An introduction to coding theory

Adrish Banerjee

Department of Electrical Engineering
Indian Institute of Technology Kanpur
Kanpur, Uttar Pradesh
India

Mar. 6, 2017

Lecture #16B: Problem solving session-VI

Fundamental limit

- **Problem # 1:** For reliable communication in presence of Gaussian noise, what is the minimum signal-to-noise E_b/N_0 required?

Fundamental limit

- **Problem # 1:** For reliable communication in presence of Gaussian noise, what is the minimum signal-to-noise E_b/N_0 required?
- **Solution:** Capacity of Gaussian memoryless channel with two-sided noise power spectral density $N_0/2$ and without bandwidth limitation is given by

$$\begin{aligned} C^{\infty} &= \lim_{W\to\infty} W \log\left(1+\frac{S}{N_0 W}\right) \\ &= \frac{S}{N_0 \ln 2} \text{ bits/s} \end{aligned}$$

where W denotes the bandwidth and S is the signaling power.

Fundamental limit

- **Problem # 1:** For reliable communication in presence of Gaussian noise, what is the minimum signal-to-noise E_b/N_0 required?
- **Solution:** Capacity of Gaussian memoryless channel with two-sided noise power spectral density $N_0/2$ and without bandwidth limitation is given by

$$\begin{aligned} C^{\infty} &= \lim_{W \to \infty} W \log \left(1 + \frac{S}{N_0 W}\right) \\ &= \frac{S}{N_0 \ln 2} \text{ bits/s} \end{aligned}$$

  where W denotes the bandwidth and S is the signaling power.
- If we transmit K information bits over τ seconds, where τ is a multiple of T, we have

$$E_b = \frac{S\tau}{K}$$

Fundamental limit

- Since the data transmission rate $R_t = K/\tau$ bits/s, energy per bit can be written as

$$E_b = \frac{S}{R_t}$$

Fundamental limit

- Since the data transmission rate $R_t = K/\tau$ bits/s, energy per bit can be written as
$$E_b = \frac{S}{R_t}$$
- Thus we have
$$\frac{C^\infty}{R_t} = \frac{E_b}{N_0 \ln 2}$$

Fundamental limit

- Since the data transmission rate $R_t = K/\tau$ bits/s, energy per bit can be written as
$$E_b = \frac{S}{R_t}$$
- Thus we have
$$\frac{C^\infty}{R_t} = \frac{E_b}{N_0 \ln 2}$$
- For reliable communication, we must have $R_t < C^\infty$. Thus we have
$$\frac{E_b}{N_0} > \ln 2 = 0.69 = -1.6 \text{ dB}$$

Fundamental limit

- Since the data transmission rate $R_t = K/\tau$ bits/s, energy per bit can be written as
$$E_b = \frac{S}{R_t}$$
- Thus we have
$$\frac{C^\infty}{R_t} = \frac{E_b}{N_0 \ln 2}$$
- For reliable communication, we must have $R_t < C^\infty$. Thus we have
$$\frac{E_b}{N_0} > \ln 2 = 0.69 = -1.6 \text{ dB}$$
- Thus signal to noise ratio E_b/N_0 cannot be less than Shannon limit -1.6 dB for reliable communications.

Coding Limits

- **Problem # 2:** For reliable communication in presence of Gaussian noise, what is the minimum signal-to-noise E_b/N_0 required if we are using a rate R=K/N code?

Coding Limits

- **Problem # 2:** For reliable communication in presence of Gaussian noise, what is the minimum signal-to-noise E_b/N_0 required if we are using a rate R=K/N code?
- **Solutions:** Capacity of bandlimited Gaussian channel is given by

$$C^W = W \log\left(1 + \frac{S}{N_0 W}\right) \text{ bits/s}$$

where W denotes the bandwidth and S is the signaling power.

Coding Limits

- **Problem # 2:** For reliable communication in presence of Gaussian noise, what is the minimum signal-to-noise E_b/N_0 required if we are using a rate R=K/N code?
- **Solutions:** Capacity of bandlimited Gaussian channel is given by

$$C^W = W \log\left(1 + \frac{S}{N_0 W}\right) \text{ bits/s}$$

where W denotes the bandwidth and S is the signaling power.

