Information and Coding Theory

MA41024/ MA60020/ MA60262

Bibhas Adhikari

Spring 2022-23, IIT Kharagpur

Lecture 11
February 27, 2023

Review

→ Shannon demonstrated that with a proper encoding of the information, the errors induced by a noisy channel or storage medium can be reduced to any desired level as long as the information rate is less than the capacity of the channel

Review

- $\rightarrow$ Shannon demonstrated that with a proper encoding of the information, the errors induced by a noisy channel or storage medium can be reduced to any desired level as long as the information rate is less than the capacity of the channel
- $\rightarrow$ The source encoder transform the source output into a string of bits, called the information sequence
  - $\triangle$ The number of bits per unit time required to represent the source output is minimized
  - $\triangle$ The source output can be perfectly reconstructed from the information sequence $\mathbf{u} = (u_0, u_1, \ldots, u_{k-1})$

Review

→ Shannon demonstrated that with a proper encoding of the information, the errors induced by a noisy channel or storage medium can be reduced to any desired level as long as the information rate is less than the capacity of the channel

→ The source encoder transform the source output into a string of bits, called the information sequence

- △ The number of bits per unit time required to represent the source output is minimized
- △ The source output can be perfectly reconstructed from the information sequence $\mathbf{u} = (u_0, u_1, \ldots, u_{k-1})$

→ The channel encoder transforms the information sequence $\mathbf{u}$ into a string of bits $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ called a *codeword*

Review

→ The modulator transforms each output symbol of the channel encoder into a waveform of duration, say T seconds which is suitable for transmission

  △ This waveform enters the channel and get corrupted by noise

Review

- → The modulator transforms each output symbol of the channel encoder into a waveform of duration, say T seconds which is suitable for transmission
  - △ This waveform enters the channel and get corrupted by noise
  - △ Examples of transmission channels - telephone lines, mobile cellular technology, high-frequency (HF) radio, microwave and satellite links, optical fiber cables

Review

- → The modulator transforms each output symbol of the channel encoder into a waveform of duration, say T seconds which is suitable for transmission
  - △ This waveform enters the channel and get corrupted by noise
  - △ Examples of transmission channels - telephone lines, mobile cellular technology, high-frequency (HF) radio, microwave and satellite links, optical fiber cables
  - △ Examples of storage media - semiconductor memories, magnetic tapes, compact discs

Review

- → The modulator transforms each output symbol of the channel encoder into a waveform of duration, say T seconds which is suitable for transmission
  - △ This waveform enters the channel and get corrupted by noise
  - △ Examples of transmission channels - telephone lines, mobile cellular technology, high-frequency (HF) radio, microwave and satellite links, optical fiber cables
  - △ Examples of storage media - semiconductor memories, magnetic tapes, compact discs
  - △ Examples of noise - On a telephone line, disturbances may come from: switching impulse noise, crosstalk from other lines. On compact discs: dust particles

Review

- → The modulator transforms each output symbol of the channel encoder into a waveform of duration, say T seconds which is suitable for transmission
  - △ This waveform enters the channel and get corrupted by noise
  - △ Examples of transmission channels - telephone lines, mobile cellular technology, high-frequency (HF) radio, microwave and satellite links, optical fiber cables
  - △ Examples of storage media - semiconductor memories, magnetic tapes, compact discs
  - △ Examples of noise - On a telephone line, disturbances may come from: switching impulse noise, crosstalk from other lines. On compact discs: dust particles
- → The demodulator processes each received waveform of duration T and produces either a discrete or continuous output

Review

- → The modulator transforms each output symbol of the channel encoder into a waveform of duration, say T seconds which is suitable for transmission
  - △ This waveform enters the channel and get corrupted by noise
  - △ Examples of transmission channels - telephone lines, mobile cellular technology, high-frequency (HF) radio, microwave and satellite links, optical fiber cables
  - △ Examples of storage media - semiconductor memories, magnetic tapes, compact discs
  - △ Examples of noise - On a telephone line, disturbances may come from: switching impulse noise, crosstalk from other lines. On compact discs: dust particles
- → The demodulator processes each received waveform of duration T and produces either a discrete or continuous output
- → The sequence of demodulator outputs corresponding to the encoded sequence $\mathbf{v}$, called the received sequence $\mathbf{r}$

