

فصل سوم: نظریه اطلاعات

در این فصل مروار مقتصر بر مفاهیم تئوری اطلاعات خواهیم داشت.

انتقال داده

ابوفضل دیانت

آخرین ویرایش: ۲۵ آبان ۱۴۰۰ در ساعت ۱۰ و ۳۵ دقیقه

فهرست مطالب

۲	مفهوم اطلاعات
۲۰	انتروپی
۳۳	قضیه اول شانون
۴۷	قضیه دوم شانون
۷۴	انتروپی پیوسته
۹۸	مراجع
۹۹	فهرست اختصارات

واژه نامه انگلیسی به فارسی

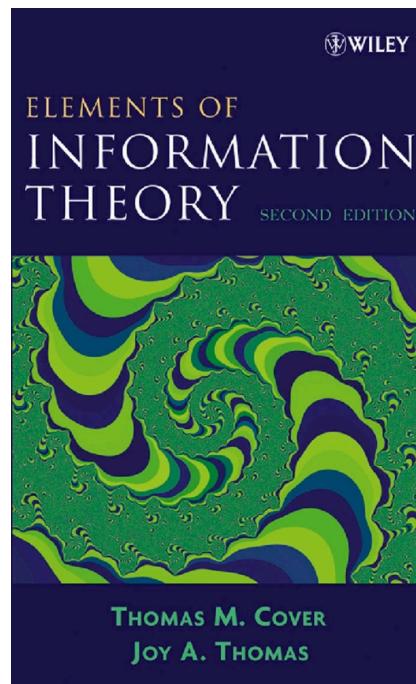
۱۰۲

واژه نامه فارسی به انگلیسی

۱۰۶

فصل اول و دوم

- [1] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Wiley, 2012.



مفهوم اطلاعات



Shannon ریاضی‌دان، مهندس الکترونیک و رمزنگار معروف آمریکایی است که به عنوان پدر نظریه اطلاعات شناخته می‌شود. او در مقاله ۱۹۴۸ خود علم نظریه اطلاعات را پایه‌گذاری می‌کند و در مقاله ۱۹۴۹ خود علم رمزنگاری را بنیان‌گذاری می‌کند. شانون در هر دو مقاله به مبحث ارسال پیام در یک سامانه مخابراتی می‌پردازد، اما با دو دیدگاه مختلف.

Shannon, Claude Elwood. “A mathematical theory of communication.” *Bell system technical journal* 27, no. 3 (1948): 379-423.

Shannon, Claude Elwood. “Communication theory of secrecy systems.” *Bell system technical journal* 28, no. 4 (1949): 656-715.



اطلاعات و ابهام دو روی یک سکه

- ۱ گاهی به جای واژه اطلاعات (Information) از واژه مقابله آن یعنی ابهام (Ambiguity) استفاده می‌شود.
- ۲ اما این دو واقعاً دو روی یک سکه و معادل همدیگر هستند.
- ۳ تا قبل از مشاهده یک پیام و یا وقوع یک حادثه، در مورد چیستی آن، ابهام وجود دارد، و بعد از رخداد آن به همان اندازه مقدار ابهام، اطلاعات بدست خواهیم آورد.
- ۴ هر پدیده هرقدر اطلاعات بیشتری داشته باشد، در صورت نداشتن آن، ابهام مانیز بیشتر است.



توجه داشته باشید که "ابهام" و "اطلاعات" معادل یکدیگرند. در این رابطه به نقل قولی از شانون توجه کنید:

"My greatest concern was what to call it. I thought of calling it 'information,' but the word was overly used, so I decided to call it 'uncertainty.' ... Von Neumann told me, 'You should call it **entropy**'".

اطلاعات چیست؟



یک حادثه به مانند A را در نظر بگیرید، مقدار اطلاعات موجود و یا ابهام باقیمانده این حادثه را با $I(A)$ نمایش می‌دهیم.

• هوای قطب شمال سرد است. میزان اطلاعات $I(A) \in \mathbb{R}^+$.

• امروز در تهران زلزله شدیدی می‌آید. میزان اطلاعات $I(B) \in \mathbb{R}^+$.

به طور حسی می‌دانیم که $I(A) < I(B)$.

• $I(A)$ به چه پارامتری بستگی دارد؟ چه ویژگی‌هایی دارد؟



اطلاعات چیست؟ (ادامه.)

☞ ویژگی‌های تابعی که قرار است اطلاعات را به صورت یک کمیت ریاضی نشان دهد:

- تابعی نامنفی است، یعنی $I(A) \in \mathbb{R}^+$.
- $I(A)$ تابعی است که وابسته به احتمال رخداد یک پدیده است. برای تاکید $I(p_A)$.
- هر چقدر امکان وقوع یک رخداد بیشتر باشد، مقدار اطلاعات یا ابهام باقیمانده کمتر خواهد بود. یعنی

تابعی است غیرافزایشی:

$$p_A \geq p_B \implies I(p_A) \leq I(p_B) \quad (1)$$

- اتفاقی که همیشه رخ می‌دهد ($p_A = 1$), برای ما اطلاعاتی ندارد یعنی $I(p_A) = 0$.
- مقدار اطلاعات دو پدیده مستقل برابر با حاصل جمع آن‌ها خواهد بود:

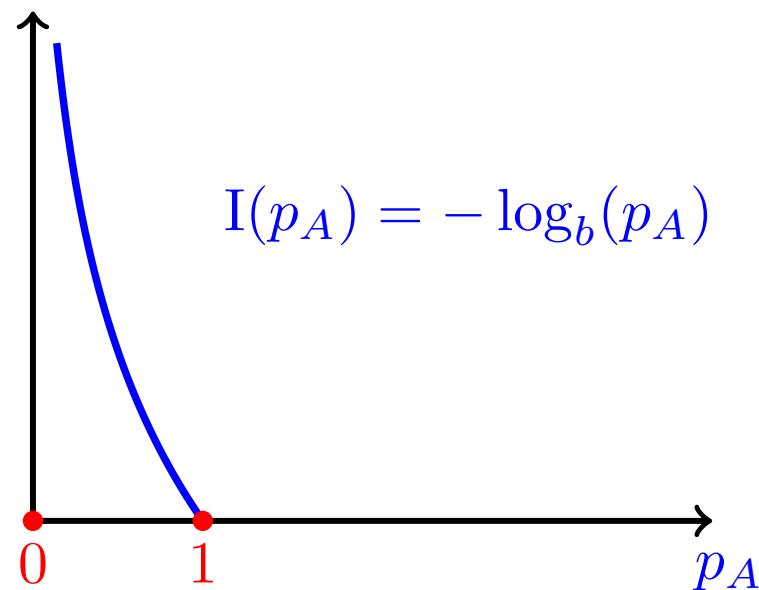
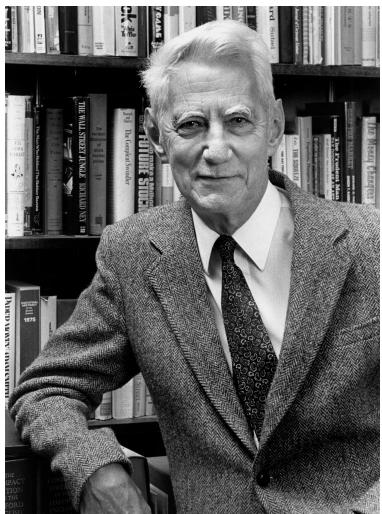
$$A \perp\!\!\!\perp B, \quad I(p_{A \cap B}) = I(p_A \times p_B) = I(p_A) + I(p_B) \quad (2)$$

اطلاعات چیست؟ (ادامه.)

☞ تنها تابعی که همه‌ی ویژگی‌های یاد شده را دارد تابع لگاریتمی است.



؟log مبنای



اطلاعات (مثال)

فرض کنید حادثه A پرتاب یک سکه سالم باشد. نتیجه پرتاب یا شیر است یا خط. صرفنظر از علم نظریه اطلاعات، نتیجه پرتاب را می‌توان با یک بیت بیان کرد. از سوی دیگر داریم:

$$I(p_A) = -\log_b\left(\frac{1}{2}\right) = \log_b(2).$$



اگر مبنای لگاریتم را 2 در نظر بگیریم، می‌توان یک قرابت بین مفهوم بیت و نظریه اطلاعات ایجاد کرد.

$$I(p_A) = \log_2(2) = 1 \text{ bit}.$$

اطلاعات - مثال مسابقه ۲۰ سوالی



در یک مسابقه ۲۰ سوالی، مجری به صورت تصادفی از یک فرهنگ لغت با ۱00000 واژه انتخاب می‌کند.

چه تعداد سوال نیاز است تا بتوان مطمئن شد که شرکت‌کننده در مسابقه حتماً پیروز می‌شود؟



اطلاعات - مثال مسابقه ۲۰ سوالی (ادامه)

برطبق تعریف شانون از اطلاعات، داریم:

$$I(p_A) = -\log_2 \frac{1}{100000} \approx 16.6 \text{ [bit]}$$

شانون ادعا می‌کند روشی وجود دارد که شرکت‌کننده می‌تواند با پرسیدن ۱۷ سوال حتماً در مسابقه به پیروزی برسد. اما چگونه؟

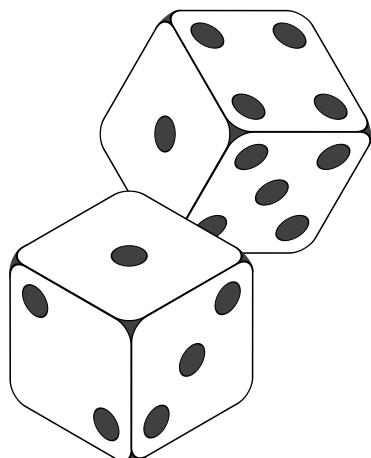
نکته ۱ نظریه اطلاعات فقط مرزها را مشخص می‌کند، ولی در برابر روش رسیدن به مرزهای یاد شده، سکوت می‌کند.

اطلاعات - پرتاب دو تاس



دو تاس را همزمان و به صورت مستقل از هم پرتاب می‌کنیم. اگر شخصی نتیجه پرتاب را به ما خبر دهد، چه مقدار اطلاعات به ما منتقل کرده است؟ و یا چه مقدار از ابهام ما را برطرف کرده است؟

برطبق تعریف اطلاعات داریم:



$$I(p_A) = -\log_2\left(\frac{1}{6 \times 6}\right) = \log_2(6 \times 6) = 5.17 \text{ [bit]}$$

به یاد آورید که میزان اطلاعات دورخداد مستقل از یکدیگر ($A_1 \perp\!\!\!\perp A_2$)، برابر با حاصل جمع اطلاعات هر یک از رخدادها است:

$$I(p_A) = I(p_{A1}) + I(p_{A2}) = -\log_2\left(\frac{1}{6}\right) - \log_2\left(\frac{1}{6}\right) = 5.17 \text{ [bit]}$$

مثال ۱

یک سکه را ۱۰ بار پرتاب می‌کنیم. اگر به ما گفته شود که در این ۱۰ پرتاب حداقل سه بار سکه شیر آمده است، چه مقدار اطلاعات منتقل شده است؟ یا به عبارت دیگر چه میزان از ابهام ما برطرف شده است؟

پاسخ: دقیق کنید که مساله بدست آوردن مقدار اطلاعات به مساله بدست آوردن احتمال پیشامد مورد نظر منتج خواهد شد. پس در مرحله نخست باید احتمال پیشامد مذکور را محاسبه کنیم.