- Assuming we are transmitting at a rate of 2W samples per second and using a rate R=K/N block code. If we transmit K information bits during τ seconds, we have

$$N = 2W\tau \text{ samples per codeword}$$

Coding Limits

- **Problem # 2:** For reliable communication in presence of Gaussian noise, what is the minimum signal-to-noise E_b/N_0 required if we are using a rate R=K/N code?
- **Solutions:** Capacity of bandlimited Gaussian channel is given by

$$C^W = W \log\left(1 + \frac{S}{N_0 W}\right) \text{ bits/s}$$

  where W denotes the bandwidth and S is the signaling power.
- Assuming we are transmitting at a rate of 2W samples per second and using a rate R=K/N block code. If we transmit K information bits during τ seconds, we have

$$N = 2W\tau \text{ samples per codeword}$$

- Hence

$$R_t = K/\tau = 2WK/N = 2WR \text{ bits/s}$$

Coding Limits

- Since, $E_b = S/R_t$, we have

$$\frac{S}{WN_0} = 2RE_b/N_0$$

Coding Limits

- Since, $E_b = S/R_t$, we have

$$\frac{S}{WN_0} = 2RE_b/N_0$$

- For reliable communications, we must have $R_t < C^W$, thus

$$R_t = 2WR < W \log\left(1 + \frac{2RE_b}{N_0}\right)$$

Coding Limits

- Since, $E_b = S/R_t$, we have

$$\frac{S}{WN_0} = 2RE_b/N_0$$

- For reliable communications, we must have $R_t < C^W$, thus

$$R_t = 2WR < W \log\left(1 + \frac{2RE_b}{N_0}\right)$$

- We can write equivalently

$$E_b/N_0 > \frac{2^{2R} - 1}{2R}$$

Coding Limits

- Since, $E_b = S/R_t$, we have

$$\frac{S}{WN_0} = 2RE_b/N_0$$

- For reliable communications, we must have $R_t < C^W$, thus

$$R_t = 2WR < W \log\left(1 + \frac{2RE_b}{N_0}\right)$$

- We can write equivalently

$$E_b/N_0 > \frac{2^{2R} - 1}{2R}$$

- Since RHS is an increasing function of R, in order to communicate close to Shannon limit, we have to use both an information rate R_t and code rate R close to zero.

Coding Limits

- Since, $E_b = S/R_t$, we have

$$\frac{S}{WN_0} = 2RE_b/N_0$$

- For reliable communications, we must have $R_t < C^W$, thus

$$R_t = 2WR < W \log\left(1 + \frac{2RE_b}{N_0}\right)$$

- We can write equivalently

$$E_b/N_0 > \frac{2^{2R} - 1}{2R}$$

- Since RHS is an increasing function of R, in order to communicate close to Shannon limit, we have to use both an information rate R_t and code rate R close to zero.
- If we let $R \to 0$, we get $E_b/N_0 > \ln 2$.

Coding Limits

- Since, $E_b = S/R_t$, we have
$$\frac{S}{WN_0} = 2RE_b/N_0$$
- For reliable communications, we must have $R_t < C^W$, thus
$$R_t = 2WR < W \log\left(1 + \frac{2RE_b}{N_0}\right)$$
- We can write equivalently
$$E_b/N_0 > \frac{2^{2R} - 1}{2R}$$
- Since RHS is an increasing function of R, in order to communicate close to Shannon limit, we have to use both an information rate R_t and code rate R close to zero.
- If we let $R \to 0$, we get $E_b/N_0 > \ln 2$.
- If we let $R = 1/2$, we get $E_b/N_0 > 1 = 0$ dB.

Convolutional codes

- **Problem # 3:** Prove that every convolutional code C has a generator matrix that is delayfree.

Convolutional codes

- **Problem # 3:** Prove that every convolutional code C has a generator matrix that is delayfree.
- **Solution:** Let $G(D)$ be any generator matrix for C. The nonzero entries of G(D) can be written as

$$g_{ij}(D) = D^{s_{ij}} f_{ij}(D)/q_{ij}(D)$$

where s_{ij} is an integer such that
$f_{ij}(0) = q_{ij}(0) = 1, 1 \leq i \leq k, 1 \leq j \leq n$.

