$\boxed{y_{11} \cdots y_{1n} \;\big|\; y_{21} \cdots y_{2n} \;\big|\; \cdots \;\big|\; y_{N1} \cdots y_{Nn}}$$

Brute force $\downarrow$

$$\boxed{Z_1 \;\big|\; Z_2 \;\big|\; \cdots \;\big|\; Z_N}$$

Outer decoder $\Downarrow$

$$\boxed{\tilde{m}_1 \quad \tilde{m}_2 \quad \cdots \quad \tilde{m}_k}$$

$$Z_i = \underset{z}{\arg\min} \left\{ \Delta\left(E_{inner}(z), (y_{i1} \cdots y_{in}) \right) \right\}$$

$\uparrow$

minimizes distance to $\boxed{y_{i1} \cdots y_{in}}$

Claim 1: if # errors in block $i < d/2$

then $y_i = z_i$

Claim 2: if $\#\{\text{block } i \text{ s.t. } y_i \neq z_i\} < D/2$

then $(m_1 \ldots m_K) = (\tilde{m}_1 \ldots \tilde{m}_K)$

Claim 3: if total # errors $< \frac{D}{2} \cdot \frac{d}{2}$ then

$\#\{\text{blocks with} \geq d/2 \text{ errors}\} < D/2$

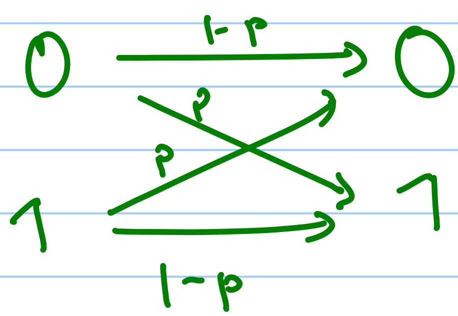
Proof: Else # errors $\geq \frac{d}{2} \cdot \frac{D}{2}$.

Theorem 1: Simple Decoder corrects $\frac{d}{2} \cdot \frac{D}{2}$ errors.

(Imm. from Claims 1, 2, 3)

Notes:
- Not best possible since one should be able to correct $\frac{D \cdot d}{2}$ (as opposed to $\frac{Dd}{4}$) errors.
- Still .... suffices to get Shannon Capacity on BSC

Recall BSC(p)



Bits flipped independently

Shannon Coding / Decoding

- Can pick code at random; decode in exp(n) time; get error $2^{-\epsilon n}$; with $R = 1 - H(p) - \delta$
- Can easily get polytime alg. with error $1/\text{poly}(n)$; & $R = 1 - H(p) - \delta$
  - Break message into $c \log n$ bit blocks & apply Shannon code separately to each.

- $\Pr[i^{th}$ block decoded incorrectly$] \leq \frac{1}{poly(n)}$
- $\Pr[\exists\, i$ s.t. $\quad] \leq \frac{n}{poly(n)}$
- Decoding time $= n \cdot \exp(c \log n)$
  $= poly(n)$.
- So main question: Can we reduce error to $\exp(-n)$. with $poly(n)$ running time.
- GOOD NEWS: Can count on even distribution of errors.

Forney's Result

- Outer code of rate $(1-\epsilon)$; length N
- Inner code of rate $1 - H(p) - \epsilon$; length n
- Rate of composed code $1 - H(p) - 2\epsilon$
- $\Pr[i^{th}$ block decoded incorrectly$]$

$$\leq \exp(-n) \quad [\text{Shannon}]$$

- $\Pr[$more than $\frac{\epsilon N}{2}$ blocks decoded incorrectly$] \leq 2^N \cdot (\exp(-n))^{\frac{\epsilon N}{2}}$

$$= \exp(-nN)$$

- Decoding runs in time $\text{poly}(N) \cdot \exp(n)$

Theorem 2 [Forney]: Can get arbit. close to capacity (of any) channel with poly time encoding + decoding. & exp(− length) error.

Decoding More Errors

Key Insights:

- Can get RS decoder to correct more erasures than errors.
- If # errors in inner block too many, then better to declare erasure!

Algorithm:

- Let z_i = decoding of inner block i
- Let $e_i = \Delta(E(z_i), y_i)$ = # apparent errors i^{th} block
- W.p. $\frac{e_i}{(d/2)}$ declare i^{th} block erased; & W.p. $1 - \frac{e_i}{(d/2)}$ keep z_i; Decode outer stuff.

Analysis

Claim: Outer decoder corrects s erasures & t errors provided $s + 2t < d$

Proof: Outer code becomes $[n-s, k, d-s]$ RS code.

$\Rightarrow$ Decoder corrects $t < \frac{d-s}{2}$ errors.

Let $\tilde{e}_i$ = actual # errors in i^{th} block.

if $Y_i = Z_i \Rightarrow e_i = \tilde{e}_i$

$Y_i \neq Z_i \Rightarrow \tilde{e}_i \geq d - e_i$

Let $U_i = 1$ if i^{th} block erased

$V_i = 1$ if i^{th} block not erased & $Y_i \neq Z_i$

Claim: $E[U_i + 2V_i] \leq \dfrac{2\tilde{e}_i}{d}$

Proof:

Case 1: $\boxed{Y_i = Z_i}$

$$E[V_i] = 0$$

$$E[U_i] = \frac{2e_i}{d} = \frac{2\tilde{e}_i}{d}$$

Case 2: $\boxed{Y_i \neq Z_i}$

$$\left.\begin{aligned} E[V_i] &= 1 - \frac{2e_i}{d} \\ E[U_i] &= \frac{2e_i}{d} \end{aligned}\right\} \Rightarrow E[U_i + 2V_i]$$

$$= 2 - \frac{2e_i}{d}$$

$$\leq \frac{2\tilde{e}_i}{d}$$

$$\Rightarrow \quad E\left[\#\text{erasures} + 2\cdot\#\text{errors}\right]$$

$$= \frac{2\,\tilde{e}_{total}}{d}$$

$\Rightarrow$ Can decode if $\dfrac{2\tilde{e}_{total}}{d} < D$

$$\iff \quad \tilde{e}_{total} < \frac{D\cdot d}{2} \qquad \boxtimes$$