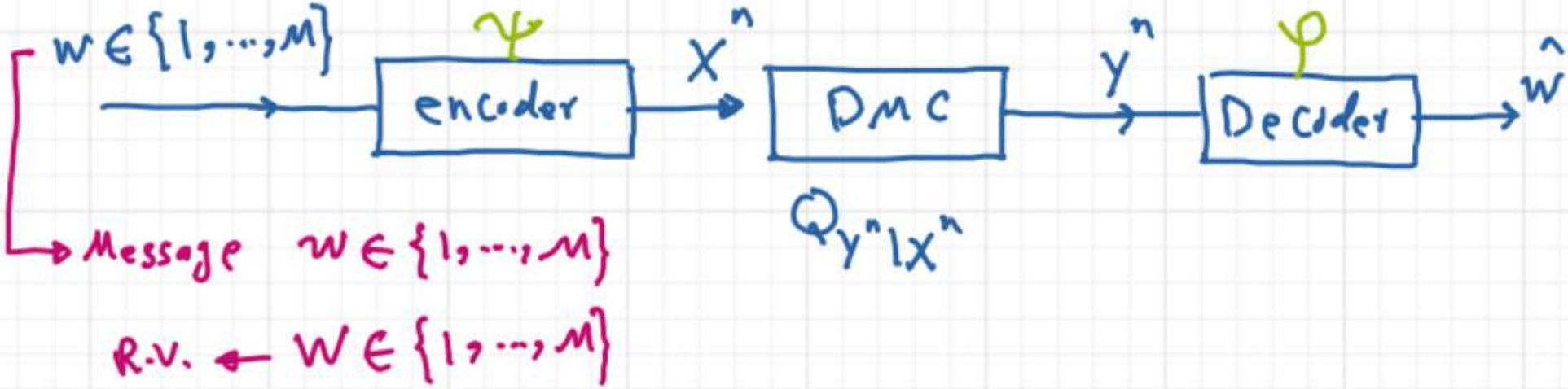
تئوری اطلاعات و کدینگ : جلسه 17 ، 8 آذر 99

* مطالب جلسه:
  - برخی تعاریف لازم برای بیان قضیه ظرفیت کانال
  - قضیه ظرفیت کانال شنون { achievability, Converse }
  - یادآوری نامساوی مارکوف
  - اثبات بخش Converse قضیه ظرفیت کانال شنون

یادآوری مسئله انتقال اطلاعات بر روی کانال شنون (کانال DMC):



* تعریف (کد بلاکی یا block code): یک کد بلاکی (n, M) داریم که n طول کدواژه‌ها و M تعداد کدواژه‌های این کد است.

A block code $\leftarrow C = \{\underline{x}^{(1)}, \dots, \underline{x}^{(M)}\}, \quad \underline{x}^{(i)} \in \mathcal{X}^n$

* انکودر (کدگذار): یک نگاشت از پیام‌ها به $\mathcal{X}^n$ ؛

$$\Psi_C \leftarrow \Psi : \{1, \dots, M\} \longrightarrow \mathcal{X}^n$$

* نرخ یک کد بلاکی: نرخ یک کد بلاکی (n, M) به صورت زیر تعریف می‌شود:

$$R_C = \frac{\log_2(M)}{n} \quad \text{bits/channel use}$$

نماینده خطا در دیکودکردن

* دیکودر: یک نگاشت از خروجی کانال به مجموعه $\{0, 1, \dots, M\}$

$$\varphi : \mathcal{Y}^n \longrightarrow \{0, 1, \dots, M\}$$

* تعریف (احتمال خطای ارسال پیام iام):

$$\lambda_i(C) \triangleq \mathbb{P}\left[\hat{W} \neq i \mid W = i, C\right]$$

$$= \mathbb{P}\left[\varphi(Y^n) \neq i \mid X^n = \underline{x}^{(i)}, C\right]$$

$$= \sum_{\underline{y} \in \mathcal{Y}^n} Q_{Y^n|X^n}(\underline{y} \mid \underline{x}^{(i)}) \, \mathbb{1}_{\{\varphi(\underline{y}) \neq i\}}$$