Convolutional codes

- **Problem # 3:** Prove that every convolutional code C has a generator matrix that is delayfree.
- **Solution:** Let $G(D)$ be any generator matrix for C. The nonzero entries of G(D) can be written as

$$g_{ij}(D) = D^{s_{ij}} f_{ij}(D)/q_{ij}(D)$$

where s_{ij} is an integer such that
$f_{ij}(0) = q_{ij}(0) = 1, 1 \leq i \leq k, 1 \leq j \leq n$.
- The number s_{ij} is the delay of the sequence

$$g_{ij}(D) = D^{s_{ij}} f_{ij}(D)/q_{ij}(D) = D^{s_{ij}} + g_{s_{ij}+1} D^{s_{ij}+1} + \cdots$$

Convolutional codes

- **Problem # 3:** Prove that every convolutional code C has a generator matrix that is delayfree.
- **Solution:** Let $G(D)$ be any generator matrix for C. The nonzero entries of G(D) can be written as

$$g_{ij}(D) = D^{s_{ij}} f_{ij}(D)/q_{ij}(D)$$

where s_{ij} is an integer such that
$f_{ij}(0) = q_{ij}(0) = 1, 1 \leq i \leq k, 1 \leq j \leq n$.

- The number s_{ij} is the delay of the sequence

$$g_{ij}(D) = D^{s_{ij}} f_{ij}(D)/q_{ij}(D) = D^{s_{ij}} + g_{s_{ij}+1} D^{s_{ij}+1} + \cdots$$

- Let $s = \min_{i,j}\{s_{ij}\}$, then

$$G'(D) = D^{-s} G(D)$$

is both delayfree and realizable and both G(D) and G'(D) generate the same convolutional code.

Convolutional codes

- **Problem # 4:** Prove that every convolutional code C has a polynomial delayfree generator matrix.

Convolutional codes

- **Problem # 4:** Prove that every convolutional code C has a polynomial delayfree generator matrix.
- **Solutions:** Let G(D) be any realizable and delayfree generator for C and let q(D) be the least common multiple of all the denominators of the nonzero entries of G(D).

Convolutional codes

- **Problem # 4:** Prove that every convolutional code C has a polynomial delayfree generator matrix.
- **Solutions:** Let G(D) be any realizable and delayfree generator for C and let q(D) be the least common multiple of all the denominators of the nonzero entries of G(D).
- Since q(D) is a delayfree polynomial, we have

$$G'(D) = q(D)G(D)$$

is a polynomial delayfree generator matrix for C.

Convolutional codes

- **Problem # 5:** The dual code $C^{\perp}$ to a convolutional code C is the set of all n-tuples of sequences $\mathbf{v}^{\perp}$ such that the inner product

$$(\mathbf{v}, \mathbf{v}^{\perp}) = \mathbf{v}(\mathbf{v}^{\perp})^{T}$$

is zero.

Convolutional codes

- **Problem # 5:** The dual code $C^{\perp}$ to a convolutional code C is the set of all n-tuples of sequences $\mathbf{v}^{\perp}$ such that the inner product

$$(\mathbf{v}, \mathbf{v}^{\perp}) = \mathbf{v}(\mathbf{v}^{\perp})^{T}$$

is zero.

- Let rate k/n convolutional code be generated by the semi-infinite generator matrix $\mathbf{G}$ and the rate $R = (n-k)/n$ dual code $C^{\perp}$ be generated by the semi-infinite generator matrix $\mathbf{G}^{\perp}$, where

$$\mathbf{G}^{\perp} = \begin{pmatrix} G_0^{\perp} & G_1^{\perp} & \cdots & G_m^{\perp} & & \\ & G_0^{\perp} & G_1^{\perp} & \cdots & G_m^{\perp} & \\ & & \ddots & \ddots & & \ddots \end{pmatrix}$$

Then

$$\mathbf{G}(\mathbf{G}^{\perp}) = \mathbf{0}$$

Convolutional codes

- Let $\mathbf{v} = \mathbf{uG}$ and $\mathbf{v}^{\perp} = \mathbf{u}^{\perp}\mathbf{G}^{\perp}$, where $\mathbf{v}$ and $\mathbf{v}^{\perp}$ are orthogonal. Then we have

$$\mathbf{v}(\mathbf{v}^{\perp})^{\mathbf{T}} = \mathbf{uG}(\mathbf{u}^{\perp}\mathbf{G}^{\perp})^{\mathbf{T}} = \mathbf{uG}(\mathbf{G}^{\perp})^{\mathbf{T}}(\mathbf{u}^{\perp})^{\mathbf{T}} = \mathbf{0}$$

Convolutional codes

- Let $\mathbf{v} = \mathbf{uG}$ and $\mathbf{v}^{\perp} = \mathbf{u}^{\perp}\mathbf{G}^{\perp}$, where $\mathbf{v}$ and $\mathbf{v}^{\perp}$ are orthogonal. Then we have

$$\mathbf{v}(\mathbf{v}^{\perp})^{\mathbf{T}} = \mathbf{uG}(\mathbf{u}^{\perp}\mathbf{G}^{\perp})^{\mathbf{T}} = \mathbf{uG}(\mathbf{G}^{\perp})^{\mathbf{T}}(\mathbf{u}^{\perp})^{\mathbf{T}} = \mathbf{0}$$