Review

- → The channel decoder transforms the received sequence $\mathbf{r}$ into a binary sequence $\widehat{\mathbf{u}}$, called the estimated information sequence
  - △ The decoding strategy is based on the rules of channel encoding and the noise characteristics of the channel or the storage medium
  - △ Ideally, $\widehat{\mathbf{u}} = \mathbf{u}$, although noise may cause decoding errors

Review

→ The channel decoder transforms the received sequence $\mathbf{r}$ into a binary sequence $\widehat{\mathbf{u}}$, called the estimated information sequence

- △ The decoding strategy is based on the rules of channel encoding and the noise characteristics of the channel or the storage medium
- △ Ideally, $\widehat{\mathbf{u}} = \mathbf{u}$, although noise may cause decoding errors

The big picture

$$\mathbf{u} \to \mathbf{v} \to \mathbf{r} \to \widehat{\mathbf{u}}$$

Review

$\rightarrow$ The channel decoder transforms the received sequence $\mathbf{r}$ into a binary sequence $\widehat{\mathbf{u}}$, called the estimated information sequence

- $\triangle$ The decoding strategy is based on the rules of channel encoding and the noise characteristics of the channel or the storage medium
- $\triangle$ Ideally, $\widehat{\mathbf{u}} = \mathbf{u}$, although noise may cause decoding errors

The big picture

$$\mathbf{u} \rightarrow \mathbf{v} \rightarrow \mathbf{r} \rightarrow \widehat{\mathbf{u}}$$

Problem Design and implementation of encoder/decoder pair such that - information can be transmitted in noisy environment, and the information can be reliably reproduced at the output of the channel decoder

Codes

Observation

→ The k-tuple $\mathbf{u} = (u_0, u_1, \ldots, u_{k-1})$, called a message (sometimes $\mathbf{u}$ is used to denote a k-bit message rather than the entire information sequence)

Codes

Observation

- $\rightarrow$ The k-tuple $\mathbf{u} = (u_0, u_1, \ldots, u_{k-1})$, called a message (sometimes $\mathbf{u}$ is used to denote a k-bit message rather than the entire information sequence)
- $\rightarrow$ There are 2^k different possible messages

Codes

Observation

- → The k-tuple $\mathbf{u} = (u_0, u_1, \ldots, u_{k-1})$, called a message (sometimes $\mathbf{u}$ is used to denote a k-bit message rather than the entire information sequence)
- → There are 2^k different possible messages
- → The encoder transform each message $\mathbf{u}$ into an n-tuple $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$, called a codeword (sometimes $\mathbf{v}$ is used to denote an n-symbol block rather than the entire encoded sequence)

Codes

Observation

- $\rightarrow$ The k-tuple $\mathbf{u} = (u_0, u_1, \ldots, u_{k-1})$, called a message (sometimes $\mathbf{u}$ is used to denote a k-bit message rather than the entire information sequence)
- $\rightarrow$ There are 2^k different possible messages
- $\rightarrow$ The encoder transform each message $\mathbf{u}$ into an n-tuple $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$, called a codeword (sometimes $\mathbf{v}$ is used to denote an n-symbol block rather than the entire encoded sequence)
- $\rightarrow$ Therefore, corresponding to 2^k different possible messages, there are 2^k different possible codewords at the endoder output

Codes

Observation

- $\rightarrow$ The k-tuple $\mathbf{u} = (u_0, u_1, \ldots, u_{k-1})$, called a message (sometimes $\mathbf{u}$ is used to denote a k-bit message rather than the entire information sequence)
- $\rightarrow$ There are 2^k different possible messages
- $\rightarrow$ The encoder transform each message $\mathbf{u}$ into an n-tuple $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$, called a codeword (sometimes $\mathbf{v}$ is used to denote an n-symbol block rather than the entire encoded sequence)
- $\rightarrow$ Therefore, corresponding to 2^k different possible messages, there are 2^k different possible codewords at the endoder output
- $\rightarrow$ This set of 2^k codewords of length n is called an (n, k) block code