بر تعریف احتمال می‌باشد تعداد رخدادهای مطوب را بر کل رخدادها تقسیم کنیم. در ۱۰ بار پرتاب یک سکه، تعداد کل حالات ممکنه برابر با 2^{10} خواهد بود.

از سوی دیگر منظور از این که حداقل سه بار شیر بیاید، یعنی یا هیچ بار شیر نیاید، یا یک بار، یا دو بار و در نهایت یا سه بار. در اینجا کافی است که تعداد حالت را برای هر یک از چهار حالت بیان شده، محاسبه کنیم،

پس خواهیم داشت:

$$p_A = \frac{\binom{10}{0} + \binom{10}{1} + \binom{10}{2} + \binom{10}{3}}{2^{10}}$$

در گام بعدی برای محاسبه میزان اطلاعات خواهیم داشت:

$$\begin{aligned} I(p_A) &= -\log_2 p_A = \log_2 \frac{2^{10}}{\binom{10}{0} + \binom{10}{1} + \binom{10}{2} + \binom{10}{3}} \\ &= 10 - \log_2(1 + 10 + 45 + 120) = 10 - \log_2(176) \end{aligned}$$

مثال ۲ در یک کلاس ۲۵ نفری به ما گفته شده است که حداقل دو نفر تاریخ تولد یکسانی دارند. چه میزان

اطلاعات به ما منتقل شده است؟



پاسخ: دقت کنید که با پیشامدی به نام A مواجه هستیم که در آن قرار است حداقل دو نفر تاریخ تولد یکسانی داشته باشند. برای بدست آوردن اطلاعات این پیشامد، می بایست در ابتدا احتمال رخداد آن را محاسبه کنیم. می دانیم که این پیشامد متمم حالتی است که هیچ دو نفری تاریخ تولد یکسانی نداشته باشند. پس خواهیم داشت:

$$p'_A = \frac{P_{25}^{365}}{365^{25}} = \frac{365 \times 364 \times \dots \times (365 - 25 + 1)}{365^{25}}$$

برای محاسبه اطلاعات نیز بسادگی خواهیم داشت.

$$I(p_A) = -\log_2(1 - p'_A)$$

مثال ۳

فرض کنید که یک شبکه کامپیوتری با تعداد N کاربر داریم. هر کاربر در ۱۰ درصد موارد فعال است

و در ۹۰ درصد موارد در مُد بیکار قرار دارد. به ما خبر داده شده است که در این شبکه در هر بازه زمانی بیش از ۱۱ (یا بیشتر) کاربر فعل نیستند. چه میزان اطلاعات به ما منتقل شده است.

پاسخ: به مانند قبل، برای محاسبه اطلاعات نخست باید احتمال پیشامد مورد نظر را محاسبه کنیم. می‌دانیم

که احتمال این که در هر بازه زمانی دقیقا m کاربر فعل باشد، برابر است با

$$\binom{N}{m} (0.1)^m (0.9)^{N-m}$$

این همان توزیع دوجمله‌ای است که پیشتر در درس آمار و احتمال در مورد آن خوانده‌اید. آن‌جا خواندید که احتمال این که در N بار اجرای یک آزمایش برنولی با احتمال پیروزی p ، دقیقا M بار پیروز شویم چقدر است؟

$$\binom{N}{M} p^M (1-p)^{N-M} \quad (3)$$

پس احتمال موردنظر برابر با احتمال فعال نبودن تمام کاربران، احتمال این که یک کاربر فعل باشد، احتمال

فعال بودن ۲ کاربر تا احتمال فعال بودن ۱۰ کاربر. پس خواهیم داشت:

$$p_A = \sum_{i=0}^{10} \binom{N}{i} (0.1)^i (0.9)^{N-i}$$

در نهایت نیز خواهیم داشت:

$$I(p_A) = \log_2 \frac{1}{p_A} = -\log_2 \sum_{i=0}^{10} \binom{N}{i} (0.1)^i (0.9)^{N-i}$$

مثال ۴

پادشاهی دو فرزند دارد. اگر به ما گفته شود که ولیعهد (فرزند پسر)، خواهر دارد، چند بیت اطلاعات

منتقل شده است؟

پاسخ: اگر پادشاه دو فرزند داشته باشد چیدمان پسر یا دختر بودن آنها در مجموعه $\{bb, gg, bg, gb\}$ خلاصه می‌شود. می‌خواهیم احتمال داشتن فرزند دختر برای شاه را با شرط داشتن فرزند پسر بیابیم. پس اگر پیشامد B بیانگر داشتن فرزند پسر باشد، خواهیم داشت:

$$P(G|B) = \frac{P(G \cap B)}{P(B)} = \frac{\frac{2}{4}}{\frac{3}{4}} = \frac{2}{3}$$

در نهایت نیز با این احتمال می‌توان به سادگی میزان اطلاعات را محاسبه کرد.

اِنْتِرُوپُوِيٰ

إنتروپی (Entropy) (مثال)

- یک سکه اریب را در نظر بگیرید، به طوری که احتمال شیر آمدن $p_H = 0.8$ باشد.
- اگر به ما این خبر داده شود که سکه شیر آمده، به مقدار $I(p_H)$ اطلاعات منتقل می‌شود.

$$I(p_H) = -\log_2(0.8) = 0.32 \text{ [bit]}$$

- اگر به ما این خبر داده شود که سکه خط آمده، به مقدار $I(p_T)$ اطلاعات منتقل می‌شود.

$$I(p_T) = -\log_2(0.2) = 2.32 \text{ [bit]}$$

- در صورتی که نتیجه پرتاب گفته شود، به صورت میانگین H بیت اطلاعات منتقل می‌شود.

$$H = p_H \log_2 \frac{1}{p_H} + p_T \log_2 \frac{1}{p_T} = 0.8 \times 0.32 + 0.2 \times 2.32 = 0.72 \left[\frac{\text{bit}}{\text{symbol}} \right]$$

مفهوم انتروپی

فرض کنید که یک منبع اطلاعات (Information Source) شروع به تولید پیام بکند.

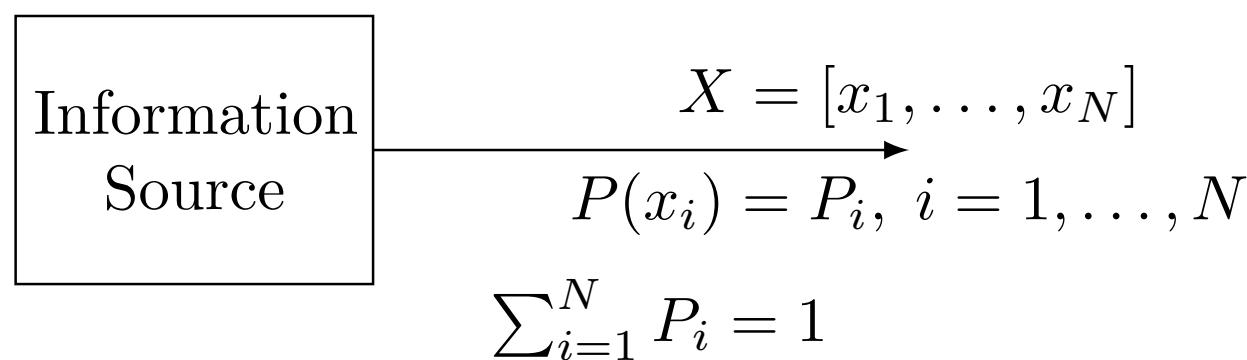
هر پیام از اجزایی (حروف، ارقام و به طور کلی سمبل) تشکیل شده است، که ما آنها را الفبای منبع می‌نامیم.

مثلا در یک نوشتار انگلیسی $\{A, B, C, \dots, Z\}$ ، یا در یک تصویر خاکستری (Gray Scale Image) هشت بیتی

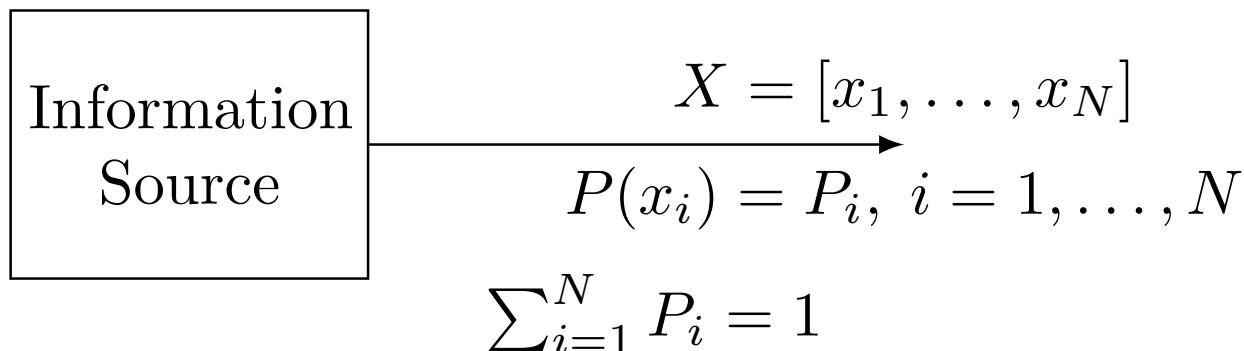
رنگ یک پیکسل $\{s | s \in \mathbb{N}, 0 \leq s \leq 255\}$ و

به طور کلی خروجی یک منبع اطلاعات، ماهیت تصادفی دارد. یعنی هر سمبل منبع با یک احتمال معین

رخ می‌دهد.



مفهوم انتروپی (ادامه.)



