

Lecture 6

Lecturer: Haim Permuter

Scribe: Uria Basher

I. ACHIEVABILITY OF THE CAPACITY REGION FOR MULTIPLE-ACCESS CHANNEL

We consider the following channel coding problem:

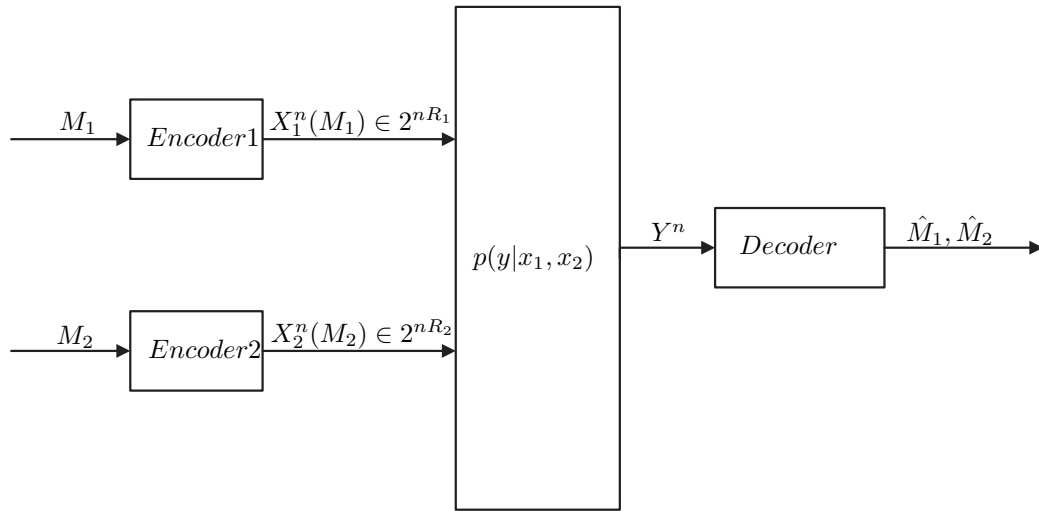


Fig. 1. Multiple-Access Channel

Theorem 1 (MAC capacity region)

The capacity of a multiple-access channel $(\mathcal{X}_1 \times \mathcal{X}_2, P(y|x_1, x_2), \mathcal{Y})$ is the closure of the convex hull of all (R_1, R_2) satisfying:

$$R_1 < I(X_1; Y|X_2), \quad (1)$$

$$R_2 < I(X_2; Y|X_1), \quad (2)$$

$$R_1 + R_2 < I(X_1, X_2; Y) \quad (3)$$

for some product distribution $P_1(x_1)P_2(x_2)$ on $\mathcal{X}_1 \times \mathcal{X}_2$.

In the previous lecture we gave the converse proof. We will now prove the achievability of the rate region in Theorem 1, but first let us give a short review on typical sets.

A. Typical Sets

Definition 1 (Typical set)

The *typical set*, $A_\epsilon^{(n)}(X)$, with respect to $P(x)$, is the set of sequences $(x_1, x_2, \dots, x_n) \in \mathcal{X}^n$ with the property

$$2^{-n(H(X)+\epsilon)} \leq \Pr(x^n) \leq 2^{-n(H(X)-\epsilon)} \quad (4)$$

Theorem 2 (Typical set properties)

For every $\epsilon > 0$ and n sufficiently large, we can show that the set $A_\epsilon^{(n)}$, has the following properties:

- 1) if $x^n \in A_\epsilon^{(n)} \rightarrow H(X) - \epsilon \leq -\frac{1}{n} \log p(x^n) \leq H(X) + \epsilon$.
- 2) $\Pr \{A_\epsilon^{(n)}\} \geq 1 - \epsilon$ for n sufficiently large.
- 3) $|A_\epsilon^{(n)}| \leq 2^{n(H(X)+\epsilon)}$, where $|A|$ denotes the number of elements (cardinality) in the set A .
- 4) $|A_\epsilon^{(n)}| \geq (1 - \epsilon)2^{n(H(X)-\epsilon)}$.