Codes

Observation

- → The k-tuple $\mathbf{u} = (u_0, u_1, \ldots, u_{k-1})$, called a message (sometimes $\mathbf{u}$ is used to denote a k-bit message rather than the entire information sequence)
- → There are 2^k different possible messages
- → The encoder transform each message $\mathbf{u}$ into an n-tuple $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$, called a codeword (sometimes $\mathbf{v}$ is used to denote an n-symbol block rather than the entire encoded sequence)
- → Therefore, corresponding to 2^k different possible messages, there are 2^k different possible codewords at the endoder output
- → This set of 2^k codewords of length n is called an (n, k) block code
- → The ratio $R = k/n$ is called the *code rate*, and it can be interpreted as the number of information bits entering the encoder per transmitted symbol

Codes

Observation

- → The k-tuple $\mathbf{u} = (u_0, u_1, \ldots, u_{k-1})$, called a message (sometimes $\mathbf{u}$ is used to denote a k-bit message rather than the entire information sequence)
- → There are 2^k different possible messages
- → The encoder transform each message $\mathbf{u}$ into an n-tuple $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$, called a codeword (sometimes $\mathbf{v}$ is used to denote an n-symbol block rather than the entire encoded sequence)
- → Therefore, corresponding to 2^k different possible messages, there are 2^k different possible codewords at the endoder output
- → This set of 2^k codewords of length n is called an (n, k) block code
- → The ratio $R = k/n$ is called the *code rate*, and it can be interpreted as the number of information bits entering the encoder per transmitted symbol
- → Each message is encoded independently, so the encoder is memoryless and can be implemented with a *combinatorial logic circuit*

Linear block codes

Definition A block code of length n and 2^k codewords is called a linear (n, k)-code if and only if its 2^k codewords form a k-dimensional subspace of the vector space of all n-tuples over the field $GF(2)$, the Galois Field of order 2

Linear block codes

Definition A block code of length n and 2^k codewords is called a linear (n, k)-code if and only if its 2^k codewords form a k-dimensional subspace of the vector space of all n-tuples over the field $GF(2)$, the Galois Field of order 2

Conclusion

- △ A binary block code is linear if and only if the modulo-2 sum of two codewords is also a codeword
- △ Since (n, k) linear block code C is a k-dimension subspace of V_n, the vector space of all binary n-tuples, it is possible to find k linearly independent codewords $\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{k-1}$ in C such that any codeword $\mathbf{v}$ in C can be written as

$$v = u_0\mathbf{g}_0 + u_1\mathbf{g}_1 + \ldots u_{k-1}\mathbf{g}_{k-1}$$

where $u_i \in \{0, 1\}, 0 \leq i \leq k-1$

Linear block codes

Write

$$\mathbf{G} = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_{k-1} \end{bmatrix} = \begin{bmatrix} g_{00} & g_{01} & \cdots & g_{0,n-1} \\ g_{10} & g_{11} & \cdots & g_{1,n-1} \\ \vdots & \vdots & \vdots & \vdots \\ g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,n-1} \end{bmatrix}_{k \times n}$$

where

$$\mathbf{g}_i = (g_{i0}, g_{i1}, \ldots, g_{i,n-1}), 0 \leq i \leq k-1.$$

Linear block codes

Write

$$\mathbf{G} = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_{k-1} \end{bmatrix} = \begin{bmatrix} g_{00} & g_{01} & \cdots & g_{0,n-1} \\ g_{10} & g_{11} & \cdots & g_{1,n-1} \\ \vdots & \vdots & \vdots & \vdots \\ g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,n-1} \end{bmatrix}_{k \times n}$$

where

$$\mathbf{g}_i = (g_{i0}, g_{i1}, \ldots, g_{i,n-1}), 0 \leq i \leq k-1.$$

Then

$$\begin{aligned} \mathbf{v} &= \mathbf{u} \cdot \mathbf{G} \\ &= u_0\mathbf{g}_0 + u_1\mathbf{g}_1 + \ldots + \ldots, u_{k-1}\mathbf{g}_{k-1} \end{aligned}$$

Linear block codes

Since $\mathbf{G}$ generate the (n, k) linear code C, the matrix $\mathbf{G}$ is called a generator matrix for C.