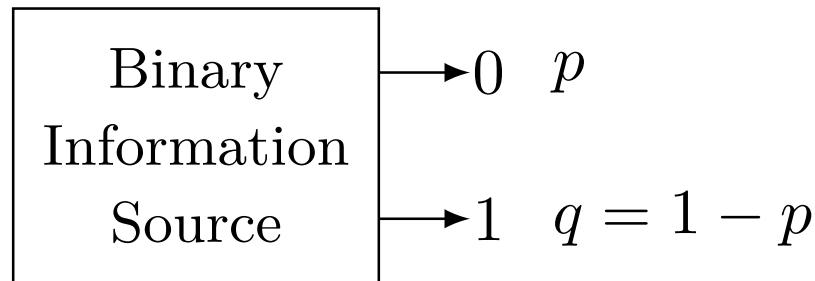
اگر $I(x_i)$ بیانگر میزان اطلاعات برای پیشامد x_i بود. انتروپی (Entropy)، بیانگر متوسط اطلاعات

تعريف ۱

یا ابهام مربوط به کل پیشامدهای خروجی منبع اطلاعات است.

$$H(X) = \sum_{i=1}^N p_i I(p_i) = \sum_{i=1}^N p_i \log_2 \frac{1}{p_i} = - \sum_{i=1}^N p_i \log_2(p_i) \quad \left[\frac{\text{bit}}{\text{symbol}} \right] \quad (4)$$

إنتروپی (مثال)



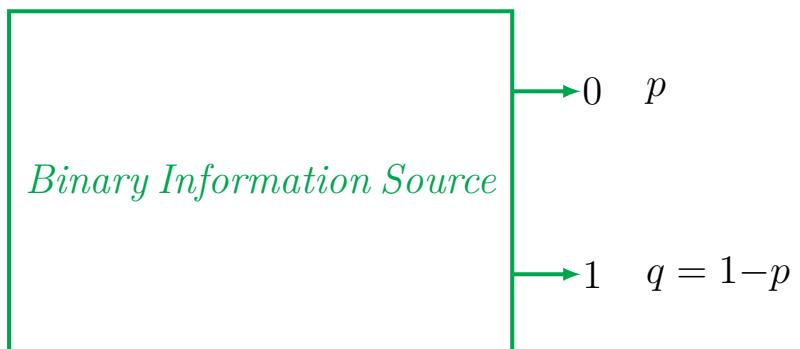
یک منبع اطلاعات دودویی را در نظر بگیرید. الفبای این منبع مجموعه $\{0, 1\}$ است. صفر با احتمال p رخ می‌دهد و ۱ با احتمال $.q = 1 - p$ رخ می‌دهد.

$$H(X) = \sum_{i=1}^2 p_i I(p_i) = - \sum_{i=1}^2 p_i \log_2(p_i) = -p \log_2 p - (1-p) \log_2(1-p) \quad (5)$$

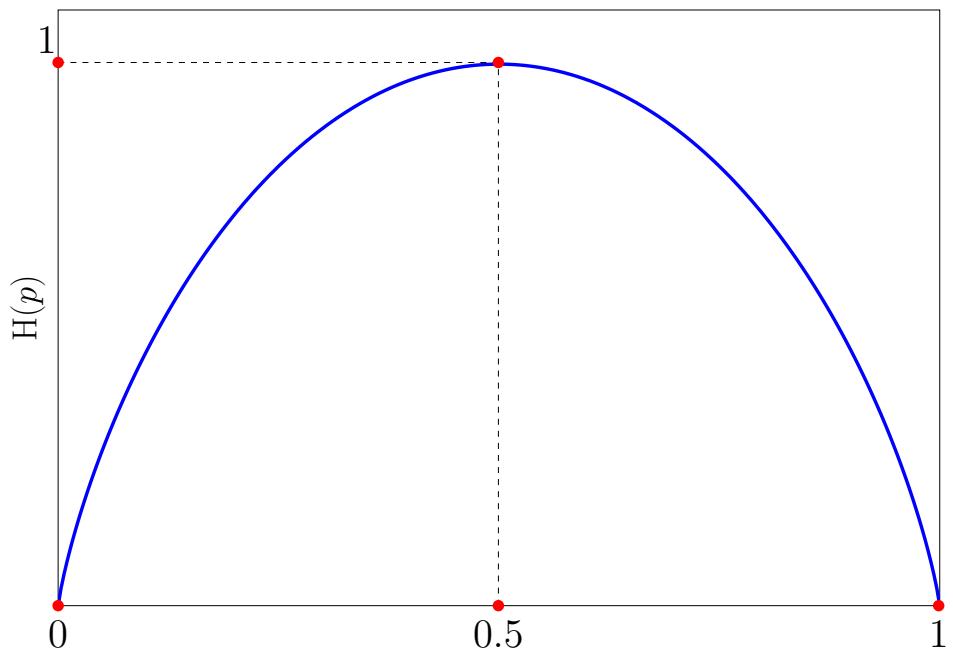
به مقدار $H(X)$ در رابطه فوق، اصطلاحاً تابع إنتروپی دودویی (Binary Entropy Function) گفته می‌شود و آن را با نماد $H_b(p)$ نشان می‌دهیم. واضح است که $H_b(p) = H_b(1-p)$ خواهد بود.

إنتروپی (ادامه.)

نمودار إنتروپی یک منبع دودویی ($H_b(p)$) بر حسب احتمال p .



$$H_b(p) = -p \log_2 p - (1 - p) \log_2(1 - p)$$

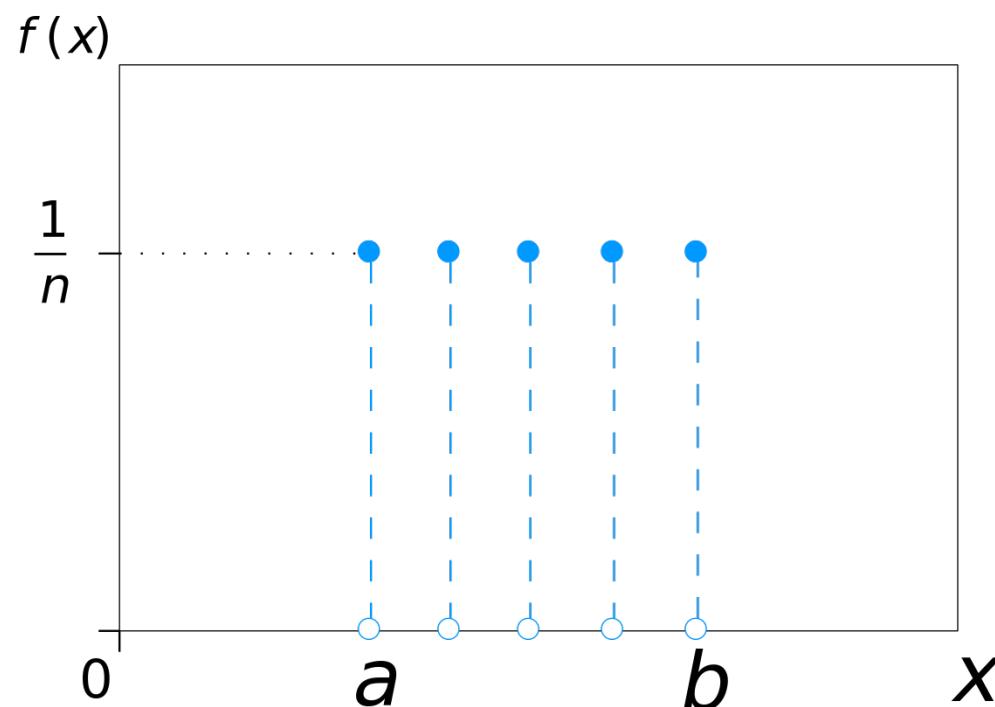


بیشینه مقدار انتروپی

که بیشینه مقدار انتروپی چه زمانی رخ می‌دهد؟ بیشینه مقدار انتروپی زمانی رخ می‌دهد که تمامی سمبول‌ها

هم احتمال باشد. یعنی $p_i = \frac{1}{n}$

$$H(X) = - \sum_{i=1}^n p_i \log_2(p_i) = - \sum_{i=1}^n \frac{1}{n} \log_2\left(\frac{1}{n}\right) = \log_2(n)$$



مثال ۵

Alice دو تاس را پرتاب می‌کند. او سپس مجموع نتایج را طی پیامی به اطلاع Bob می‌رساند. چه

مقدار إنتروپی در این پیام مبادله شده است؟

پاسخ: می‌دانیم که مجموع دو تاس عددی است بین ۲ تا ۱۲. از سوی دیگر می‌دانیم احتمال این که مجموع دو

تاس عدد ۲ شود برابر با $\frac{1}{6} \times \frac{1}{6} = \frac{1}{36}$ است. به همین روش احتمال این که مجموع دو تاس ۳ شود نیز برابر است با

$$\frac{1}{6} \times \frac{1}{6} + \frac{1}{6} \times \frac{1}{6} = \frac{2}{36}$$

چرا؟ به این علت که موقعی مجموع دو تاس برابر با ۳ خواهد شد که تاس اول برابر با ۲ و تاس دوم برابر با ۱ شود، و

{(1, 3), (3, 1), (2, 2)} بر عکس. همین طور می‌توان ادامه داد. مثلا در صورتی که دو تاس یکی از اعضای مجموعه

شود مجموع دو تاس برابر با خواهد شد. با کمی دقت می‌توان دریافت که احتمال این که مجموع دو تاس برابر با

۴ شود برابر با $\frac{3}{36}$ است، و همین طور الی آخر.

از سوی دیگر می‌دانیم که هر انتروپی برابر است با میانگین اطلاعات هر یک از پیشامدهای ذکر شده. پس

خواهیم داشت:

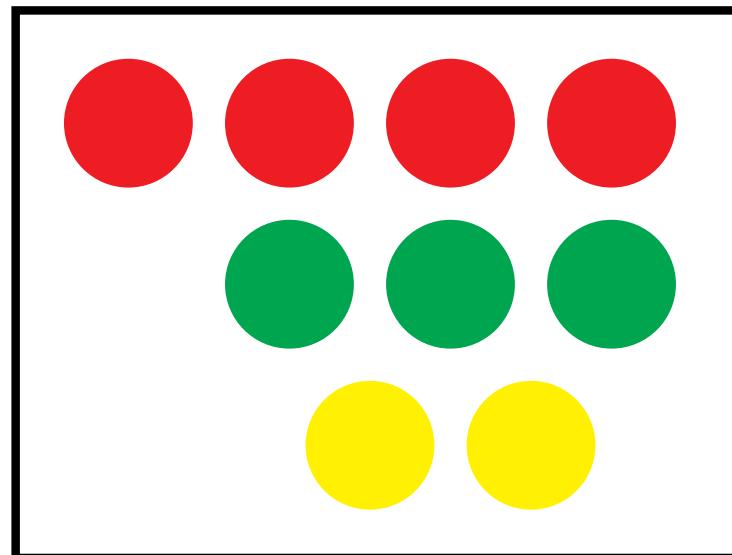
$$\begin{aligned} H(X) &= -\frac{1}{36} \log_2 \frac{1}{36} - \frac{2}{36} \log_2 \frac{2}{36} - \frac{3}{36} \log_2 \frac{3}{36} - \frac{4}{36} \log_2 \frac{4}{36} - \dots \\ &\quad - \frac{6}{36} \log_2 \frac{6}{36} - \frac{5}{36} \log_2 \frac{5}{36} - \frac{4}{36} \log_2 \frac{4}{36} - \dots - \frac{1}{36} \log_2 \frac{1}{36} \\ &= 3.274402 \end{aligned}$$

