

# ECEN 655: Advanced Channel Coding

## Maximum-Likelihood Performance of Linear Block Codes

Henry D. Pfister

Department of Electrical and Computer Engineering  
Texas A&M University

# Outline

- 1 General Codes
  - Optimal Decoding Rules
  - The Bhattacharyya Union Bound
  
- 2 Linear Codes
  - Simplifications Due to Symmetry
  - Random Codes and Improved Bounds

# Codes and Decoding Rules (1)

## ■ Setup

- Let  $\mathcal{X}$  be an arbitrary alphabet and  $\mathcal{C} \subset \mathcal{X}^n$  be a length- $n$  code
- Consider a **discrete memoryless channel (DMC)** defined by

$$W(y|x) \triangleq \Pr(Y = y \mid X = x)$$

- The codeword  $x_1^n \in \mathcal{C}$  is transmitted with prob.  $p(x_1^n)$  and

$$\Pr(Y_1^n = y_1^n \mid X_1^n = x_1^n) \triangleq W(y_1^n | x_1^n) = \prod_{i=1}^n W(y_i | x_i)$$

- The **maximum likelihood (ML)** decoding rule is defined by

$$\hat{x}^{ML}(y_1^n) = \arg \max_{x_1^n \in \mathcal{C}} W(y_1^n | x_1^n)$$

## Codes and Decoding Rules (2)

- Error rate is minimized by MAP (or maximum a posteriori) decoding
  - Block-MAP decoding returns the cw  $x_1^n \in \mathcal{C}$  that maximizes

$$\Pr(X_1^n = x_1^n | Y_1^n = y_1^n) = \frac{p(x_1^n) W(y_1^n | x_1^n)}{\sum_{\tilde{x}_1^n \in \mathcal{C}} p(\tilde{x}_1^n) W(y_1^n | \tilde{x}_1^n)}$$

- Since the denominator only depends on  $y_1^n$ , we find that

$$\hat{x}^{MAP}(y_1^n) \triangleq \arg \max_{x_1^n \in \mathcal{C}} p(x_1^n) W(y_1^n | x_1^n)$$

# Codes and Decoding Rules (2)

- Error rate is minimized by **MAP (or maximum a posteriori)** decoding
  - Block-MAP decoding returns the cw  $x_1^n \in \mathcal{C}$  that maximizes

$$\Pr(X_1^n = x_1^n | Y_1^n = y_1^n) = \frac{p(x_1^n) W(y_1^n | x_1^n)}{\sum_{\tilde{x}_1^n \in \mathcal{C}} p(\tilde{x}_1^n) W(y_1^n | \tilde{x}_1^n)}$$

- Since the denominator only depends on  $y_1^n$ , we find that

$$\hat{x}^{MAP}(y_1^n) \triangleq \arg \max_{x_1^n \in \mathcal{C}} p(x_1^n) W(y_1^n | x_1^n)$$

- Bit-MAP decoding picks  $x$ , to maximize  $\Pr(X_i = x | Y_1^n = y_1^n)$  and

$$\hat{x}_i^{MAP} \triangleq \arg \max_{x \in \mathcal{X}} \underbrace{\Pr(X_i = x | Y_1^n = y_1^n)}_{\sum_{x_1^n \in \mathcal{C}, x_i = x} \Pr(X_1^n = x_1^n | Y_1^n = y_1^n)}$$

- the sum **marginalizes out all variables except  $x_i$**

# Decoding Performance

- The block error rate of block-MAP decoding is given by

$$\begin{aligned} P_B &= \sum_{x_1^n \in \mathcal{C}} p(x_1^n) \Pr \left( \left\{ \bigcup_{z_1^n \in \mathcal{C} \setminus x_1^n} \{ \hat{x}^{MAP}(Y_1^n) = z_1^n \} \right\} \mid x_1^n \text{ sent} \right) \\ &\leq \sum_{x_1^n \in \mathcal{C}} p(x_1^n) \sum_{z_1^n \in \mathcal{C} \setminus x_1^n} \Pr \left( \hat{x}^{MAP}(Y_1^n) = z_1^n \mid x_1^n \text{ sent} \right) \end{aligned}$$