* تعریف (احتمال متوسط خطا):

$$P_e^{(n)}(C) \triangleq \frac{1}{M} \sum_{i=1}^{M} \lambda_i(C)$$

* تعریف (احتمال خطای ماکسیمم):

$$P_{e,\max}^{(n)}(C) \triangleq \max_{i \in \{1,\dots,M\}} \lambda_i(C)$$

* توجه: اگر توزیع روی پیام‌ها یکنواخت باشد (W یک متغیر تصادفی یکنواخت روی $\{1,\dots,M\}$ باشد)، آنگاه

$$P[\hat{W} \neq W \mid C] = \sum_{i \in [1:M]} P_W(i) \cdot \lambda_i(C)$$

$$= P_e^{(n)}(C)$$

---

* تعریف (ظرفیت کانال‌های نویزی):

برای کانال‌های DMC با ظرفیت (اطلاعاتی) C ($C > 0$) داریم:

① (achievability):

برای $\varepsilon > 0$ و برای $R < C$ یک کد بلاکی V_C با طول n به اندازه کافی بزرگ و نرخ $R_C \geq R$ و یک روش دیکودینگ وجود دارد که

$$P_{e,max}^{(n)}(C) < \varepsilon$$

② (converse):

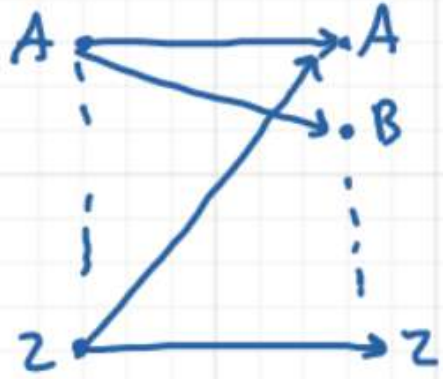
برای هر دنباله کدهای بلاکی به صورت $(n, 2^{nR})$ که داشته باشیم

(برای n های بسیار بزرگ)

$$P_{e,max}^{(n)} \xrightarrow{n \to \infty} 0$$

آنگاه باید داشته باشیم $R \leq C$.

* مثال: کانال ماشین تحریر نویزی:



$\Rightarrow C = \log_2 13$

$\{1, \dots, 13\}$

$\psi(1) \longrightarrow A$

$\psi(2) \longrightarrow C$

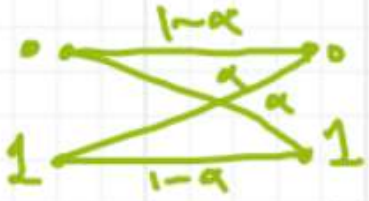
$\vdots$

$\psi(13) \longrightarrow Y$

در اینجا با یک کد به طول $n=1$ به راحتی به ظرفیت کانال می‌رسیم.

---

* مثال: کانال باینری متقارن $BSC(\alpha)$ را در نظر بگیرید: $(\alpha < \frac{1}{2})$



$$\psi = \begin{cases} 0 \longrightarrow 0^n \\ 1 \longrightarrow 1^n \end{cases}$$

repetition code

دیکودر: φ: majority decoding : تعداد صفرها و یک‌های دریافتی را می‌شمارد و هرکدام بیشتر بود به آن دیکود می‌کند.

$$P_e^{(n)} = \sum_{i=\lceil \frac{n}{2} \rceil}^{n} \binom{n}{i} \alpha^i (1-\alpha)^{n-i}$$: average prob. of error

$$= \mathbb{P}\left[Z \geq \lceil \tfrac{n}{2} \rceil \right] \qquad Z \sim \text{Binomial}(n, \alpha)$$

$$= \mathbb{P}\left[Z \geq \underbrace{\mathbb{E}[Z]}_{n\alpha} + \underbrace{\left(\lceil \tfrac{n}{2} \rceil - \mathbb{E}[Z] \right)}_{>0} \right]$$

$$\leq e^{-\eta n} \xrightarrow{n \to \infty} 0.$$

↳ Chernoff bound

اثبات قضیه‌ی این‌که با افزایش n به بینهایت صفر می‌رود.

