# Electrical Engineering 229A Lecture 15 Notes

Daniel Raban

October 14, 2021

## 1 Proof of the Slepian-Wolf Theorem and Introduction to Channel Coding

### 1.1 Proof of the Slepian-Wolf theorem

Last time, we were proving the Slepian-Wolf theorem. We had an iid sequence of pairs $(X_i, Y_i) \sim (p(x,y), x \in \mathscr{X}, y \in \mathscr{Y})$. Alice and Bob had respective encoding maps

$$e_n^{(1)} : \mathscr{X}^n \mapsto [M_n^{(1)}],$$

$$e_n^{(2)} : \mathscr{Y}^n \mapsto [M_n^{(2)}],$$

and a fusion center tries to decode the pairs of messages using the decoding maps

$$d_n : [M_n^{(1)}] \times [M_n^{(2)}] \to \mathscr{X}^n \times \mathscr{Y}^n.$$

We called the rate pair $(R_1, R_2)$ **achievable** if there exist $((e_n^{(1)}, e_n^{(2)}, d_n), n \geq 1)$ such that

$$\limsup_n \frac{1}{n} \log M_n^{(1)} \leq R_1,$$

$$\limsup_n \frac{1}{n} \log M_n^{(2)} \leq R_2,$$

$$\lim_{n \to \infty} \mathbb{P}(d_n(e_n^{(1)}(X_1^n), e_n^{(2)}(Y_1^n)) \neq (X_1^n, Y_1^n)) = 0.$$

**Theorem 1.1** (Slepian-Wolf)**.** *The set of achievable rate pairs is*

$$\{(R_1, R_2) : R_1 \geq H(X \mid Y), R_2 \geq H(Y \mid X), R_1 + R_2 \geq H(X, Y)\}.$$

We set up the proof of achievability using a random binning argument.

*Proof.* Achievability: By a diagonal-type argument, it suffices to consider $(R_1, R_2)$ such that $R_1 > H(X \mid Y) + \varepsilon$, $R_2 > H(Y \mid X) + \varepsilon$, and $R_1 + R_2 > H(X, Y) + \varepsilon$. The idea is to let $M_n^{(1)} = \lceil 2^{nR_1} \rceil$ and $M_n^{(2)} = \lceil 2^{nR_2} \rceil$. Define random $e_n^{(1)}$ and $e_n^{(2)}$ via:

- $e_n^{(1)}$ randomly assigns each $x_1^n \in \mathscr{X}^n$ to one of $M_n^{(1)}$ bins uniformly, indepndently over $x_1^n$,
- $e_n^{(2)}$ randomly assigns each $y_1^n \in \mathscr{Y}^n$ to one of $M_n^{(2)}$ bins uniformly, indepndently over $y_1^n$
- $d_n(m_n^{(1)}, m_n^{(2)}) = (\widehat{x}_1^n, \widehat{x}_2^n)$ if there is exactly one $(\widehat{x}_1^n, \widehat{y}_1^n) \in A_\delta^{(n)}$ with $e_n^{(1)}(\widehat{x}_1^n) = m_n^{(1)}$ and $e_n^{(2)}(\widehat{y}_1^n) = m_n^{(2)}$. Otherwise, $d_n(m_n^{(1)}, m_n^{(2)})$ can take any value.

We have the probability (over randomness in $(X_1^n, Y_1^n)$ and in $(e_n^{(1)}, e_n^{(2)})$)

$$\mathbb{P}(d_n(e_n^{(1)}(X_1^n), e_n^{(2)}(Y_1^n)) \neq (X_1^n, Y_1^n)) \leq \mathbb{P}(E_{0,n}) + \mathbb{P}(E_{1,n}) + \mathbb{P}(E_{2,n}) + \mathbb{P}(E_{12,n}),$$