# Decoding Performance

- The block error rate of block-MAP decoding is given by

$$\begin{aligned} P_B &= \sum_{x_1^n \in \mathcal{C}} p(x_1^n) \Pr \left( \left\{ \bigcup_{z_1^n \in \mathcal{C} \setminus x_1^n} \{ \hat{x}^{MAP}(Y_1^n) = z_1^n \} \right\} \mid x_1^n \text{ sent} \right) \\ &\leq \sum_{x_1^n \in \mathcal{C}} p(x_1^n) \sum_{z_1^n \in \mathcal{C} \setminus x_1^n} \Pr \left( \hat{x}^{MAP}(Y_1^n) = z_1^n \mid x_1^n \text{ sent} \right) \end{aligned}$$

- If  $p(x_1^n) = 1/|\mathcal{C}|$ , then this simplifies to

$$P_B \leq \frac{1}{|\mathcal{C}|} \sum_{x_1^n \in \mathcal{C}} \sum_{z_1^n \in \mathcal{C} \setminus x_1^n} P(x_1^n \rightarrow z_1^n)$$

- $P(x_1^n \rightarrow z_1^n)$  is the **pairwise error probability** between  $x_1^n$  and  $z_1^n$ :

$$P(x_1^n \rightarrow z_1^n) = \sum_{y_1^n \in \mathcal{Y}^n} W(y_1^n | x_1^n) I(W(y_1^n | x_1^n) \leq W(y_1^n | z_1^n)),$$

where the  $I$  function is 1 if its argument is true and 0 otherwise

# The Bhattacharyya Bound (1)

- For any  $s \in [0, 1]$ , we have the bound

$$I(W(y_1^n|x_1^n) \leq W(y_1^n|z_1^n)) \leq \left( \frac{W(y_1^n|z_1^n)}{W(y_1^n|x_1^n)} \right)^s$$

- because LHS= 0 if the RHS < 1 and the LHS= 1 if RHS > 1

# The Bhattacharyya Bound (1)

- For any  $s \in [0, 1]$ , we have the bound

$$I(W(y_1^n|x_1^n) \leq W(y_1^n|z_1^n)) \leq \left( \frac{W(y_1^n|z_1^n)}{W(y_1^n|x_1^n)} \right)^s$$

- because LHS= 0 if the RHS < 1 and the LHS= 1 if RHS > 1
- For BMS channels,  $s = 1/2$  gives the best bound and

$$\begin{aligned} P(x_1^n \rightarrow z_1^n) &= \sum_{y_1^n \in \mathcal{Y}^n} W(y_1^n|x_1^n) \left( \frac{W(y_1^n|z_1^n)}{W(y_1^n|x_1^n)} \right)^{1/2} \\ &= \prod_{i=1}^n \sum_{y_i \in \mathcal{Y}} \sqrt{W(y_i|x_i) W(y_i|z_i)} \end{aligned}$$

---


$$\sum_{y_i \in \mathcal{Y}} \sqrt{W(y_i|x_i) W(y_i|z_i)} = \begin{cases} \sum_{y \in \mathcal{Y}} \sqrt{W(y|x_i) W(y|x_i)} = 1 & \text{if } x_i = y_i \\ \sum_{y \in \mathcal{Y}} \sqrt{W(y|0) W(y|1)} \triangleq \gamma & \text{if } x_i \neq y_i \end{cases}$$

## The Bhattacharyya Bound (2)

- Since  $x_i \neq z_i$  gives a factor of  $\gamma$  and  $x_i = z_i$  gives a 1, we find that

$$P(x_1^n \rightarrow z_1^n) = \prod_{i=1}^{d_H(x_1^n, z_1^n)} \overbrace{\sum_{y \in \mathcal{Y}} \sqrt{W(y|0) W(y|1)}}^{\gamma} = \gamma^{d_H(x_1^n, z_1^n)},$$

where  $\gamma$  is the **Bhattacharyya constant** of the channel

## The Bhattacharyya Bound (2)

- Since  $x_i \neq z_i$  gives a factor of  $\gamma$  and  $x_i = z_i$  gives a 1, we find that

$$P(x_1^n \rightarrow z_1^n) = \prod_{i=1}^{d_H(x_1^n, z_1^n)} \overbrace{\sum_{y \in \mathcal{Y}} \sqrt{W(y|0)W(y|1)}}^{\gamma} = \gamma^{d_H(x_1^n, z_1^n)},$$

where  $\gamma$  is the **Bhattacharyya constant** of the channel

- For the BSC( $p$ ) channel, it is easy to compute  $\gamma_{BSC} = 2\sqrt{p(1-p)}$
  - For the BEC( $\epsilon$ ) channel, it is easy to compute  $\gamma_{BEC} = \epsilon$
  - For BPSK in AWGN,  $\gamma_{AWGN} = e^{-E_s/N_0}$  for SNR  $E_s/N_0$
  - Note:  $\gamma$  is the best possible constant for a bound of the form  $\gamma^{d_H}$
- Applying this to the union bound gives

$$P_B \leq \frac{1}{|\mathcal{C}|} \sum_{x_1^n \in \mathcal{C}} \sum_{z_1^n \in \mathcal{C} \setminus x_1^n} \gamma^{d_H(x_1^n, z_1^n)}.$$