Linear block codes

Since $\mathbf{G}$ generate the (n, k) linear code C, the matrix $\mathbf{G}$ is called a generator matrix for C.

Example

$$\mathbf{G} = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \mathbf{g}_2 \\ \mathbf{g}_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

generates a $(7, 4)$ linear code

Linear block codes

Since $\mathbf{G}$ generate the (n, k) linear code C, the matrix $\mathbf{G}$ is called a generator matrix for C.

Example

$$\mathbf{G} = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \mathbf{g}_2 \\ \mathbf{g}_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

generates a $(7, 4)$ linear code

Question Verify that $\mathbf{v} = (0\,0\,0\,1\,1\,0\,1)$ is a codeword for the above generator matrix

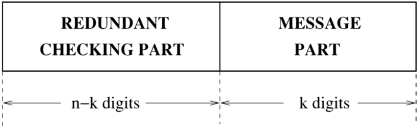
Linear block codes

Systematic format of a codeword A codeword is divided into two parts - the message part and the redundant checking part

Linear block codes

Systematic format of a codeword A codeword is divided into two parts - the message part and the redundant checking part

The message part consists of k unaltered information digits, and the redundant checking part consists of $n-k$ *parity-check* digits



A linear block with this structure is referred to as *linear systematic block code*

Linear block code

Thus a linear systematic (n, k) code is completely described by a $k \times n$ matrix $\mathbf{G}$ of the following form

$$\mathbf{G} = \begin{bmatrix} \mathbf{P} & I_k \end{bmatrix}, \ \mathbf{P} = [p_{ij}] \in \{0, 1\}^{k \times (n-k)}$$

Linear block code

Thus a linear systematic (n, k) code is completely described by a $k \times n$ matrix $\mathbf{G}$ of the following form

$$\mathbf{G} = \begin{bmatrix} \mathbf{P} & I_k \end{bmatrix}, \ \mathbf{P} = [p_{ij}] \in \{0, 1\}^{k \times (n-k)}$$

Let $\mathbf{u} = (u_0, u_1, \ldots, u_{k-1})$ be the message to be encoded. Then the corresponding codeword is

$$\mathbf{v} = \mathbf{u} \cdot \mathbf{G}$$

which gives two equations

$$\begin{aligned} v_{n-k+i} &= u_i, \ 0 \leq i \leq k-1 && (1) \\ v_j &= u_0 p_{0j} + u_1 p_{1j} + \ldots + u_{k-1} p_{k-1,j}, \ 0 \leq j \leq n-k-1. && (2) \end{aligned}$$

Linear block code

Thus a linear systematic (n, k) code is completely described by a $k \times n$ matrix $\mathbf{G}$ of the following form

$$\mathbf{G} = \begin{bmatrix} \mathbf{P} & I_k \end{bmatrix}, \ \mathbf{P} = [p_{ij}] \in \{0, 1\}^{k \times (n-k)}$$

Let $\mathbf{u} = (u_0, u_1, \ldots, u_{k-1})$ be the message to be encoded. Then the corresponding codeword is

$$\mathbf{v} = \mathbf{u} \cdot \mathbf{G}$$

which gives two equations

$$\begin{aligned} v_{n-k+i} &= u_i, \ 0 \leq i \leq k-1 & (1) \\ v_j &= u_0 p_{0j} + u_1 p_{1j} + \ldots + u_{k-1} p_{k-1,j}, \ 0 \leq j \leq n-k-1. & (2) \end{aligned}$$

The $(n-k)$ equations given by equation (2) are called parity-check equations.

