بهنام خدا

خواص ظرفیت

1- همواره $C \geq 0$ زیرا $I(X,Y) \geq 0$

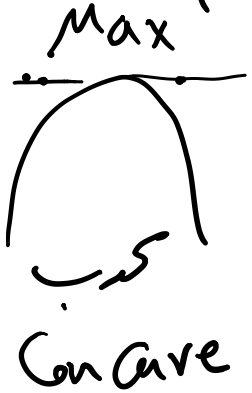
2- همواره $C \leq \log|X|$ زیرا $I(X;Y) = H(X) - H(X|Y) \leq H(X)$

3- همواره $C \leq \log|Y|$ زیرا $I(X;Y) = H(Y) - H(Y|X) \leq H(Y)$

4+ $I(X;Y)$ تابعی پیوسته از $p(x)$ است و اگر $H(X|Y)$, $H(X)$ توابع پیوسته از $p(x)$ هستند)

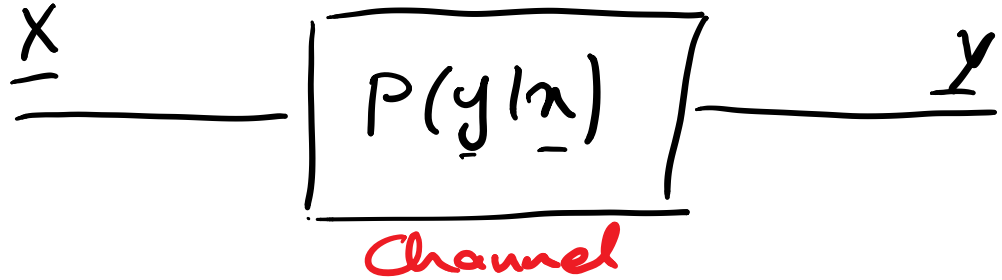
5- $I(X;Y)$ تابعی Concave با کرب نسبت به $P(x)$ است. / قضیه فصل ۷م

اگر $P(y|x)$ ثابت باشد، $I(X;Y)$ تابعی Concave از $P(x)$ خواهد بود.