# Block Error Rate of Linear Codes

- Assume the pairwise error probability satisfies, for some  $f$ ,

$$P(x_1^n \rightarrow z_1^n) \leq f(d_H(x_1^n, z_1^n))$$

- If the code is linear, then  $P_B$  is upper bounded by

$$\begin{aligned} P_B &\leq \sum_{x_1^n \in \mathcal{C}} \frac{1}{|\mathcal{C}|} \sum_{z_1^n \in \mathcal{C}, z_1^n \neq x_1^n} f(d_H(x_1^n, z_1^n)) \\ &= \sum_{x_1^n \in \mathcal{C}} \frac{1}{|\mathcal{C}|} \sum_{z_1^n \in \mathcal{C}, z_1^n \neq \mathbf{0}} f(d_H(\mathbf{0}, z_1^n)) \\ &= \sum_{z_1^n \in \mathcal{C}, z_1^n \neq \mathbf{0}} f(w_H(z_1^n)) = -f(0) + \sum_{h=0}^n A_h f(h), \end{aligned}$$

where  $A_h = |\{x_1^n \in \mathcal{C} \mid w_H(x_1^n) = h\}|$  is the **weight enumerator** of  $\mathcal{C}$

# Example: The Hamming Code

- The **weight enumerator function** is given by

$$A(H) \triangleq \sum_{h=0}^n A_h H^h$$

- Combined with the Bhattacharyya bound, we find

$$P_B \leq -1 + \sum_{h=0}^n A_h \gamma^h = -1 + A(\gamma)$$

- The (7,4) binary Hamming code has  $A(H) = 1 + 7H^3 + 7H^4 + H^7$  and, for BPSK in AWGN, we find

$$P_B \leq 7e^{-3E_s/N_0} + 7e^{-4E_s/N_0} + e^{-7E_s/N_0}.$$

# Example: The Random Generator Matrix Ensemble (1)

- $G$  is a random  $k \times n$  matrix with i.i.d. equiprobable binary entries
  - $\mathcal{C}$  is the set of vectors formed by encoding all  $2^k$  message vectors
  - $A_h$  is a random variable and we consider its average  $\bar{A}_h = \mathbb{E}[A_h]$
- Let  $u(i)$  be the  $k$ -bit binary expansion of  $i$  and write

$$\begin{aligned}\bar{A}_h &= \mathbb{E} \left[ \sum_{i=0}^{2^k-1} I(w_H(u(i)G) = h) \right] \\ &= \sum_{i=0}^{2^k-1} \mathbb{E} [I(w_H(u(i)G) = h)] \\ &= \sum_{i=0}^{2^k-1} \Pr(w_H(u(i)G) = h) \\ &= \begin{cases} 1 + \frac{2^k-1}{2^n} & \text{if } h = 0 \\ \frac{(2^k-1)\binom{n}{h}}{2^n} & \text{otherwise} \end{cases}\end{aligned}$$

## Example: The Random Generator Matrix Ensemble (2)

- Computing the Bhattacharyya union bound gives

$$\begin{aligned} P_B &\leq -1 + \sum_{h=0}^n \bar{A}_h \gamma^h \leq \frac{2^k - 1}{2^n} \sum_{h=0}^n \binom{n}{h} \gamma^h \\ &= \frac{2^k - 1}{2^n} (1 + \gamma)^n \leq \frac{2^{Rn}}{2^n} (1 + \gamma)^n \\ &= (2^{R-1} (1 + \gamma))^n \end{aligned}$$