Linear block code

Parity-check matrix

- $\triangle$ The generator matrix $\mathbf{G}$ has k linearly independent rows from $\{0,1\}^n$

Linear block code

Parity-check matrix

- △ The generator matrix $\mathbf{G}$ has k linearly independent rows from $\{0,1\}^n$
- △ Then there can be $n-k$ linearly independent rows from $\{0,1\}^n$, say $\mathbf{h}_0, \mathbf{h}_1, \ldots, \mathbf{h}_{n-k}$ such that any vector in the row space of $\mathbf{G}$ is orthogonal to $\mathbf{h}_j$, $0 \leq j \leq n-1$

Linear block code

Parity-check matrix

- $\triangle$ The generator matrix $\mathbf{G}$ has k linearly independent rows from $\{0,1\}^n$
- $\triangle$ Then there can be $n-k$ linearly independent rows from $\{0,1\}^n$, say $\mathbf{h}_0, \mathbf{h}_1, \ldots, \mathbf{h}_{n-k}$ such that any vector in the row space of $\mathbf{G}$ is orthogonal to $\mathbf{h}_j$, $0 \leq j \leq n-1$
- $\triangle$ Define

$$\mathbf{H} = \begin{bmatrix} \mathbf{h}_0 \\ \mathbf{h}_1 \\ \vdots \\ \mathbf{h}_{n-k} \end{bmatrix}$$

Linear block code

Parity-check matrix

- △ The generator matrix $\mathbf{G}$ has k linearly independent rows from $\{0,1\}^n$
- △ Then there can be $n-k$ linearly independent rows from $\{0,1\}^n$, say $\mathbf{h}_0, \mathbf{h}_1, \ldots, \mathbf{h}_{n-k}$ such that any vector in the row space of $\mathbf{G}$ is orthogonal to $\mathbf{h}_j$, $0 \le j \le n-1$
- △ Define

$$\mathbf{H} = \begin{bmatrix} \mathbf{h}_0 \\ \mathbf{h}_1 \\ \vdots \\ \mathbf{h}_{n-k} \end{bmatrix}$$

Then an n-tuple $\mathbf{v}$ is a codeword in the code C generated by $\mathbf{G}$ if and only if $\mathbf{v} \cdot \mathbf{H}^T = \mathbf{0}$

Linear block code

Then the code C is just the null-space of H, which is called a parity-check matrix of the code.

Note The rows of $\mathbf{H}$ also generate a $(n, n-k)$ linear code C_d, which is called the dual code of C.

Linear block code

Then the code C is just the null-space of H, which is called a parity-check matrix of the code.

Note The rows of $\mathbf{H}$ also generate a $(n, n-k)$ linear code C_d, which is called the dual code of C.

Problem The code C_d is the null space $\mathbf{G}$.

Linear block code

Then the code C is just the null-space of H, which is called a parity-check matrix of the code.

Note The rows of $\mathbf{H}$ also generate a $(n, n-k)$ linear code C_d, which is called the dual code of C.

Problem The code C_d is the null space $\mathbf{G}$.

If the generator matrix of an (n, k) linear code is in the systematic form then the parity-check matrix can be in the following form:

$$\mathbf{H} = \begin{bmatrix} I_{n-k} & \mathbf{P}^T \end{bmatrix}.$$

Linear block code

Then the code C is just the null-space of H, which is called a parity-check matrix of the code.

Note The rows of $\mathbf{H}$ also generate a $(n, n-k)$ linear code C_d, which is called the dual code of C.

Problem The code C_d is the null space $\mathbf{G}$.

If the generator matrix of an (n, k) linear code is in the systematic form then the parity-check matrix can be in the following form:

$$\mathbf{H} = \begin{bmatrix} I_{n-k} & \mathbf{P}^T \end{bmatrix}.$$

Then see that

$$\mathbf{G} \cdot \mathbf{H}^T = \mathbf{0}.$$