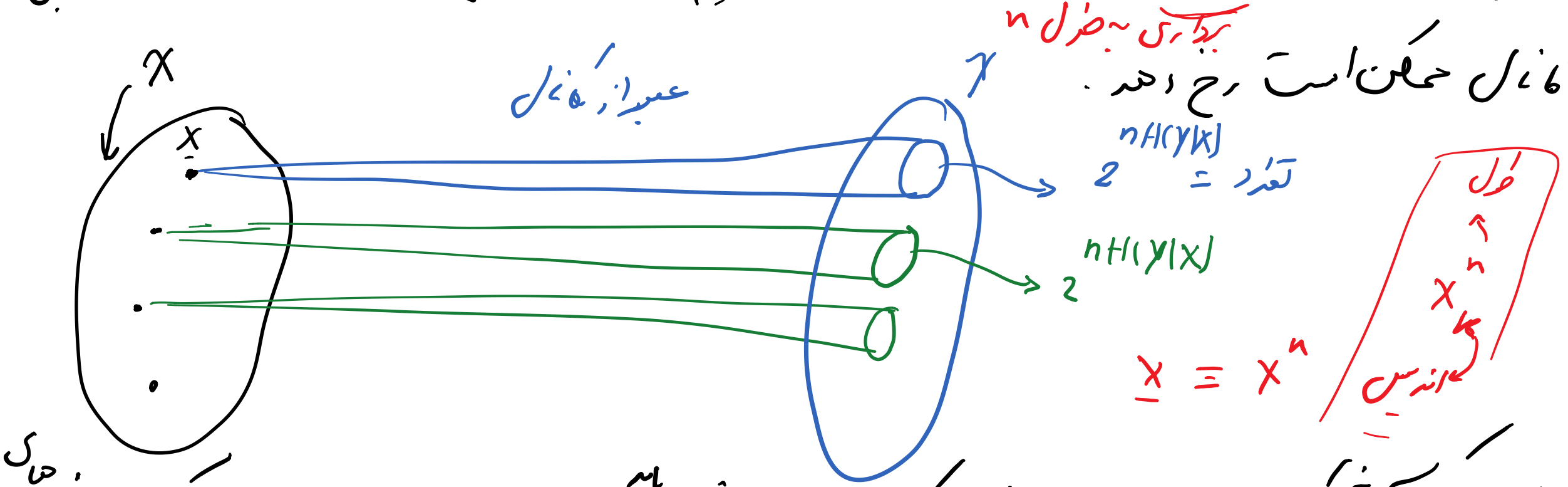


اثبات ستهوری ظرفیت کانال

ظرفیت کانال، بزرگترین تعداد بیتی که در هر بار استفاده از کانال، با خطای به میزان دلخواه کم قابل انتقال است یا به بیان دیگر بزرگترین نرخ قابل اطمینان برای انتقال روی کانال reliable



اگر دنباله نوعی $\underline{X}$ را به ورودی کانال اعمال کنیم، $2^{nH(Y|X)}$ حالت مختلف در خروجی کانال ممکن است رخ دهد.



برای اینکه آشکارسازی بدون خطا امکان پذیر باشد، باید مجموعه Y های مربوط به هریک از دنباله های نوعی با مجموعه Y های مربوط به بقیه دنباله های نوعی، هیچ‌گونه اشتراکی نداشته باشد.

از طرف دیگر تعداد حالتهای ممکن برای Y برابر است با $2^{nH(Y)}$. بنابراین تعداد

دنباله های نرمی $\underline{x}$ که می توان بدون خطا از کانال عبور داد، برابر است با تعداد زیر-
مجموعه های غیرهمپوشان در Y یعنی

$$\text{تعداد } \underline{x} \text{ های قابل استفاده بدون خطا} = \frac{\text{تعداد کل}}{\text{تعداد اعضای مجموعه متصل}} = \frac{2^{nH(Y)}}{2^{nH(Y|X)}} = 2^{n(H(Y)-H(Y|X))}$$

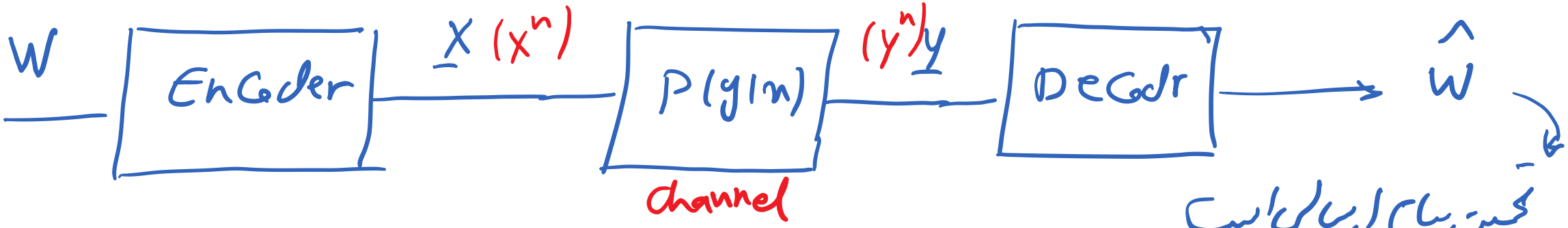
$$= 2^{nI(X;Y)} \leq 2^{nC}$$

بنابراین حداکثر تعداد دنباله های n قابل ارسال بدون خطا روی کانال برابر $2^{nI(X;Y)}$ است.
پس می توان گفت که ظرفیت کانال (ماکزیمم تعداد بیت های قابل ارسال بدون خطا) برابر C است.
(با خطای بسیار ناچیز)

C bits/channel use

بنابراین می‌توان با تصویر کردن مناسب پیام‌های منبع به یک مجموعه نزدیک، ارسال را با احتمال قابل اطمینان (با خطای به میزان دلخواه کم) انجام داد. این تصویرسازی همان کدینگ کانال است

