Today: Decoding Concatenated Codes

- Simple Decoding
- Achieving Shannon Capacity on BSc.
- Decoding up to 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

\[
\begin{array}{cccccc}
m_1 & m_2 & m_3 & \cdots & m_K \\
\end{array}
\]

\[
\begin{array}{ccccccc}
x_1 & x_2 & x_3 & x_4 & \cdots & x_N \\
\end{array}
\]

\[
\begin{array}{ccccccc}
y_{11} & \cdots & y_{1n} & y_{21} & \cdots & y_{2n} & \cdots & \cdots & y_{N1} & \cdots & y_{Nn} \\
\end{array}
\]

Channel

\[
\begin{array}{ccccccc}
y_{11} & \cdots & y_{1n} & y_{21} & \cdots & y_{2n} & \cdots & \cdots & y_{N1} & \cdots & y_{Nn} \\
\end{array}
\]

Decoding Problem: Compute \( m_1 \ldots m_K \) given \( y_{11} \ldots y_{m} \ldots y_{N} \ldots y_{nn} \)
Simple Decoding

\[ y_1 \ldots y_{in} \quad Y_1 \ldots Y_{2n} \quad \cdots \quad Y_{n-1} \ldots Y_{an} \]

\[ Z_1 \quad Z_2 \quad \cdots \quad Z_N \]

\[ \tilde{m}_1 \quad \tilde{m}_2 \quad \cdots \quad \tilde{m}_K \]

\[ Z_i = \arg\min_{z} \left\{ \Delta( E_{inner}(z), (y_i \ldots y_{in})) \right\} \]

minimize distance to \[ y_i \ldots y_{in} \]
Claim 1: if \( \# \) errors in block \( i < d/2 \),
then \( y_i = z_i \).

Claim 2: if \( \# \{ \text{block } i \text{ s.t. } y_i = z_i \} < D/2 \),
then \( (m, \ldots, m_k) = (\tilde{m}, \ldots, \tilde{m}_k) \).

Claim 3: if total \( \# \) errors < \( D/2 \cdot d/2 \) then
\( \# \{ \text{blocks with } \geq d/2 \text{ errors} \} < D/2 \).

Proof: Else \( \# \) errors < \( d/2 \cdot D/2 \).

Theorem 1: Simple Decoder Corrects \( \frac{d}{2} \cdot \frac{D}{2} \) errors.
(Implied from Claims 1, 2, 3)

Note:
- Not best possible since one should be able to correct \( \frac{D \cdot d}{2} \) (as opposed to \( \frac{D^2}{4} \)) errors.
- Still sufficient to get Shannon Capacity on Bsc.
Recall $\text{BSC}(p)$

\[
\begin{array}{c}
0 \\ 1
\end{array} \xrightarrow{1-p} \begin{array}{c}
0 \\ 1
\end{array} \quad \text{Bits flipped independently}
\]

Shannon Coding/Decoding

- Can pick code at random; decode in $O(x(n))$ time; get error $2^{-en}$; with $R = 1 - H(p) - \delta$

- Can easily get polytime alg. with error $1/poly(n)$; & $R = 1 - H(p) - \delta$
  - Break message into $clogn$ bit blocks
  & apply Shannon code separately to each.
\[ \Pr \left[ \text{block decoded in correctly} \right] \leq \frac{1}{\text{poly}(n)} \]

\[ \Pr \left[ \exists \ i \ s.t. \right] \leq \frac{n}{\text{poly}(n)} \]

Decoding time = \( n \cdot \exp(c \cdot \log n) \) = \( \text{poly}(n) \).

**So main question:** Can we reduce error to \( \exp(-n) \) with \( \text{poly}(n) \) running time.

**Good News:** Can count on even distribution of error.
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 \(1 - H(p) - 2\epsilon\)
- \(\Pr[i^{th}\text{ block decoded incorrectly}]\)
  \[\leq \exp(-n) \quad [\text{Shannon}]\]
- \(\Pr[\text{more than } \frac{\epsilon N}{2} \text{ blocks decoded incorrectly}] \leq 2^N \cdot \left(\exp(-n)\right)^{\frac{\epsilon N}{2}} = \exp(-nN)\)
- Decoding runs in time \(\text{poly}(N) \cdot \exp(n)\)

Theorem 2 [Forney]: Can get arbitrarily close to capacity (of any) channel with poly time encoding + decoding, \& \(\exp(-\text{length})\) error.
Decoding Move 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 $e_i = \Delta(E(Z_i), Y_i) = \# \text{ apparent errors in } i^{th} \text{ block}$
- 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 $d$ errors if $t$ 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 $\hat{e}_i =$ actual # errors in $i^{th}$ block.

If $Y_i = Z_i \Rightarrow e_i = \hat{e}_i$

$Y_i \neq Z_i \Rightarrow \hat{e}_i > d - e_i$

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

$V_i = 1$ if $i^{th}$ block not erased

$\Rightarrow Y_i \neq Z_i$
Claim: \[ E[U_i + 2v_i] \leq \frac{2\tilde{e}_i}{d} \]

Proof:

Case 1: \[ Y_i = Z_i \]
\[ E[v_i] = 0 \]
\[ E[U_i] = \frac{2e_i}{d} = \frac{2\tilde{e}_i}{d} \]

Case 2: \[ Y_i \neq Z_i \]
\[ E[v_i] = 1 - \frac{2e_i}{d} \]
\[ E[U_i] = \frac{2e_i}{d} \]
\[ E[U_i + 2v_i] \leq 2 - \frac{2e_i}{d} \leq \frac{2\tilde{e}_i}{d} \]
\[ \Rightarrow E[\#\text{errors} + 2 \cdot \#\text{errors}] = 2 \frac{\bar{e}_{\text{total}}}{d} \]

\[ \Rightarrow \text{Can decide if } 2\bar{e}_{\text{total}} < D \frac{d}{d} \]

\[ \Leftrightarrow \bar{e}_{\text{total}} < \frac{D \cdot d}{2} \]