مثال ۶

یک جعبه حاوی چهار مهره قرمز، سه مهره سبز و دو مهره زرد همسان را در نظر بگیرید. اگر به تصادف

یک مهره از این جعبه خارج کنیم، ورنگ مهره حاصل شده را به شما اطلاع دهیم، به صورت میانگین چه میزان

اطلاعات به شما منتقل کردیم؟



پاسخ: رنگ مهره بیرون آمده قرمز، سبز یا زرد است. ابتدا باید احتمال انتخاب هر یک از رنگ‌های یاد شده را محاسبه کنیم. سپس میانگین اطلاعات هر یک از پیشامدهای یاد شده را به عنوان H محاسبه می‌کنیم. براحتی خواهیم داشت:

$$p_R = \frac{4}{9} \implies I(p_R) = \log_2 \frac{9}{4}$$

$$p_G = \frac{3}{9} \implies I(p_R) = \log_2 \frac{9}{3}$$

$$p_B = \frac{2}{9} \implies I(p_R) = \log_2 \frac{9}{2}$$

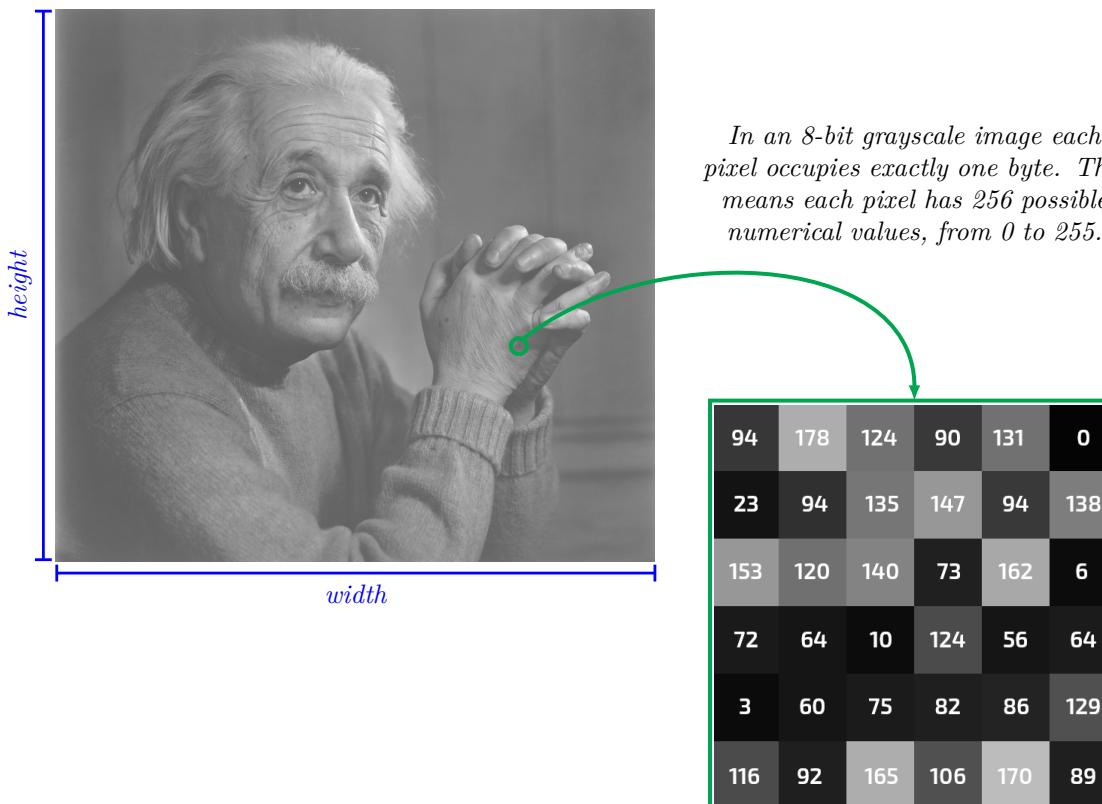
می‌دانیم که انتروپی میانگین اطلاعات پیشامدهای ذکر شده است.

$$H(X) = \frac{4}{9} \log_2 \frac{9}{4} + \frac{3}{9} \log_2 \frac{9}{3} + \frac{2}{9} \log_2 \frac{9}{2}$$

مثال ۷

هر پیکسل موجود در یک تصویر خاکستری (Gray Scale Image) هشت بیتی با ابعاد 600×600

دارای سطح روشنایی مشخصی است. میزان روشنایی هر پیکسل چه میزان اطلاعات دارد؟

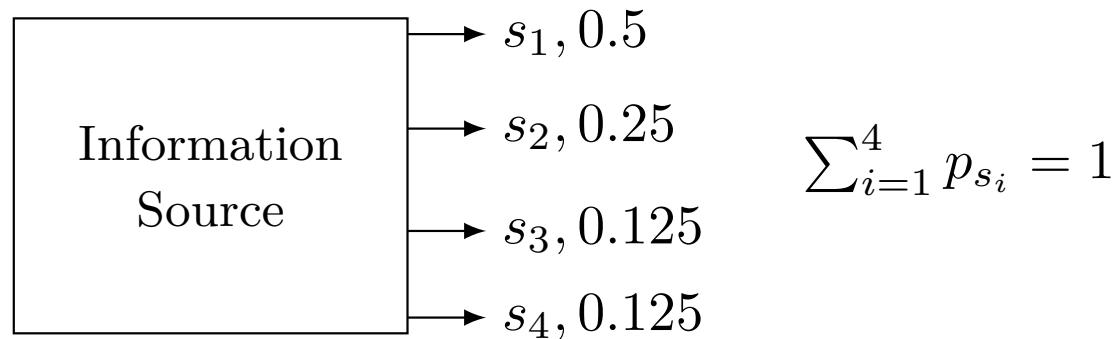


پاسخ: رنگ یک پیکسل از تصویر در طیف خاکستری رنگ دارای 256 حالت ممکن است که از سیاه تا سفید و در 256 سطح تغییر می‌کند. لذا می‌توانیم آنرا یک متغیر تصادفی با توزیع یکنواخت روی ۲۵۶ مقدار ممکن در نظر بگیریم. به این ترتیب اندازه اطلاعاتی که با دانستن سطح روشنایی یک پیکسل از تصویر به دست می‌آید عبارت است از

$$H(X) = -\log_2\left(\frac{1}{256}\right) = 26.45 \text{ [bit]}$$

قہبہ اول شناور

مثالی از انتروپی



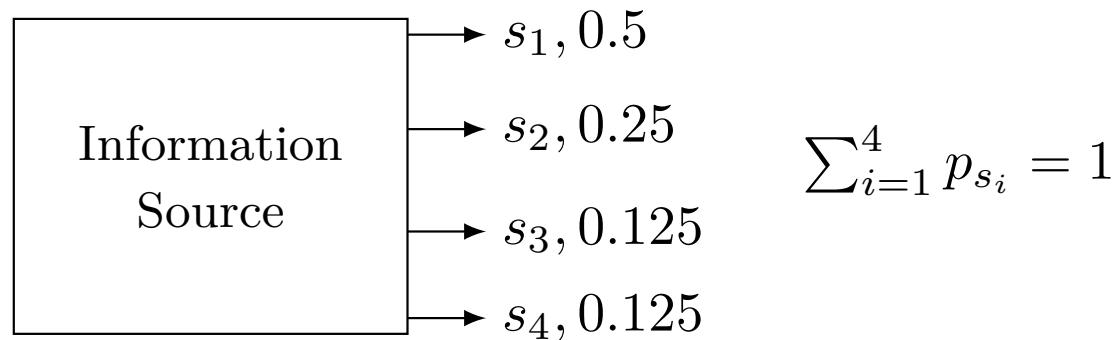
☞ یک منبع اطلاعات با الفبای $\{s_1, s_2, s_3, s_4\}$ را در نظر بگیرید. در ساده‌ترین روش برای ارسال هر سمبول این منبع مجبور هستیم تا 2 بیت تخصیص دهیم.

$$s_1 : 00 \quad s_2 : 10 \quad s_3 : 01 \quad s_4 : 11$$

☞ برای ذخیره‌سازی 1000 سمبول، باید 2000 بیت مصرف شود.
☞ به عنوان مثال، فرض کنید که منبع می‌خواهد دنباله زیر را ارسال کند.

$$s_1s_1s_4s_3s_1s_2s_1s_2 \implies 00\ 00\ 11\ 01\ 00\ 10\ 00\ 10$$

مثالی از انتروپی (ادامه.)



در ادامه مثال قبل اجازه دهید مقدار انتروپی منبع یاد شده را محاسبه کنیم:

$$\begin{aligned}
 H(X) &= - \sum_{i=1}^4 p_i \log_2 p_i \\
 &= \frac{1}{2} \log_2 2 + \frac{1}{4} \log_2 4 + \frac{1}{8} \log_2 8 + \frac{1}{8} \log_2 8 = 1.75 \left[\frac{\text{bit}}{\text{Symbol}} \right]
 \end{aligned}$$

آیا مقدار انتروپی یعنی 1.75 ایده‌ای به ما می‌دهد؟!



قضیه اول شانون

در علم نظریه اطلاعات، قضیه اول شانون و یا قضیه موسوم به قضیه کدگذاری منبع (Shannon's source) در علوم نظریه اطلاعات، قضیه اول شانون و یا قضیه موسوم به قضیه کدگذاری منبع (Shannon's source)، محدودیت حداقل فشرده سازی داده‌ها را مشخص می‌کند. (coding theorem)