- This vanishes iff  $R < R_u = 1 - \log_2(1 + \gamma)$

# Example: The Random Generator Matrix Ensemble (2)

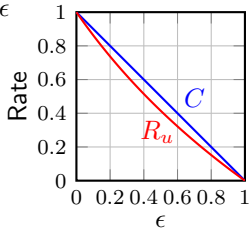
- Computing the Bhattacharyya union bound gives

$$\begin{aligned}
 P_B &\leq -1 + \sum_{h=0}^n \bar{A}_h \gamma^h \leq \frac{2^k - 1}{2^n} \sum_{h=0}^n \binom{n}{h} \gamma^h \\
 &= \frac{2^k - 1}{2^n} (1 + \gamma)^n \leq \frac{2^{Rn}}{2^n} (1 + \gamma)^n \\
 &= (2^{R-1} (1 + \gamma))^n
 \end{aligned}$$

- This vanishes iff  $R < R_u = 1 - \log_2(1 + \gamma)$
- For the BEC( $\epsilon$ ), we can compare with  $C = 1 - \epsilon$

$$\begin{aligned}
 R_u &= 1 - \log_2(1 + \gamma_{BEC}) \\
 &= 1 - \frac{1}{\ln 2} \ln(1 + \epsilon)
 \end{aligned}$$

- Code achieves capacity but bound too weak!



# Improving the Bound (1)

- Joint Typicality (JT) Decoder:
  - If there is exactly one  $x_1^n \in \mathcal{C}$  jointly typical with  $y_1^n$ , then return it
  - Otherwise, declare failure
- What does it mean to be jointly typical?
  - For the BEC, the received must have  $\approx \epsilon n$  erasures and the two sequences must match on all non-erased positions

# Improving the Bound (1)

- Joint Typicality (JT) Decoder:
  - If there is exactly one  $x_1^n \in \mathcal{C}$  jointly typical with  $y_1^n$ , then return it
  - Otherwise, declare failure
- What does it mean to be jointly typical?
  - For the BEC, the received must have  $\approx \epsilon n$  erasures and the two sequences must match on all non-erased positions
- Consider  $x_1^n, z_1^n \in \mathcal{C}$  with  $d_H(x_1^n, z_1^n) = h$ 
  - Assume  $Y_1^n$  is  $x_1^n$  altered by random pattern of exactly  $\epsilon n$  erasures
  - How many erasure patterns? How many make  $z_1^n$  JT with  $Y_1^n$ ?
    - total number of ways to choose erasures is  $\binom{n}{\epsilon n}$
    - number of ways to choose erasures for JT is  $\binom{n-h}{\epsilon n-h}$

## Improving the Bound (2)

- Hence, the pairwise error probability for the JT decoder is

$$\begin{aligned}\Pr(Y_1^N \text{ JT } z_1^n) &= \binom{n-h}{\epsilon n-h} / \binom{n}{\epsilon n} \\ &= \frac{(n-h)!}{(\epsilon n-h)!(n-\epsilon n)!} \cdot \frac{(\epsilon n)!(n-\epsilon n)!}{n!} \\ &= \frac{(n-h)!}{(\epsilon n-h)!} \cdot \frac{(\epsilon n)!}{n!} \cdot \frac{h!}{h!} \\ &= \binom{\epsilon n}{h} / \binom{n}{h}\end{aligned}$$

# Improving the Bound (2)

- Hence, the pairwise error probability for the JT decoder is

$$\begin{aligned}\Pr(Y_1^N \text{ JT } z_1^n) &= \binom{n-h}{\epsilon n-h} / \binom{n}{\epsilon n} \\ &= \frac{(n-h)!}{(\epsilon n-h)!(n-\epsilon n)!} \cdot \frac{(\epsilon n)!(n-\epsilon n)!}{n!} \\ &= \frac{(n-h)!}{(\epsilon n-h)!} \cdot \frac{(\epsilon n)!}{n!} \cdot \frac{h!}{h!} \\ &= \binom{\epsilon n}{h} / \binom{n}{h}\end{aligned}$$

- Plugging into the union bound gives

$$\begin{aligned}P_B &\leq -1 + \sum_{h=0}^n \bar{A}_h \left[ \binom{\epsilon n}{h} / \binom{n}{h} \right] \\ &= \sum_{h=0}^n \left[ 2^{-n} (2^k - 1) \binom{n}{h} \right] \left[ \binom{\epsilon n}{h} / \binom{n}{h} \right] \\ &\leq 2^{n(R-1)} \sum_{h=0}^n \binom{\epsilon n}{h} \\ &= 2^{n(R-1+\epsilon)} \rightarrow 0 \quad \text{if } R < 1 - \epsilon\end{aligned}$$