- Thus we have

$$\mathbf{G}(\mathbf{G}^{\perp}) = \mathbf{0}$$

Convolutional codes

- Let $\mathbf{v} = \mathbf{uG}$ and $\mathbf{v}^{\perp} = \mathbf{u}^{\perp}\mathbf{G}^{\perp}$, where $\mathbf{v}$ and $\mathbf{v}^{\perp}$ are orthogonal. Then we have

$$\mathbf{v}(\mathbf{v}^{\perp})^{\mathbf{T}} = \mathbf{uG}(\mathbf{u}^{\perp}\mathbf{G}^{\perp})^{\mathbf{T}} = \mathbf{uG}(\mathbf{G}^{\perp})^{\mathbf{T}}(\mathbf{u}^{\perp})^{\mathbf{T}} = \mathbf{0}$$

- Thus we have

$$\mathbf{G}(\mathbf{G}^{\perp}) = \mathbf{0}$$

- The convolutional dual code $C^{\perp}$ to a convolutional code C which is encoded by the rate $R = k/n$ generator matrix $G(D)$ is the set of all codewords encoded by any rate $R = (n-k)/n$ generator matrix $G_{\perp}(D)$ such that

$$\mathbf{G(D)G}_{\perp}^{\mathbf{T}}\mathbf{(D)} = \mathbf{0}$$

Convolutional codes

- **Problem # 6:** The convolutional dual to the code encoded by the generator matrix G(D) is the reversal of the convolutional code dual to the code encoded by G(D).

Convolutional codes

- **Problem # 6:** The convolutional dual to the code encoded by the generator matrix G(D) is the reversal of the convolutional code dual to the code encoded by G(D).
- Let us consider a rate $R = k/n$ convolutional code encoded by the polynomial generator matrix

$$G(D) = G_0 + G_1 D + \cdots + G_m D^m$$

Convolutional codes

- **Problem # 6:** The convolutional dual to the code encoded by the generator matrix G(D) is the reversal of the convolutional code dual to the code encoded by G(D).
- Let us consider a rate $R = k/n$ convolutional code encoded by the polynomial generator matrix

$$G(D) = G_0 + G_1 D + \cdots + G_m D^m$$

- Let $\tilde{G}^{\perp}(D)$ denote the rate R=$(n-k)/n$ polynomial generator matrix

$$\tilde{G}^{\perp}(D) = G_m^{\perp} + G_{m^{\perp}-1} D + \cdots + G_0 D^{m^{\perp}}$$

which is the reciprocal of the generator matrix

$$G^{\perp}(D) = G_0^{\perp} + G_1^{\perp} D + \cdots + G_{m^{\perp}}^{\perp}$$

for the dual code $C^{\perp}$.

Convolutional codes

- Then we have

$$\begin{aligned} G(D)(\tilde{G}(D))^T &= G_0(G_{m^\perp}^\perp)^T + G_0(G_{m^\perp-1}^\perp)^T + G_1(G_{m^\perp}^\perp)D \\ &\quad + \cdots + G_m(G_0^\perp)^T D^{m+m^\perp} \\ &= \left(\sum_{j=-m}^{m^\perp}\left(\sum_{i=0}^{m} G_i(G_{i+j}^\perp)^T\right)\right) D^{m+j} = 0 \end{aligned}$$

Convolutional codes

- **Problem # 7:** Show that the free distance for any binary rate $R = k/n$ convolutional code encoded by a minimal encoding matrix of memory m and overall constraint length ν satisfies

$$d_{\text{free}} \leq \min_{i \geq 1}\left\{\left\lfloor \frac{(m+i)n}{2(1-2^{\nu-k(m+i)})}\right\rfloor\right\}$$

Convolutional codes

- **Problem # 7:** Show that the free distance for any binary rate $R = k/n$ convolutional code encoded by a minimal encoding matrix of memory m and overall constraint length ν satisfies

$$d_{\text{free}} \leq \min_{i \geq 1} \left\{ \left\lfloor \frac{(m+i)n}{2(1-2^{\nu-k(m+i)})} \right\rfloor \right\}$$

- A rate $R = k/n$ convolutional code can be encoded by a minimal encoding matrix whose realization in controller canonical form has 2^{ν} encoder states.