Where $P(x^n) = \prod_{i=1}^n P_X(x_i)$.

Definition 2 (Jointly typical set)

The set $A_\epsilon^n(X, Y)$ of *jointly typical* sequences $\{(x^n, y^n)\}$ with respect to the distribution $p(x, y)$ is the set of n -sequences with empirical entropies ϵ -close to the true entropies:

$$A_\epsilon^{(n)}(X, Y) = \{(x^n, y^n) \in \mathcal{X}^n \times \mathcal{Y}^n : \quad (5)$$

$$| -\frac{1}{n} \log p(x^n) - H(X) | \leq \epsilon,$$

$$| -\frac{1}{n} \log p(y^n) - H(Y) | \leq \epsilon, \quad (6)$$

$$| -\frac{1}{n} \log p(x^n, y^n) - H(X, Y) | \leq \epsilon \}, \quad (7)$$

where

$$p(x^n, y^n) = \prod_{i=1}^n p(x_i, y_i). \quad (8)$$

Theorem 3 (Jointly Typical set properties)

Let (X^n, Y^n) be sequences of length n drawn *i.i.d.* according to $p(x^n, y^n) = \prod_{i=1}^n p(x_i, y_i)$. Then:

- 1) $\Pr(x^n, y^n \in A_\epsilon^{(n)}) \xrightarrow{n \rightarrow \infty} 1$.
- 2) $|A_\epsilon^{(n)}| \leq 2^{n(H(X, Y)+\epsilon)}$.
- 3) If $(\tilde{X}^n, \tilde{Y}^n) \sim P_{X^n}(x^n) P_{Y^n}(y^n)$, then

$$\Pr((\tilde{X}^n, \tilde{Y}^n) \in A_\epsilon^n) \leq 2^{-n(I(X, Y)-3\epsilon)}. \quad (9)$$

also, for sufficiently large n ,

$$\Pr((\tilde{X}^n, \tilde{Y}^n) \in A_\epsilon^n) \geq (1 - \epsilon)2^{-n(I(X, Y)+3\epsilon)}. \quad (10)$$

B. Achievability

Definition 3 (Average probability of error)

The Average probability of error is defined as,

$$P_e^{(n)} = \Pr \left\{ (M_1, M_2) \neq (\hat{M}_1, \hat{M}_2) \right\}. \quad (11)$$

To prove the achievability of the capacity region for Multiple-Access Channel, we need to show that for a fix $p(x_1)p(x_2)$ where,

$$R_1 < I(X_1; Y | X_2), \quad (12)$$

$$R_2 < I(X_2; Y | X_1), \quad (13)$$

$$R_1 + R_2 < I(X_1, X_2; Y) \quad (14)$$

there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes where $P_e^{(n)} \rightarrow 0$ as $n \rightarrow \infty$.

Proof: (Achievability in Theorem 1)

codeboook generation :Generate 2^{nR_1} independent codewords $X_1^n(i)$ where $i \in \{1, 2, \dots, 2^{nR_1}\}$ of length n , generating each symbol *i.i.d*, $X_1^n(i) \sim \prod_{i=1}^n p_1(x_{1i})$. Similarly generate 2^{nR_2} independent codewords $X_2^n(j)$ where $j \in \{1, 2, \dots, 2^{nR_2}\}$, $X_2^n(j) \sim \prod_{j=1}^n p_2(x_{2j})$.

Encoding: If User 1 want to send message i he sends the codeword $X_1^n(i)$. Similarly, if user 2 want to send message j he sends the codeword $X_2^n(j)$.

Decoding: Given Y_1^n The receiver chooses a pair (i, j) s.t.

$$(X_1^n(i), X_2^n(j), Y^n) \in A_\epsilon^{(n)}(X_1, X_2, Y). \quad (15)$$

if no such a pair is found an error will be declared.