بلوک دیاگرام این سیستم انتقال به صورت زیر خواهد بود



تخمین پیام ارسالی است

و ممکن است با خطا همراه باشد

W اندیس پیام ارسالی است و داریم $W \in \{1, 2, \dots, M\}$

این اندیس وارد محوک انکودری شود و در خروجی به طول n کلمه کد $X^n(W)$ در خروجی خواهیم داشت که وابسته به مقدار W است. $X^n(W)$ از کانال عبور می‌کند و در خروجی دنباله Y^n را خواهیم داشت. عملیات دیکدینگ به صورت تابعی بر روی Y^n اعمال می‌شود $\hat{W} = g(Y^n)$ تا اندیس خروجی تعیین شود. $\hat{W}$ می‌تواند دقیقاً همان W نباشد، یعنی همواره خطا خواهیم داشت. اگر خطا به میزان دلخواه کم باشد، ارسال قابل اطمینان روی کانال امکان‌پذیر است. در ادامه می‌خواهیم قضیه‌ی مهم شانون در مورد کانال را به صورت ریاضی اثبات کنیم. برای این منظور ابتدا مفاهیم زیر را معرفی می‌کنیم.

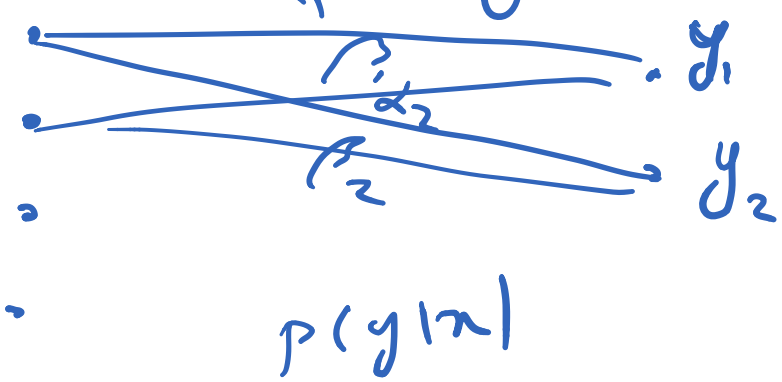
کانال گسسته Discrete Channel

کانال گسسته به صورت $(X, P(y|x), Y)$ تعریف می‌شود که در آن

$$P(y|x) \geq 0 \quad , \quad \sum_{y} P(y|x) = 1$$

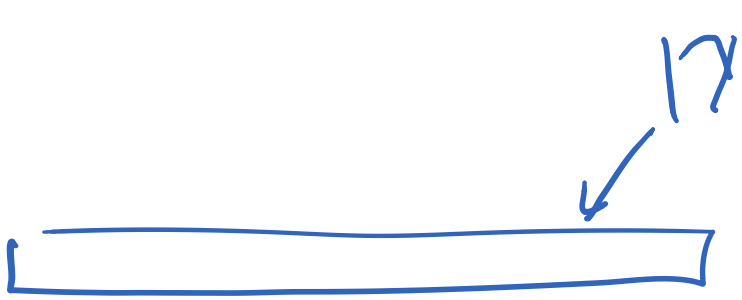
$$P(x) \rightarrow \sum_{x} P(x) = 1$$

$$P(y|x) \rightarrow \sum_{y} P(y|x) = 1$$



$\alpha_1 + \alpha_2 = 1$

$\beta_1 + \beta_2 = 1$



توزیع احتمالاتی $\rightarrow$ y

متغیر ورودی کپه $|Y|$

کانال گسسته بدون حافظه — Discrete Memoreless Channel (DMC)

سطح مرتبه ام یک کانال DMC به صورت $(X^n, P(y^n/x^n), Y^n)$ تعریف می‌شود.

که در آن

$$x^n = (x_1, x_2, \dots, x_n)$$

$$y^{k-1} = (y_1, y_2, \dots, y_{k-1})$$

$$P(y_k / x^n, y^{k-1})$$

$$= P(y_k / x^n) = P(y_k / x_k)$$

شرط بی‌حافظه بودن

اگر کانال گسسته بدون حافظه، فیدبک نداشته باشد، یعنی سمبلهای ورودی در هر لحظه بسمبلهای خروجی در لحظات قبل بستگی نداشته باشد!

$$P(x_k / y^{k-1}, x^{k-1}) = P(x_k / x^{k-1})$$

بدون فیدبک بودن

در این صورت داریم،

$$P(y^n|x^n) = \prod_{i=1}^{n} P(y_i|y^{i-1}, x^n)$$

$P(\underline{y}|\underline{x})$

$$= \prod_{i=1}^{n} P(y_i|y^{i-1}, x^i)$$

$\updownarrow$ علی

$$= \prod_{i=1}^{n} P(y_i|x_i)$$

$\uparrow$ DMC

کدینگ کانال Channel Coding

کدینگ کانال دارای اجزای زیر است

۱- مجموعه اندیس $\{1, 2, \dots, M\}$

۲- یک تابع کدینگ به صورت

$$\{1, 2, \dots, M\} \xrightarrow{x^n} \mathcal{X}^n$$

بنابراین کلمات کد به صورت $x^n(1), x^n(2), \dots, x^n(M)$ خواهند بود.