Convolutional codes

- **Problem # 7:** Show that the free distance for any binary rate $R = k/n$ convolutional code encoded by a minimal encoding matrix of memory m and overall constraint length ν satisfies

$$d_{\text{free}} \leq \min_{i \geq 1} \left\{ \left\lfloor \frac{(m+i)n}{2(1-2^{\nu-k(m+i)})} \right\rfloor \right\}$$

- A rate $R = k/n$ convolutional code can be encoded by a minimal encoding matrix whose realization in controller canonical form has 2^{ν} encoder states.
- Consider $2^{k(m+i)}, i = 1, 2, \cdots$ information sequences.

Convolutional codes

- **Problem # 7:** Show that the free distance for any binary rate $R = k/n$ convolutional code encoded by a minimal encoding matrix of memory m and overall constraint length ν satisfies

$$d_{\text{free}} \leq \min_{i \geq 1} \left\{ \left\lfloor \frac{(m+i)n}{2(1-2^{\nu-k(m+i)})} \right\rfloor \right\}$$

- A rate $R = k/n$ convolutional code can be encoded by a minimal encoding matrix whose realization in controller canonical form has 2^{ν} encoder states.
- Consider $2^{k(m+i)}, i = 1, 2, \cdots$ information sequences.
- There exist $2^{k(m+i)}/2^{\nu}$ information sequences starting in the zero state leading to the zero state.

Convolutional codes

- **Problem # 7:** Show that the free distance for any binary rate $R = k/n$ convolutional code encoded by a minimal encoding matrix of memory m and overall constraint length ν satisfies

$$d_{\text{free}} \leq \min_{i \geq 1} \left\{ \left\lfloor \frac{(m+i)n}{2(1-2^{\nu-k(m+i)})} \right\rfloor \right\}$$

- A rate $R = k/n$ convolutional code can be encoded by a minimal encoding matrix whose realization in controller canonical form has 2^{ν} encoder states.
- Consider $2^{k(m+i)}, i = 1, 2, \cdots$ information sequences.
- There exist $2^{k(m+i)}/2^{\nu}$ information sequences starting in the zero state leading to the zero state.
- Corresponding code sequences constitute a block code with $M = 2^{k(m+i)-\nu}$ codewords and blocklength $N = (m+i)n$ for $i = 1, 2, \cdots$.

Convolutional codes

- From Plotkin bound, we have

$$d_{\min} \leq \left\lfloor \frac{NM}{2(M-1)} \right\rfloor$$

Convolutional codes

- From Plotkin bound, we have

$$d_{\min} \leq \left\lfloor \frac{NM}{2(M-1)} \right\rfloor$$

- Putting the value of N and M, we get the desired bound.

Convolutional codes

- **Problem #8:** The free distance for any binary $R = k/n$ convolutional code encoded by minimal encoding matrix of memory m satisfies

$$d_{\text{free}} \leq \min_{i \geq 1} \left\{ \frac{(m+i)n}{2(1-2^{-ki})} \right\}$$

Convolutional codes

- **Problem #8:** The free distance for any binary $R = k/n$ convolutional code encoded by minimal encoding matrix of memory m satisfies

$$d_{\text{free}} \leq \min_{i \geq 1} \left\{ \frac{(m+i)n}{2(1-2^{-ki})} \right\}$$

- Also

$$\lim_{m \to \infty} \frac{d_{free}}{mn} \leq \frac{1}{2}$$

Convolutional codes

- **Problem #8:** The free distance for any binary $R = k/n$ convolutional code encoded by minimal encoding matrix of memory m satisfies
$$d_{\text{free}} \leq \min_{i \geq 1} \left\{ \frac{(m+i)n}{2(1-2^{-ki})} \right\}$$
- Also
$$\lim_{m \to \infty} \frac{d_{free}}{mn} \leq \frac{1}{2}$$
- **Solutions:** Since $\nu \leq km$, the bound follows from the result of the last question.

Convolutional codes

- **Problem #8:** The free distance for any binary $R = k/n$ convolutional code encoded by minimal encoding matrix of memory m satisfies
$$d_{\text{free}} \leq \min_{i \geq 1} \left\{ \frac{(m+i)n}{2(1-2^{-ki})} \right\}$$
- Also
$$\lim_{m \to \infty} \frac{d_{free}}{mn} \leq \frac{1}{2}$$
- **Solutions:** Since $\nu \leq km$, the bound follows from the result of the last question.
- Let $m \to \infty$, and noting that $(1 - 2^{-ki}) < 1$, we get the desired result.