where

$$E_{0,n} = \{(X_1^n, Y_1^n) \notin A_\delta^{(n)}\},$$

$$\begin{aligned}
E_{1,n} &= \{\exists\, \widetilde{x}_1^n \neq X_1^n \text{ with } e_n^{(1)}(\widetilde{x}_1^n) = e_n^{(1)}(X_1^n) \text{ and } (\widetilde{x}_1^n, y_1^n) \in A_n^{(\delta)}\}, \\
E_{2,n} &= \{\exists\, \widetilde{x}_1^n \neq X_1^n \text{ with } e_n^{(1)}(\widetilde{x}_1^n) = e_n^{(1)}(X_1^n) \text{ and } (\widetilde{x}_1^n, y_1^n) \in A_n^{(\delta)}\}, \\
E_{12,n} &= \{\exists\, \widetilde{y}_1^n \neq Y_1^n \text{ with } e_n^{(2)}(\widetilde{y}_1^n) = e_n^{(2)}(Y_1^n) \text{ and } (x_1^n, \widetilde{y}_1^n) \in A_n^{(\delta)}\},
\end{aligned}$$

$$\begin{aligned}
E_{12,n} = \{\exists\, &(\widetilde{x}_1^n, \widetilde{y}_1^n) \text{ s.t. } \widetilde{x}_1^n \neq X_1^n, \widetilde{y}_1^n \neq Y_1^n, \\
&e_n^{(1)}(\widetilde{x}_1^n) = e_n^{(1)}(X_1^n), e_n^{(2)}(\widetilde{y}_1^n) = e_n^{(2)}(Y_1^n), (\widetilde{x}_1^n, \widetilde{x}_1^n) \in A_\delta^{(n)}\}.
\end{aligned}$$

We saw that the probabilities of the first three events goes 0 to as $n \to \infty$ if we pick $2\delta < \varepsilon$. It remains to show that $\mathbb{P}(E_{12,n}) \to 0$ as $n \to \infty$. Write

$$\mathbb{P}(E_{12,n}) = \mathbb{E}\left[\sum_{x_1^n, y_1^n} p(x_1^n, y_1^n) \sum_{\substack{\widetilde{x}_1^n \neq x_1^n \\ \widetilde{y}_1^n \neq y_1^n \\ (\widetilde{x}_1, \widetilde{y}_1^n) \in A_\delta^{(n)}}} \mathbb{1}_{\{e_n^{(1)}(\widetilde{x}_1^n) = e_n^{(1)}(x_1^n)\}} \mathbb{1}_{\{e_n^{(2)}(\widetilde{y}_1^n) = e_n^{(2)}(y_1^n)\}}\right]$$

Bring the expectation inside the sum, where the expectation of the inside is just a product of probabilities

$$\begin{aligned}
&= \sum_{x_1^n, y_1^n} p(x_1^n, y_1^n) \sum_{\substack{\widetilde{x}_1^n \neq x_1^n \\ \widetilde{y}_1^n \neq y_1^n \\ (\widetilde{x}_1, \widetilde{y}_1^n) \in A_\delta^{(n)}}} \mathbb{1}_{\{e_n^{(1)}(\widetilde{x}_1^n) = e_n^{(1)}(x_1^n)\}} \frac{1}{M_n^{(1)}} \frac{1}{M_n^{(2)}} \\
&\leq \sum_{x_1^n, y_1^n} p(x_1^n, y_1^n) |A_\delta^{(n)}| \frac{1}{M_n^{(1)}} \frac{1}{M_n^{(2)}} \\
&= |A_\delta^{(n)}| \frac{1}{M_n^{(1)}} \frac{1}{M_n^{(2)}}
\end{aligned}$$

$$\leq 2^{nH(X,Y)} 2^{n\delta} 2^{-nR_1} 2^{-nR_2}.$$

So if $\varepsilon > \delta$, this goes to 0 as $n \to \infty$ because $R_1 + R_2 > H(X,Y) + \varepsilon$ by assumption.

Converse: Consider any scheme $((e_n^{(1)}, e_n^{(2)}, d_n), n \geq 1)$ for which the error probability vanishes asymptotically. Letting $W_n^{(1)} = e_n^{(1)}(X_1^n)$ and $W_n^{(2)} = e_n^{(2)}(Y_1^n)$, we have

$$\begin{tikzcd}
X_1^n \arrow[r, dash] & W_n^{(1)} \arrow[dr, dash] & \\
 & & (\widehat{X}_1^n, \widehat{Y}_1^n) = d_n(W_n^{(1)}, W_n^{(2)}) \\
Y_1^n \arrow[r, dash] & W_n^{(2)} \arrow[ur, dash] &
\end{tikzcd}$$