ولی این‌که خوب نیست چون نرخ آن در حد به بینهایت صفر می‌رود:

$$M = 2 \quad \Rightarrow \quad R = \frac{\log_2 M}{n} = \frac{1}{n} \xrightarrow{n \to \infty} 0 \neq C_{BSC(\alpha)} = 1 - h_2(\alpha)$$

یادآوری تساوی فانو:

فرض کنید X یک متغیر تصادفی گسسته با شد و توزیع مشترک با Y دارد. از روی Y یک تخمین $\hat{X}$ برای X پیدا می‌کنیم. اگر احتمال خطا را تعریف کنیم

$$P_e = P[\hat{X} \neq X]$$

آنگاه:

$$H(X|Y) \leq H(X|\hat{X}) \leq h_2(P_e) + P_e \log_2(|\mathcal{X}|-1)$$
$$\leq 1 + P_e \log_2(|\mathcal{X}|)$$

* لم زیر را هم نیاز داریم (Single letterization lemma)

اگر Y^n رشته خروجی یک کانال DMC با شد که ورودی آن رشته X^n بوده و ظرفیت کانال هم C با شد، آنگاه داریم:

$$I(X^n;Y^n) \leq n\, I(X;Y) \leq nC \quad \text{for all } P_{X^n}$$

اثبات:

$$I(X^n;Y^n) = H(Y^n) - H(Y^n|X^n)$$

$$= H(Y^n) - \sum_{i=1}^{n} H(Y_i \mid Y_1, \dots, Y_{i-1}, X^n)$$

DMC ⟶

$$= H(Y^n) - \sum_{i=1}^{n} H(Y_i|X_i)$$

$$\leq \sum_{i=1}^{n} H(Y_i) - \sum_{i=1}^{n} H(Y_i|X_i)$$

$$= \sum_{i=1}^{n} I(X_i;Y_i)$$

$$\leq n \cdot C$$

* اثبات Converse متغیر کانال :

فرض: یک دنباله کد $(n, 2^{nR})$ داریم که $P_{e,max}^{(n)} \xrightarrow{n\to\infty} 0$

می‌خواهیم نشان دهیم که $R \leq C$.

نکته اول: $P_{e,max}^{(n)} \to 0 \Leftarrow P_e^{(n)} \xrightarrow{n\to\infty} 0$

نکته دوم: فرتبه مارکف رو برو را داریم:

$$W \longleftrightarrow X^n \longleftrightarrow Y^n \longleftrightarrow \hat{W}$$

$W \in \{1, \dots, 2^{nR}\}$

فرض: توزیع روی پیام های ورودی (W) یکنواخت است. $\Rightarrow H(W) = nR$

$$P_e = P[\hat{W} \neq W] = P_e^{(n)}$$

$$nR = H(W)$$

$$= H(W|\hat{W}) + I(W;\hat{W})$$

$$\leq 1 + P_e^{(n)}(C) \cdot nR + I(X^n; Y^n)$$

Fano

↳ Data processing Ineq.

$$\leq 1 + P_e^{(n)}(C) \cdot nR + nC$$

↳ از لم با X

$$\Rightarrow \boxed{R \leq \frac{1}{n} + P_e^{(n)}(C) R + C}$$

$$R \leq C \Leftarrow P_e^{(n)}(C) \to 0 \text{ و } \frac{1}{n} \to 0 \Leftarrow n \to \infty \text{ با افزایش}$$

• یک طور دیگر هم می‌توانیم به عبارت کار در محدوده نگاه کنیم:

$$P_e^{(n)} \geq 1 - \frac{C}{R} - \frac{1}{nR}$$

حال اگر $n \to \infty$ و $R > C$ $\Leftarrow$ سمت راست یک عدد اکیداً بزرگ‌تر از صفر

می‌شود $\Leftarrow$ احتمال خطای $P_e^{(n)}$ نمی‌تواند صفر باشد.