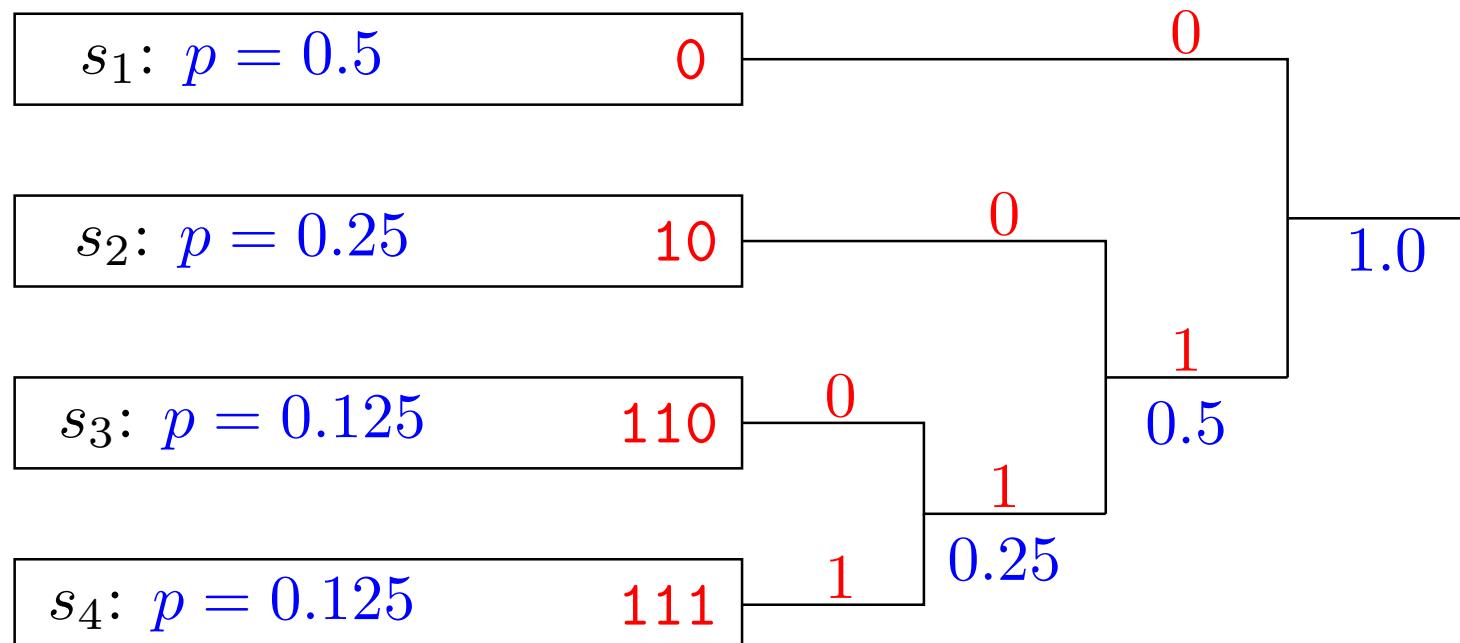
قضیه ۱ کدگذاری منبع

متغیر تصادفی با انتروپی $H(X)$ به N بیت بدون از دست دادن اطلاعات فشرده ساخت. اما اگر بیشتر فشرده‌سازی صورت پذیرد، تقریباً مسلم است که اطلاعات از دست خواهد رفت.

قضیه اول شانون (مثال)

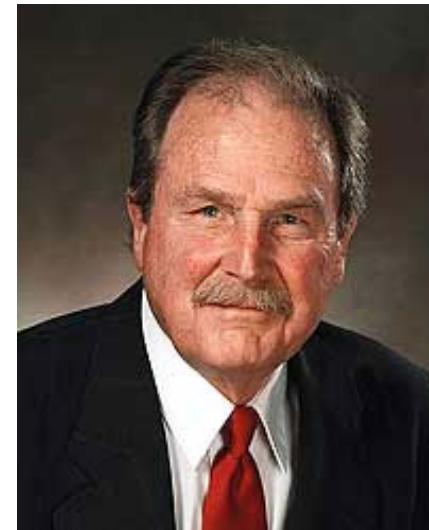
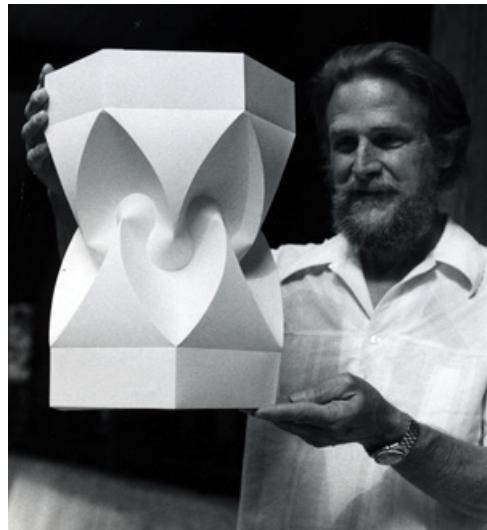
برطبق قضیه کدگذار منبع (Source Coding) در همان مثال قبلی، حتماً روش فشرده‌سازی وجود دارد که می‌توان توسط آن 1000 سمبول را بدون از دست دادن هیچ‌گونه اطلاعاتی در 1750 بیت ذخیره نمود.

اما چگونه؟ نظریه اطلاعات به این سوال پاسخ نمی‌دهد؟! روش کدگذاری هافمن.



$$\mathbb{E}[L] = (0.5 \times 1) + (0.25 \times 2) + 2 \times (0.125 \times 3) = 1.75$$

کد هافمن (Huffman Code) نوع خاصی از روش‌های کدگذاری (Encoding) است که معمولاً برای فشرده‌سازی بی‌اتلاف اطلاعات مورد استفاده قرار می‌گیرد. این روش برای نخستین بار توسط David Albert Huffman در سال ۱۹۵۲ کشف شد.

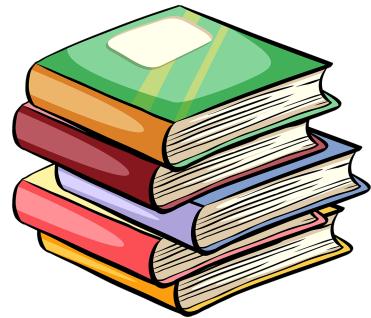


قضیه اول شانون (مثال فشرده‌سازی متن)

☞ یک کتاب تقریبا ۳۴۰ صفحه‌ای داریم که حاوی یک میلیون حرف از الفبای زبان

انگلیسی و کاراکتر فاصله است. این کتاب حاوی چه مقدار اطلاعات است؟

$$H(X) = - \sum_{i=1}^{27} \frac{1}{27} \log_2 \frac{1}{27} = \log_2 27 \approx 4.75 \quad \left[\frac{\text{bits}}{\text{character}} \right]$$



☞ برای یک میلیون کاراکتر خواهیم داشت:

$$NH(X) = 1000000 \times 4.75 \approx 573 \text{ kB} \circ\circ\circ$$



اما ما امروزه براحتی می‌توانیم یک متن یک میلیون کاراکتری را بسیار بیشتر از مقدار بدست آمده فشرده کنیم. اشکال محاسبه ما کجاست؟

قضیه اول شانون (مثال فشرده‌سازی متن-ادامه.)

☞ شاید اولین اشکال ما در این بود که فکر کردیم همه حروف انگلیسی با فرکانس یکسان در متن ظاهر می‌شوند.
اما این طور نیست:

$$p_a = 0.08167, p_b = 0.12702, p_i = 0.06966, p_m = 0.02406, p_z = 0.00074$$

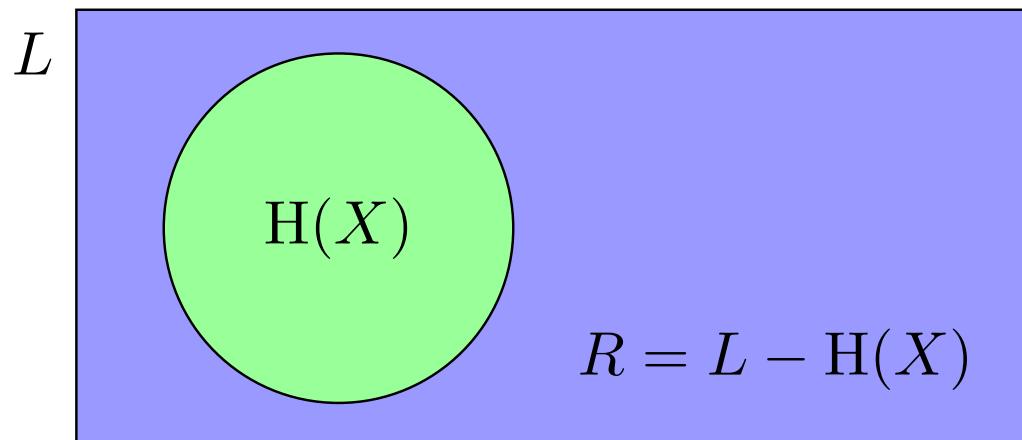
☞ با احتساب عدم یکنواختی احتمال واقع شدن حرف در متن، $H(X) = 4.219$ خواهد شد.
اما این همه ماجرا نیست، پشتسرهم قرار گرفتن حروف yx , gh و th , کلمات، جملات، مفهوم متن و

قضیه اول شانون (مثال فشرده‌سازی متن-ادامه.)

☞ در واقع اشتباه در این بود که ما برای انتروپی بیشینه مقدار آن را در نظر گرفتیم.

$$H = \sum_{i=1}^{27} \frac{1}{27} \log_2 \frac{1}{27} = \log_2 27 \approx 4.75 \quad \left[\frac{\text{bits}}{\text{character}} \right]$$

☞ شانون نشان داد که $H(X)$ برای زبان انگلیسی مقداری است بین ۰.۶ تا ۱.۳ بیت بر کاراکتر است.



قضیه اول شانون (فشردهسازی تصویر)



☞ یک تصویر خاکستری (Gray Scale Image) هشت بیتی با 800×600 را در نظر بگیرید، برای انتقال این تصویر به چند بیت اطلاعات نیاز داریم؟

$$H = \log_2 256 = 8 \quad \frac{\text{bit}}{\text{pixel}}$$

☞ کل اطلاعاتی که برای انتقال این تصویر نیاز هست:

$$600 \times 800 \times 8 = 3840000 \text{ bit} \approx 480 \text{ kB}$$

☞ اما در فشردهسازی می‌توانیم اندازه چنین تصویری را بدون از دست دادن اطلاعات حتی تا 40 kB نیز پایین آورد؟!