Let $p_e^{(n)} = \mathbb{P}((\widehat{X}_1^n, \widehat{Y}_1^n) \neq (X_1^n, Y_1^n))$. We have by Fano's inequality that

$$H(X_1^n, Y_1^n \mid W_n^{(1)}, W_n^{(2)}) \leq h(p_e^{(n)}) + p_e^{(n)}(\log|\mathscr{X}|^n + \log|\mathscr{Y}|^n),$$

so if $p_e^{(n)} \to 0$ then $H(X_1^n, Y_1^n \mid W_n^{(1)}, W_n^{(2)}) \leq n\varepsilon_n$ for some $\varepsilon_n \to 0$ as $n \to \infty$. Then, recalling that $R_1 = \frac{1}{n}\log M_n^{(1)}$ and $R_2 = \frac{1}{n}\log M_n^{(2)}$,

$$\begin{aligned}
n(R_1 + R_2) &\geq H(W_n^{(1)}, W_n^{(2)}) \\
&= I(X_1^n, Y_1^n; W_n^{(1)}, W_n^{(2)}) + H(W_n^{(1)}, W_2^{(n)} \mid X_1^n, Y_1^n) \\
&= H(X_1^n, Y_1^n) - H(X_1^n, Y_1^n \mid W_n^{(1)}, W_n^{(2)}) \\
&\geq nH(X,Y) - n\varepsilon_n.
\end{aligned}$$

But we also have

$$H(X_1^n \mid W_n(1), W_n^{(2)}, Y_1^n) \leq n\varepsilon_n,$$

which gives

$$\begin{aligned}
nR_1 &\geq H(W_1^{(n)}) \\
&\geq H(W_n^{(1)} \mid Y_1^n) \\
&= I(X_1^n l W_1^{(n)} \mid Y_1^n) + H(W_1^{(n)} \mid X_1^n, Y_1^n) \\
&= H(X_1^n \mid Y_1^n) - H(X_1^{(n)} \mid W_n^{(1)}, Y_1^n, W_n^{(2)},
\end{aligned}$$

where we can throw $W_n^{(2)}$ in for free.

$$\geq nH(X \mid Y) - n\varepsilon_n.$$

Similarly, $R_2 \geq H(Y \mid X) - n\varepsilon_n$. Now divide by $n$ and let $n \to \infty$ to get the lower bounds. This gives

$$\begin{aligned}\liminf_n \frac{1}{n} \log M_n^{(1)} + \frac{1}{n} \log M_n^{(2)} &\geq H(X, Y), \\ \liminf_n \frac{1}{n} \log M_n^{(1)} &\geq H(X \mid Y), \\ \liminf_n \frac{1}{n} \log M_n^{(2)} &\geq H(Y \mid X).\end{aligned} \qquad \square$$

## 1.2 The discrete memoryless channel model for data transmission

At each time, the transmitter sends a symbol $x \in \mathscr{X}$, and the receiver gets $y \in \mathscr{Y}$ according to the conditional probabilities $(p(y \mid X), x \in \mathscr{X}, y \in \mathscr{Y})$.

**Example 1.1** (Binary symmetric channel)**.** The receival probability is $1 - p$, so

$$H(1 \mid 0) = p(0 \mid 1) = p, \qquad p(1 \mid 1) = p(0 \mid 0) = 1 - p.$$

**Definition 1.1.** A **communication scheme** is a sequence $((e_n, d_n), n \geq 1)$ such that

$$e_n : [M_n] \to \mathscr{X}^n, \qquad d_n : \mathscr{Y}^n \to [M_n].$$

**Definition 1.2.** Communication is possible **at rate** $R$ if there exis t$((e_n, d_n), n \geq 1)$ with

$$\liminf_n \frac{1}{n} \log M_n \geq R$$

and

$$\mathbb{P}(d_n(e_n(W_n)) \neq W_n) \xrightarrow{n \to \infty} 0,$$

where $W_n \sim \mathrm{Unif}([M_n])$.

**Theorem 1.2** (Shannon's channel coding theorem)**.** *The supremum over all rates at which communication is possible is*

$$\sup_{(p(x), x \in \mathscr{X})} I(X; Y) = \sup_{(p(x), x \in \mathscr{X})} \sum_{x,y} p(x) p(y \mid x) \log \frac{p(y \mid x)}{p(x) \sum_{x'} p(x') p(y \mid x')}.$$