کتاب کد : Code Book $= \{x^n(1), x^n(2), \dots, x^n(M)\}$

کلمه کد : Codeword x^n

۳- یک تابع دیکدینگ به صورت

$$\mathcal{Y}^n \xrightarrow{g(y^n)} \{1, 2, \dots, M\}$$

این مجموعه را یک کد کانال (M, n) برای کانال $(\mathcal{X}, P(y|x), \mathcal{Y})$ می‌گوییم.

۱- احتمال خطای شرطی (Conditional Error Prob.)

احتمال خطای شرطی به شرط ارسال اندیس i ام به صورت زیر تعریف می‌شود، (λ_i)

$$\lambda_i = P_r\{\underbrace{g(y^n)}_{\hat{W}} \neq i \mid W = i\} \equiv P_r\{g(y^n) \neq i \mid x^n = x^n(i)\}$$

$$= \sum_{\substack{\text{روی همه‌ی } y^n \text{ هایی} \\ \text{که حاصل } g \text{ آن‌ها} \\ i \text{ است}}} P(y^n|x^n) = \sum_{y^n} P(y^n|x^n)\, I(g(y^n) \neq i)$$

که در آن تابع $I(\cdot)$ تابع indicator است یعنی

$$I(\cdot) = \begin{cases} 1 & \text{Correct} \\ 0 & \text{incorrect} \end{cases}$$

- احتمال خطای ماکزیمال (Maximal Error Prob.)

احتمال خطای ماکزیمال که با $\lambda^{(n)}$ نمایش داده می‌شود برای یک کد (M, n) روی کانال $(\mathcal{X}, P(y|x), \mathcal{Y})$ به صورت زیر تعریف می‌شود

$$\lambda^{(n)} = \max_{1 \le i \le M} \lambda_i$$

متوسط احتمال خطا

برای یک کد (M, n) متوسط احتمال خطا، به صورت زیر تعریف می‌شود،

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

احتمال خطای یک کد $C(M, n)$

$$P_e = \sum_{i=1}^{M} P_r\{W=i\}\,\lambda_i = P_r\{\hat{W} \neq W\} \equiv P_r\{g(y^n) \neq W\}$$

← اگر پیام‌های ارسالی هم‌احتمال باشند با توزیع احتمال یکنواخت، داریم:

$$P_r\{W=i\} = \frac{1}{M} \quad ; \quad \forall i \in \{1, 2, \ldots, M\}$$

آنگاه متوسط احتمال خطا با احتمال خطا برابر است یعنی $P_e^{(n)} = P_e$

- نرخ کد (Code rate)

برای یک کد $C(M, n)$ نرخ کد به صورت زیر تعریف می‌شود:

$$R = \frac{\log_2 M}{n} \quad \text{bit/transmission}$$

n: طول کلمه کد ، x^n : تعداد پیام‌ها یا اندیس‌های پیام M

- نرخ قابل دسترس (achievable rate)

نرخ R قابل دسترس است هرگاه دنباله‌ای از کدهای $C(2^{nR}, n)$ وجود داشته باشد که

$$C(2^{nR}, n) \equiv C(\lceil 2^{nR} \rceil, n) \qquad \lambda^{(n)} \xrightarrow[n\to\infty]{} 0$$

خاصیت کمال

خاصیت کمال برابر Supremum تمام نرخ‌های قابل دسترس روی کانال است

Supremum ≡ کوچکترین کران بالا

(کلی‌ترین تعریف خاصیت)

⟸ هر نرخ کمتر خاصیت به طول n اگر n به اندازه کافی بزرگ باشد احتمال به میزان دلخواه کم خواهد داشت.