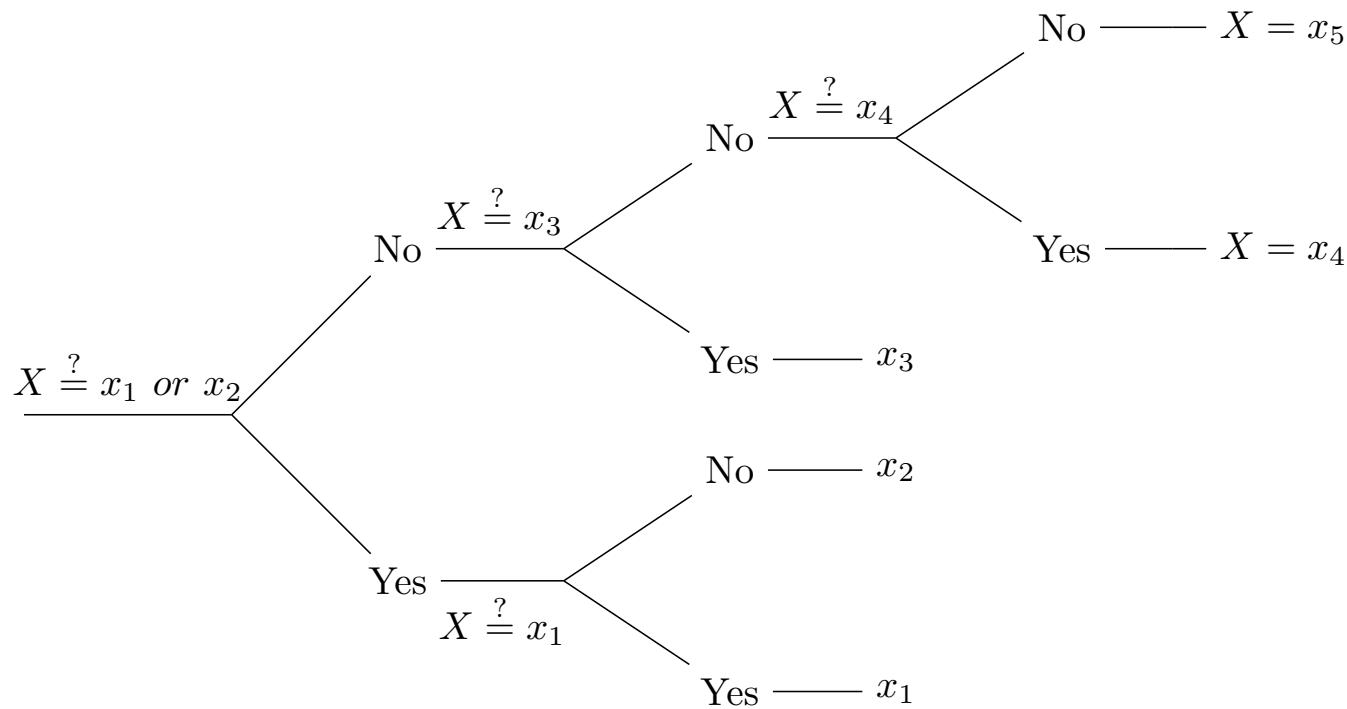
مثال ۸

احتمال‌های

X یک متغیر تصادفی (Random Variable) باشد که مقادیر آن از مجموعه $\{x_1, \dots, x_5\} = \mathcal{X}$ و با

$$p_1 = 0.3, p_2 = 0.2, p_3 = 0.2, p_4 = 0.15, p_5 = 0.15,$$

انتخاب می‌شوند. در ضمن فرض کنید تنها راه اطلاع از مقدار انتخاب شده برای متغیر تصادفی X پرسیدن سوال‌هایی که پاسخ آن «بله» یا «خیر» است، باشد. برای مثال شما می‌توانید سؤال «آیا مقدار X برابر x_1 یا x_2 است؟» را مطرح کنید و در پاسخ فقط «بله» یا «خیر» را دریافت خواهید کرد. یک روش طرح سؤال برای فهمیدن مقدار انتخاب شده در [شکل ۳](#) نمایش داده شده است و روشن است که این تنها روش موجود نیست و شما می‌توانید روش دیگری را انتخاب کنید.



شکل ۳: روشی برای طرح سؤال‌های «بله» یا «خیر» برای فهمیدن مقدار یک متغیر تصادفی

فرض کنید مقدار صحیح X برابر x_4 باشد، در این صورت با طرح سؤال $X = ? = x_1$ یا $X = ? = x_2$ پاسخ «خیر» را دریافت می‌کنیم. سپس با طرح سؤال $X = ? = x_3$ بازهم پاسخ «خیر» را دریافت می‌کنیم تا این‌که در آخر با طرح سؤال $X = ? = x_4$ پاسخ «بله» را دریافت می‌کنیم و مقدار صحیح پس از ۳ پرسش به دست می‌آید. تعداد پرسش‌های

طرح شده برای رسیدن به جواب خود یک متغیر تصادفی است که اگر X برابر x_3 یا x_2 یا x_1 باشد، مقدار آن 2 و اگر X برابر x_5 یا x_4 باشد، مقدار آن برابر 3 است. بنابراین متوسط تعداد سؤال‌های طرح شده در این روش عبارت است از

$$(0.3 + 0.2 + 0.2)2 + (0.15 + 0.15)3 = 2.3$$

این مثال ارتباط نزدیکی با کدگذاری منبع دارد، در واقع در بحث کدگذاری منبع نشان می‌دهیم که نه تنها در روش نشان داده شده در شکل ۳ بلکه با هر روش طرح سؤال دیگر نیز، متوسط تعداد پرسش‌های طرح شده نمی‌تواند از انتروپی متغیر تصادفی X کمتر باشد. در این مثال انتروپی X برابر است با

$$H(X) = -0.3 \log 0.3 - 0.4 \log 0.2 - 0.3 \log 0.15 = 2.27,$$

بنابراین به هر طریقی که سؤال‌ها را مطرح کنیم متوسط تعداد سؤال‌ها برای رسیدن به جواب صحیح از 2.27 کمتر نخواهد بود.

مثال فوق یک نمونه کامل‌تر از مثال مسابقه بیست سوالی است که پیش‌تر ذکر شد. همان‌طور که در مثال قبل ذکر شد، نظریه اطلاعات فقط به ما می‌گوید که به‌طور متوسط حداقل به چند سؤال از نوع «بله» یا «خیر»، برای رسیدن به پاسخ نیاز داریم، اما روش طرح سؤال‌ها را به ما نمی‌گوید. در واقع روش طرح سؤال موضوعی است که در نظریه کدگذاری مطالعه می‌شود.

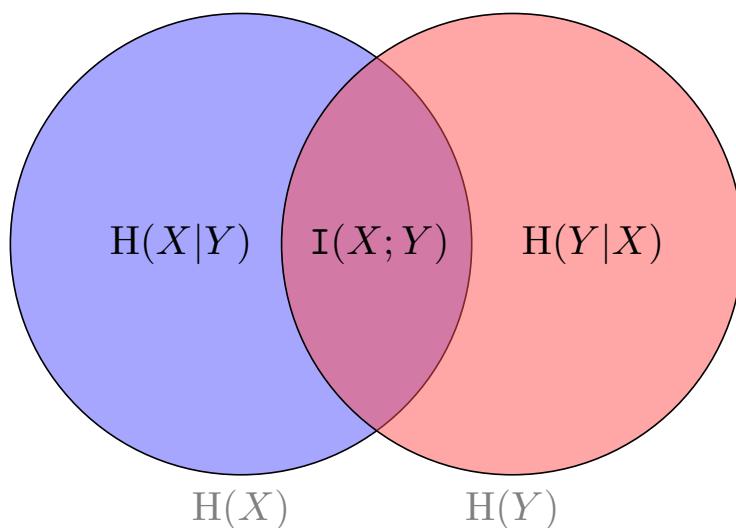
۲۹۶ قلمبیه

انتروپی توام (Joint Entropy)

فرض کنید $(X, Y) \sim P(X, Y)$ به صورت زیر تعریف می‌شود.

$$H(X, Y) = - \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} P(x, y) \log_2 P(x, y)$$

با کمی دقت به این رابطه می‌رسیم:



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

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

مثالی از انتروپی توام (Joint Entropy)

مثال ۹

احتمال توام دو متغیر تصادفی X و Y در جدول زیر ارایه شده است. مطلوب است محاسبه $H(X, Y)$ باشد.

$P(X, Y)$	$y = 0$	$y = 1$
$x = 0$	$\frac{1}{2}$	$\frac{1}{4}$
$x = 1$	0	$\frac{1}{4}$

پاسخ: با توجه به روابط مربوط به انتروپی توام براحتی داریم:

$$H(X, Y) = -\frac{1}{2} \log_2 \frac{1}{2} - \frac{1}{4} \log_2 \frac{1}{4} - 0 \log_2 0 - \frac{1}{4} \log_2 \frac{1}{4} = 1.5 \text{ [bit]}$$

مثالی از انتروپی توام (ادامه)

در ادامه همین مثال مطلوب است، محاسبه $H(X)$ و $H(Y)$. برای محاسبه این دو نیز براحتی کافی است که با استفاده از توزیع حاشیه‌ای، توزیع هر یک از متغیرهای X و Y را محاسبه کنیم.

$P(X, Y)$	$y = 0$	$y = 1$	$P(X)$
$x = 0$	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{3}{4}$
$x = 1$	0	$\frac{1}{4}$	$\frac{1}{4}$
$P(Y)$	$\frac{1}{2}$	$\frac{1}{2}$	1

باقطه به جدول فوق، براحتی خواهیم داشت:

$$H(X) = - \sum_{x \in X} P(x) \log_2 P(x) = -\frac{3}{4} \log_2 \frac{3}{4} - \frac{1}{4} \log_2 \frac{1}{4} = 0.8 \text{ [bit]}$$

$$H(Y) = - \sum_{y \in Y} P(y) \log_2 P(y) = -\frac{1}{2} \log_2 \frac{1}{2} - \frac{1}{2} \log_2 \frac{1}{2} = 1 \text{ [bit]}$$

همان طور که در این مثال مشاهده می‌کنید:

$$H(X, Y) \leq H(X) + H(Y) \implies 1.5 \leq 1.0 + 0.8 = 1.8$$

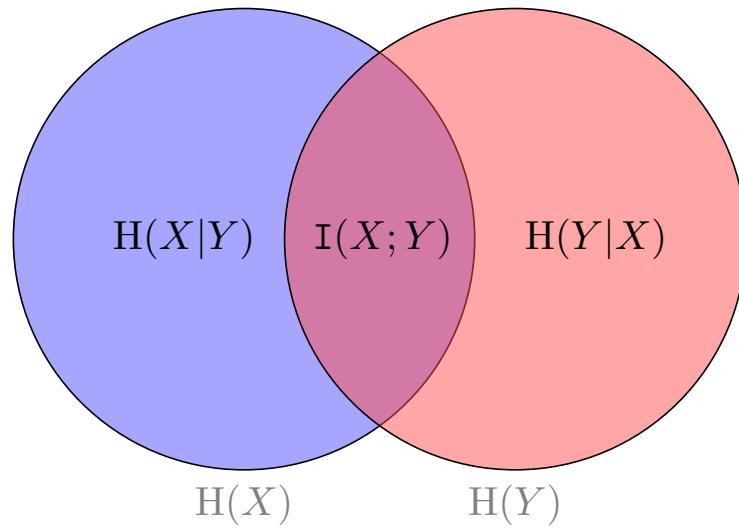
در ضمن براحتی می‌توانید مشاهده کنید که در این مثال X و Y از یکدیگر مستقل نیستند.

فرض کنید $\text{H}(Y|X)$ ، در این صورت $\text{H}(Y|X) \sim P(X, Y)$ به صورت زیر تعریف می‌شود.

$$\begin{aligned}
 \text{H}(Y|X) &= \sum_{x \in \mathcal{X}} P(x) \text{H}(Y|X=x) \\
 &= - \sum_{x \in \mathcal{X}} P(x) \sum_{y \in \mathcal{Y}} P(y|x) \log P(y|x) \\
 &= - \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} P(x, y) \log P(y|x).
 \end{aligned} \tag{6}$$

بنابراین $\text{H}(Y|X)$ بیان‌گر اندازه متوسط ابهام در مورد متغیر تصادفی Y به شرط معلوم بودن X است.

