CIE6020/MAT3350
Selected Topics in Information Theory

Lecture 15: Converse of Channel Coding Theorem

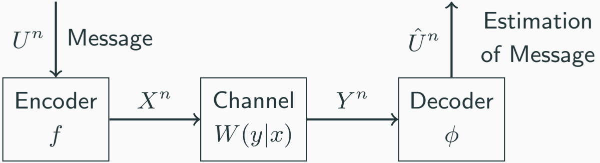
28 March 2019

The Chinese University of Hong Kong, Shenzhen

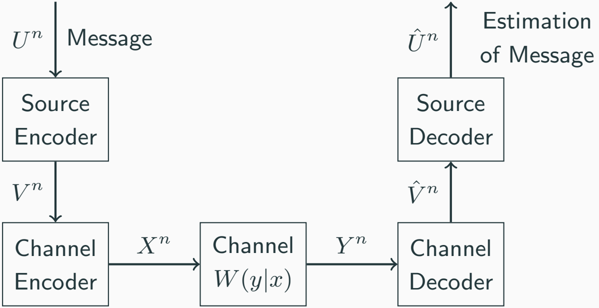
Source-Channel Separation Theorem

Communicate a Source over a Channel

- Joint coding



- Separate coding



Source-Channel Separation Theorem

- Source: a stochastic process $U_1, U_2, \ldots$ with the entropy rate H and $-\frac{1}{n} \log p(U_1, U_2, \ldots, U_n) \to H$ in probability.
- Channel: a DMC $\{W\}$ with capacity C.
- Error probability: $P_e = P(U^n \neq \hat{U}^n)$.

Source-Channel Separation Theorem

- Source: a stochastic process $U_1, U_2, \ldots$ with the entropy rate H and $-\frac{1}{n}\log p(U_1, U_2, \ldots, U_n) \to H$ in probability.
- Channel: a DMC $\{W\}$ with capacity C.
- Error probability: $P_e = P(U^n \neq \hat{U}^n)$.
- If $H < C$, there exists a separate code such that $P_e \to 0$.
- If $H > C$, the error probability is bound away from zero.

Coding Design: Preview

Linear Codes

- Suppose that $\mathcal{A}$ is the input alphabet of a channel.
- A block *error correcting code* $\mathcal{C}$ is a subset of $\mathcal{A}^n$, where n is called the *block length*.
- Most practical channel codes are linear codes, where $\mathcal{A}$ is a finite field.
- A code $\mathcal{C} \subset \mathcal{A}^n$ is *linear* if it is closed under linear combinations, in other words,

$$\alpha \mathbf{x} + \alpha' \mathbf{x}' \in \mathcal{C}, \quad \forall \mathbf{x}, \mathbf{x}' \in \mathcal{C},\ \forall \alpha, \alpha' \in \mathcal{A}.$$

- A linear code $\mathcal{C}$ is a subspace of $\mathcal{A}^n$.
- A linear code with length n and dimension k is said to be an (n, k) code.

Generator Matrix

- For an (n, k) code $\mathcal{C}$, a $k \times n$ matrix G, whose rows form a basis of $\mathcal{C}$, is called a generator matrix for $\mathcal{C}$.
- $\mathcal{C} = \langle G \rangle = \{uG : u \in \mathcal{A}^k\}$.
- A generator matrix G of $\mathcal{C}$ is said to be *systematic* if $G = [I \ P]$, where I is a $k \times k$ identity matrix.

Dual Code and Parity-Check Matrix

- The *dual code* $\mathcal{C}^\perp$ of a linear code $\mathcal{C}$ is defined by

$$\mathcal{C}^\perp = \{\mathbf{v} \in \mathcal{A}^n : \mathbf{v} \cdot \mathbf{x}^\top = 0, \forall \mathbf{x} \in \mathcal{C}\} = \{\mathbf{v} : G\mathbf{v}^\top = \mathbf{0}\}.$$

- The dimension of $\mathcal{C}^\perp$ is $n - k$.
- A generator matrix H of the dual code $\mathcal{C}^\perp$ is also called a *parity-check matrix* of the original code $\mathcal{C}$.
- We can write

$$\mathcal{C} = \{\mathbf{x} : H\mathbf{x}^\top = \mathbf{0}\}.$$

Why Linear Codes?

- The description of linear codes is simple.
- Encoding complexity $O(n^2)$, and even simpler if there exists a sparse generator matrix.
- Linear codes achieve the capacity.

Preview of Channel Codes

- Hamming codes (1950)
- Reed-Solomon codes (early 1950s)
- BCH codes (1959)
- Convolutional codes (1955)
- Turbo codes (1993)
- LDPC (1962, 1997)
- Fountain codes (1998)
- Polar codes (2006)

Hat Problem

- A number N of players are each wearing a hat, which may be of blue or red colours.
- Players can see the colors of all other players' hats, but not that of their own.
- Without any communication, some of the players must guess the color of their hat. Not all players are required to guess.
- All players who guess must decide at the same predetermined time, i.e., they don't know other's guess.
- Players win if at least one player guesses and all of those who guess do so correctly.
- How can the players maximise their chance of winning?