Analysis of the probability of error: Without loss of generality ,we assume that $(i, j) = (1, 1)$ was sent. There will be an error if either the correct codewords are not jointly typical with Y_1^n or there is a pair of incorrect codewords that are typical with Y_1^n . Let us define the following events:

$$E_1 = \left\{ (X_1^n(1), X_2^n(1), Y^n) \notin A_\epsilon^{(n)}(X_1, X_2, Y) \right\}, \quad (16)$$

$$E_2 = \left\{ \exists j \neq 1 : (X_1^n(1), X_2^n(j), Y^n) \in A_\epsilon^{(n)}(X_1, X_2, Y) \right\}, \quad (17)$$

$$E_3 = \left\{ \exists i \neq 1 : (X_1^n(i), X_2^n(1), Y^n) \in A_\epsilon^{(n)}(X_1, X_2, Y) \right\}, \quad (18)$$

$$E_4 = \left\{ \exists i \neq 1, j \neq 1 : (X_1^n(i), X_2^n(j), Y^n) \in A_\epsilon^{(n)}(X_1, X_2, Y) \right\}, \quad (19)$$

Then by the union of events bound,

$$\begin{aligned} P_e^{(n)} &= \Pr(E_1 \cup E_2 \cup E_3 \cup E_4) \\ &\leq P(E_1) + P(E_2) + P(E_3) + P(E_4), \end{aligned} \quad (20)$$

Now let us find the probability of each event,

- $P(E_1)$ - By using Theorem 3 part 1) we have,

$$P(E_1) \rightarrow 0. \quad (21)$$

- $P(E_2)$ - for $j \neq 1$ the probability of error,

$$\begin{aligned} P(E_2) &= \Pr\left((X_1^n(1), X_2^n(j), Y_1^n) \in A_\epsilon^{(n)}\right) \\ &= \sum_{j=2}^{j=2^{nR_2}} P(E_{2j}) \\ &= 2^{nR_2} \cdot 2^{-n(I(X_2;X_1,Y)-\epsilon)}, \end{aligned} \quad (22)$$

For $P(E_2) \rightarrow 0$ as $n \rightarrow \infty$, we need to choose ,

$$\begin{aligned} R_2 &< I(X_2; X_1, Y) - \epsilon \\ &= I(X_2; X_1) + I(X_2; Y|X_1) - \epsilon \\ &\stackrel{(a)}{=} I(X_2; Y|X_1) - \epsilon, \end{aligned} \quad (23)$$

where (a) follows from the independence of X_1 and X_2 .

- $P(E_3)$ - Similarly ,if $R_1 < I(X_1; Y|X_2) - \epsilon$ then $P(E_3) \rightarrow 0$ as $n \rightarrow \infty$.
- $P(E_4)$ - For $i \neq 1, j \neq 1$,

$$\begin{aligned} P(E_4) &= P\left((X_1^n(i), X_2^n(j), Y_1^n) \in A_\epsilon^{(n)}\right) \\ &= \sum_{j=2}^{j=2^{nR_2}} \sum_{i=2}^{i=2^{nR_1}} P(E_{4i,j}) \\ &= 2^{n(R_1+R_2)} \cdot 2^{-n(I(X_1,X_2;Y)-\epsilon)}. \end{aligned} \quad (24)$$

So if $R_1 + R_2 < I(X_1, X_2; Y) - \epsilon$, then $P(E_4) \rightarrow 0$ as $n \rightarrow \infty$.

Thus, the probability of error, conditioned on a particular codeword being sent, goes to zero if the conditions of the theorem are met. The above bound shows that the average probability of error, which by symmetry is equal to the probability for an individual codeword, averaged over all choices of codebooks in the random code construction, is arbitrarily small. Hence there exists at least one code \mathcal{C} with arbitrarily small probability of error. To complete the proof we use time-sharing to allow any (R_1, R_2) in the convex hull to be achieved.

■