ویژگی‌های انتروپی شرطی



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

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

$$H(X|Y) \leq H(X)$$

$$H(X, Y) = H(X) + H(Y|X) = H(Y) + H(X|Y)$$

$$I(X;Y) = H(X) - H(X|Y) = H(X) - (H(X,Y) - H(Y))$$

$$I(Y;X) = H(Y) + H(X) - H(X,Y) = H(Y) - H(Y|X)$$

مثالی از انتروپی شرطی

مثال ۱۰

باتوجه به همان مثالی که پیشتر بیان شد، مطلوب محاسبه $H(Y|X)$ است.

$P(X, Y)$	$y = 0$	$y = 1$
$x = 0$	$\frac{1}{2}$	$\frac{1}{4}$
$x = 1$	0	$\frac{1}{4}$

پاسخ: در نخستین گام باید جدول زیر را تشکیل دهیم.

$P(Y X)$	$y = 0$	$y = 1$	$H(Y X=x)$	$P(X)$
$x = 0$	$\frac{2}{3}$	$\frac{1}{3}$	$H(\frac{1}{3})$	$\frac{3}{4}$
$x = 1$	0	1	$H(0)$	$\frac{1}{4}$

مثالی از انتروپی شرطی (ادامه)

$P(Y X)$	$y = 0$	$y = 1$	$H(Y X = x)$	$P(X)$
$x = 0$	$\frac{2}{3}$	$\frac{1}{3}$	$H_b(\frac{1}{3})$	$\frac{3}{4}$
$x = 1$	0	1	$H_b(0)$	$\frac{1}{4}$

☞ این سوال را به دو روش می‌توان حل نمود.

- روش اول:

$$H(Y|X) = -\frac{1}{2} \log_2 \frac{2}{3} - \frac{1}{4} \log_2 \frac{1}{3} - 0 \log_2 0 - \frac{1}{4} \log_2 1 = 0.689 \text{ [bit]}$$

- روش دوم:

$$H(Y|X) = \frac{3}{4}H(Y|X = 0) + \frac{1}{4}H(Y|X = 1) = 0.689 \text{ [bit]}$$

در توضیح روش دوم باید گفت، که بر طبق (۶) می‌توانیم رابطه انتروپی شرطی را به صورت زیر نیز بدست آوریم:

$$H(Y|X) = - \sum_{x \in \mathcal{X}} p(x) H(Y|X=x) = -P(X=0)H(Y|X=0) - P(X=1)H(Y|X=1) \quad (7)$$

به عنوان مثال برای محاسبه $H(Y|X=0)$ می‌توان به صورت زیر عمل کرد:

$$\begin{aligned} H(Y|X=0) &= - \sum_{y \in \mathcal{Y}} P(y|X=0) \log P(y|X=0) \\ &= -P(Y=0|X=0) \log P(Y=0|X=0) - P(Y=1|X=0) \log P(Y=1|X=0) \end{aligned}$$

اگر مقادیر را در رابطه فوق جایگذاری کنیم، خواهیم داشت:

$$H(Y|X=0) = - \sum_{y \in \mathcal{Y}} P(y|X=0) \log P(y|X=0) = -\frac{2}{3} \log \frac{2}{3} - \frac{1}{3} \log \frac{1}{3} = H_b\left(\frac{2}{3}\right)$$

بر طبق (۵)، می‌دانیم که مقدار فوق برابر با $H_b\left(\frac{2}{3}\right)$ است. روند مشابه روند بیان شده را برای $H(Y|X=1)$ نیز می‌توان طی کرد و به $H_b(0)$ رسید. در نهایت نیز کافی است $H_b\left(\frac{2}{3}\right)$ و $H_b(0)$ را در (۷) قرار داد.

تمرین خانگی

فرض کنید دو متغیر تصادفی A و B بیانگر گلوله‌های رنگی خارج شده از یک جعبه باشد. اگر توزیع توام

این دو متغیر به صورت زیر باشد:

جدول شماره یک، جدول توزیع توام دو متغیر تصادفی

$P(A, B)$	$A = Red$	$A = Blue$
$B = Red$	$\frac{4}{9}$	$\frac{2}{9}$
$B = Blue$	$\frac{2}{9}$	$\frac{1}{9}$

تعريف ۲

ظرفیت اطلاعاتی اگر ورودی کانال را با متغیر تصادفی X و خروجی آن را با متغیر تصادفی Y

نمایش دهیم در این صورت ظرفیت کانال عبارت است از بیشینه متوسط اطلاعات انتقال داده شده از طریق

کانال بر حسب $\frac{bits}{symbol}$ که به صورت زیر تعریف می‌شود.

$$C = \max_{p_X(x)} I(X; Y)$$

قضیه ۲ کدگذاری کانال

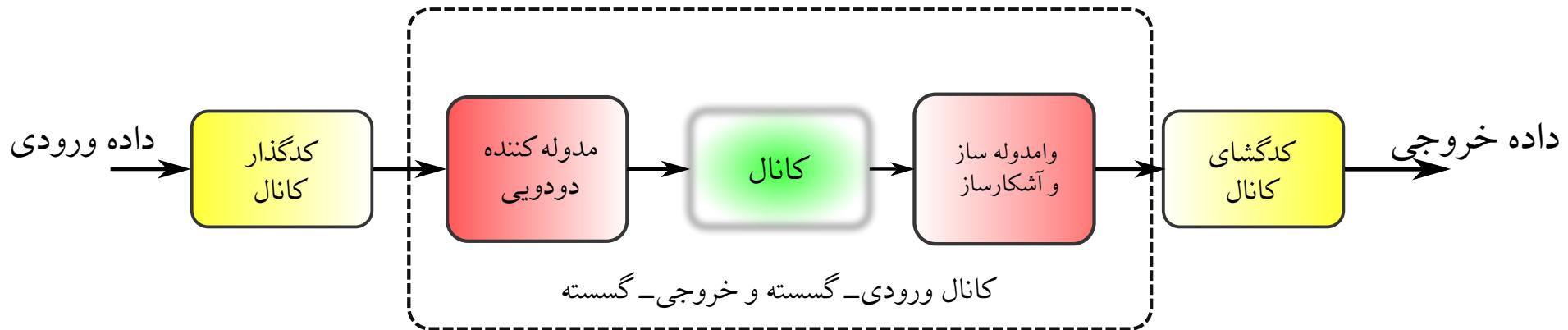
برای یک کانال گستته بدون حافظه، بیشینه نرخ اطلاعاتی که در یک کانال می‌تواند با خطای به مقدار دلخواه کوچک ارسال شود، برابر با ظرفیت کانال C است.

در علم مخابرات خروجی منبع اطلاعات (Information Source) یک فرایند تصادفی (Stochastic Process) است، چرا که در غیر این صورت، خروجی آن با احتمال ۱ قابل پیش‌بینی بوده و دیگر به مخابره و انتقال آن نیازی نبود. در عمل داده‌ها را می‌توان با استفاده از سیگنال‌های الکتریکی و از طریق کابل هم‌محور یا زوج‌سیم، یا امواج الکترومغناطیسی که در هوا منتشر می‌شوند، منتقل نمود، یا از طریق پالس‌های نوری که در فیبرهای نوری منتشر می‌شوند داده‌ها را انتقال داد. این روش‌ها در سرعت و امنیت انتقال تفاوت‌هایی با هم دارند اما وجه مشترک همه روش‌های انتقال داده این است که محیط انتقال آن‌ها دارای نویز است، عاملی که سبب می‌شود پیام دریافتی در مقصد، چیزی غیر از پیام ارسالی در مبدأ باشد. در واقع نویز یک عامل ناخواسته است که در همه کanal‌های مخابراتی وجود دارد و سبب تغییر تصادفی سیگنال دریافتی نسبت به سیگنال ارسالی می‌شود.

یک کانال مخابراتی به صورت کلی بر اساس مجموعه ورودی‌های ممکن X ، مجموعه خروجی‌های ممکن Y ، مدل می‌شود. کانال را بی‌حافظگی گوییم، هرگاه خروجی کانال در هر لحظه فقط به ورودی کانال در همان لحظه وابسته باشد و از ورودی‌ها در لحظات قبل مستقل باشد. خطای زمانی رخ می‌دهد که $Y \neq X$ باشد. در ادامه می‌خواهیم به سوال زیر پاسخ دهیم

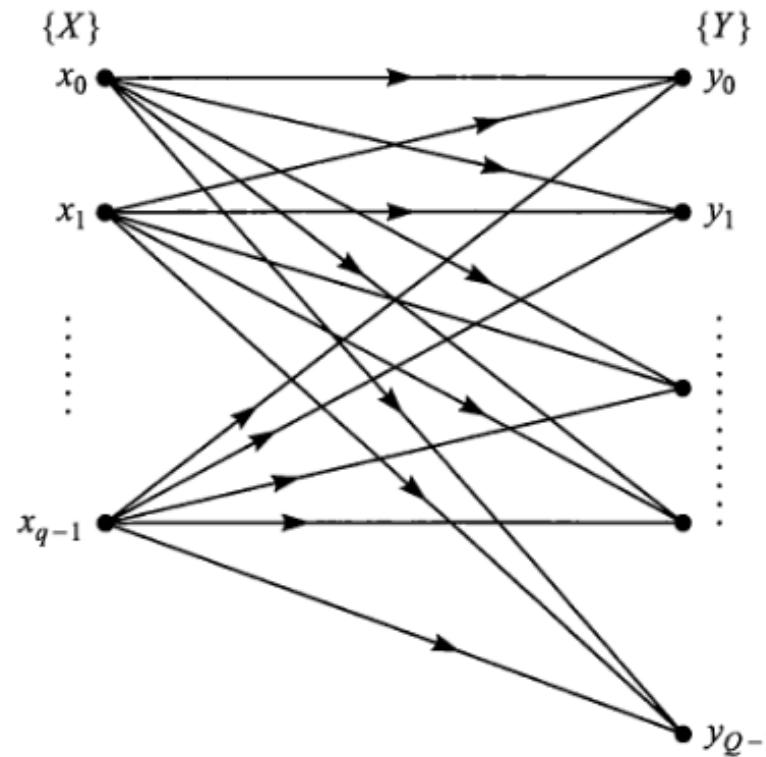
فرض کنید می‌خواهیم پیام‌هایی را از طریق یک کانال (که در آن بعضی از نمادها ممکن است تحریف شوند) برای گیرنده‌ای بفرستیم. آهنگ ماکسیمال انتقال پیام به‌ نحوی که گیرنده بتواند پیام اصلی را با احتمال خطای به اندازه دلخواه کوچک، بازیابی کند چقدر است؟

کanal گسته بدون حافظه (Discrete Memoryless Channel) که به اختصار آن را با DMC (Discrete Mem- oryless Channel) نمایش می‌دهیم، کانالی است بدون حافظه که الفبای ورودی و خروجی آن یعنی به ترتیب \mathcal{X} و \mathcal{Y} مجموعه‌هایی شمارا (یا گسته) باشند. کanal شکل زیر مرکب از مدوله‌کننده و وامدوله ساز را در نظر بگیرید.



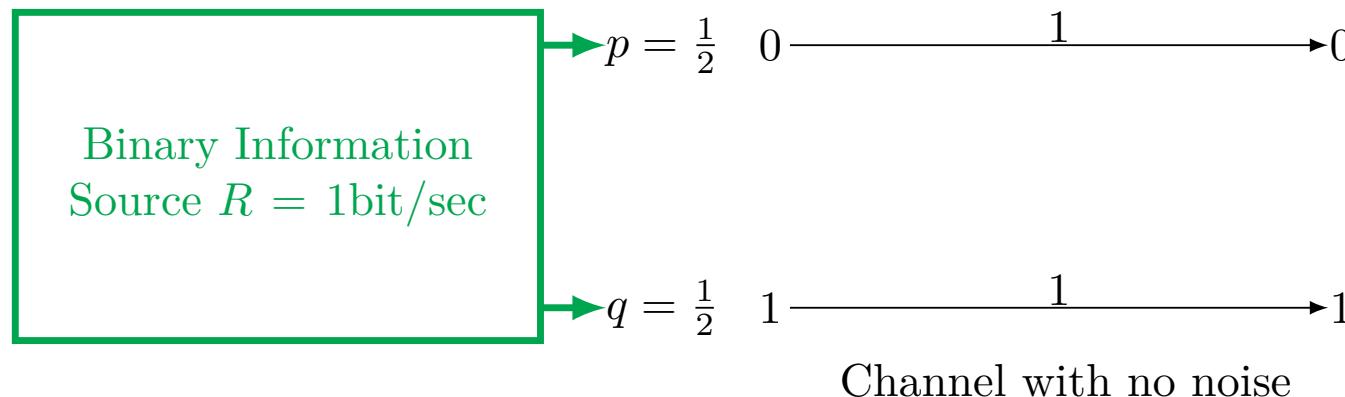
فرض کنید در این کanal از مجموعه شکل موج‌های تولیدی توسط مدولاتور یک مجموعه M عضوی و مجموعه الفبای دریافتی در آشکارساز یک مجموعه Q عضوی باشد و برای مدولاسیون از یک روش بدون حافظه استفاده کنیم، یعنی شکل موج نسبت داده شده به هر سمبول ورودی مدوله‌کننده تنها به سمبول ورودی در آن لحظه

بستگی داشته و مستقل از سمبول‌های ورودی در سایر لحظات باشد. شکل زیر، یک نمایش بصری از این DMC است.



شکل ۴: مدل نظریه اطلاعاتی یک کانال گسته بدون حافظه

کانال دودویی بدون نویز

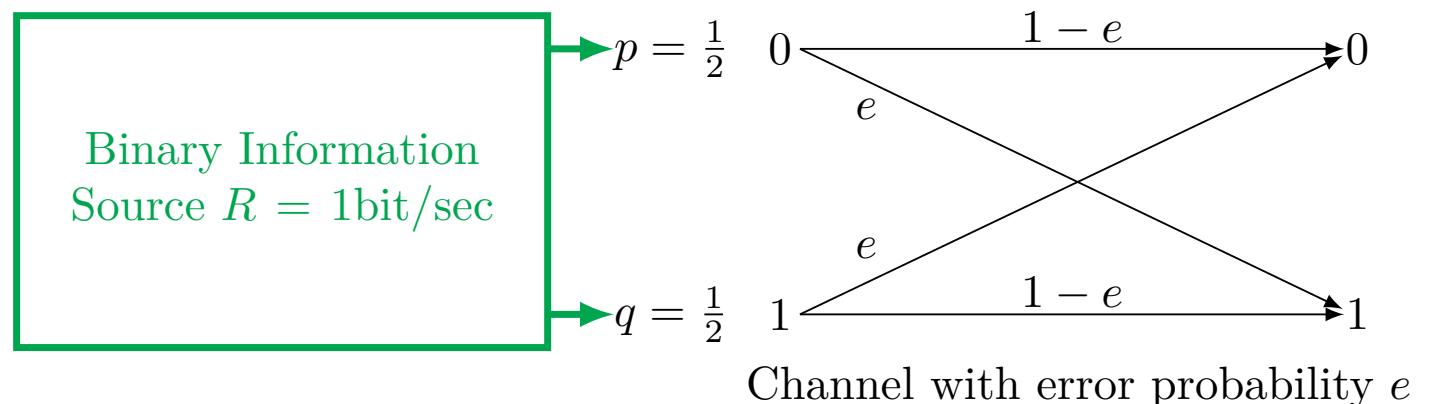


- ☞ کانالی را در نظر بگیرید که ورودی‌های دودی آن دقیقاً در خروجی بازتولید شوند، هیچ‌گونه خطایی (نویزی) در انتقال رخ ندهد.
- ☞ با توجه به این‌که در این‌حالت $H(X|Y) = 0$ لذا $H(X) = H(Y)$ است.

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

- ☞ بنابراین بیشینه $I(X;Y)$ برابر $\log_2 2 = 1(\frac{\text{bits}}{\text{symbol}})$ به‌دست می‌آید.

محاسبه ظرفیت برای کانال مخابراتی ساده



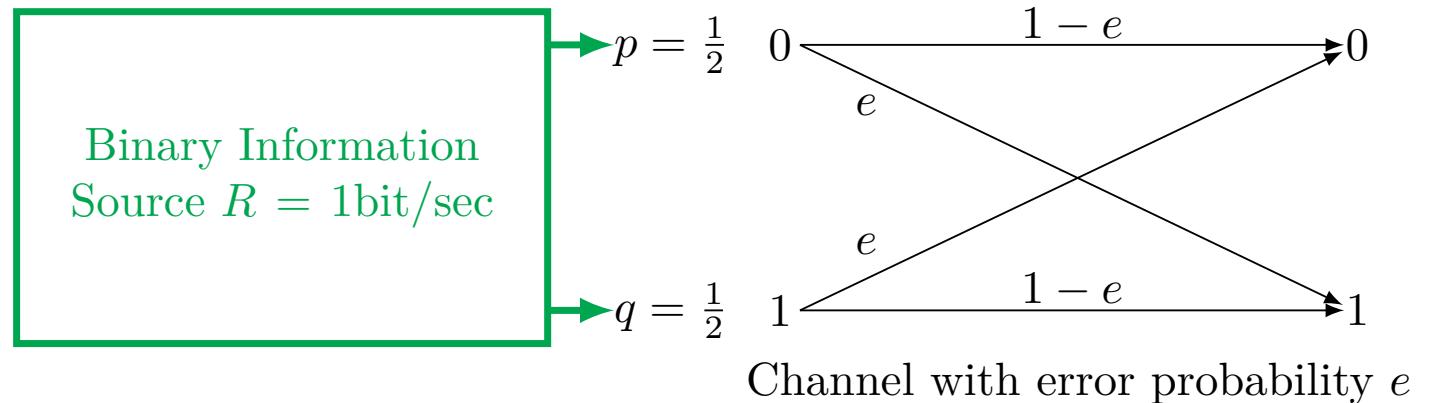
برای محاسبه ظرفیت کانال داریم:

$$C = \max_{p_X(x)} I(X; Y)$$

از سوی دیگر می‌دانیم که $I(Y; X)$ برابر با مقدار ابهام باقیمانده قبل و بعد از دریافت Y است (Leakage).

$$I(Y; X) = H(Y) + H(X) - H(X, Y) = H(Y) - H(Y|X)$$

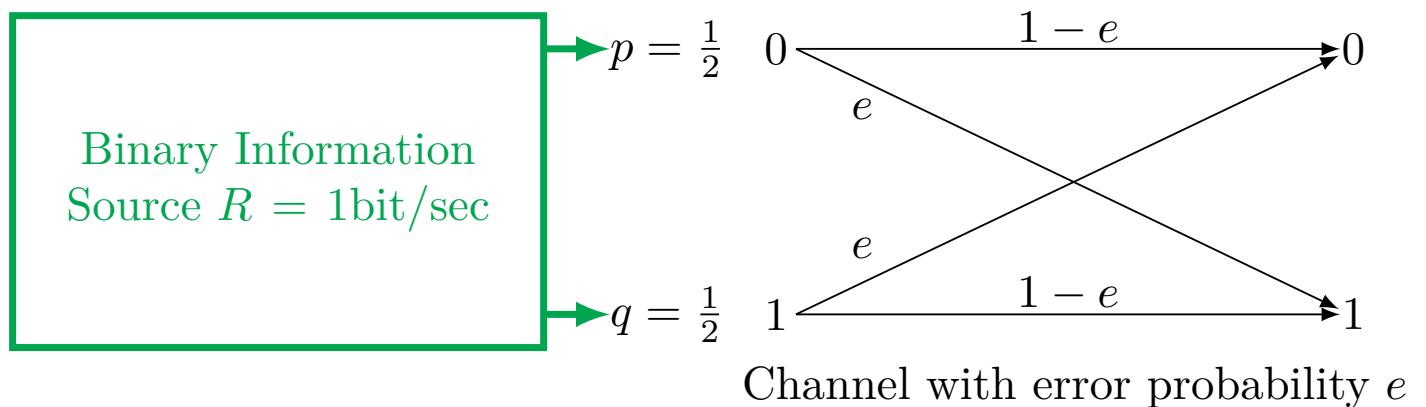
محاسبه ظرفیت برای کانال دودویی نویزدار (ادامه)



:H(X) محاسبه مقدار

$$\begin{aligned} H(X) &= -P(X = 0) \log_2 P(X = 0) - P(X = 1) \log_2 P(X = 1) \\ &= -\frac{1}{2} \log_2 \frac{1}{2} - \frac{1}{2} \log_2 \frac{1}{2} = 1 \text{ [bit]} \end{aligned}$$

محاسبه ظرفیت برای کانال دودویی نویزدار (ادامه)



برای محاسبه $H(Y)$ ابتدا باید $P(Y)$ را محاسبه کرد. در نهایت

$$P(Y = 0) = P(X = 0)P(Y = 0|X = 0) + P(X = 1)P(Y = 0|X = 1)$$

$$= \frac{1}{2} \times (1 - e) + \frac{1}{2}e = \frac{1}{2}$$

$$P(Y = 1) = P(X = 0)P(Y = 1|X = 0) + P(X = 1)P(Y = 1|X = 1)$$

$$= \frac{1}{2}e + \frac{1}{2} \times (1 - e) = \frac{1}{2}$$

محاسبه ظرفیت برای کانال دودویی نویزدار (ادامه)

محاسبه اطلاعات متقابل (Mutual Information) 

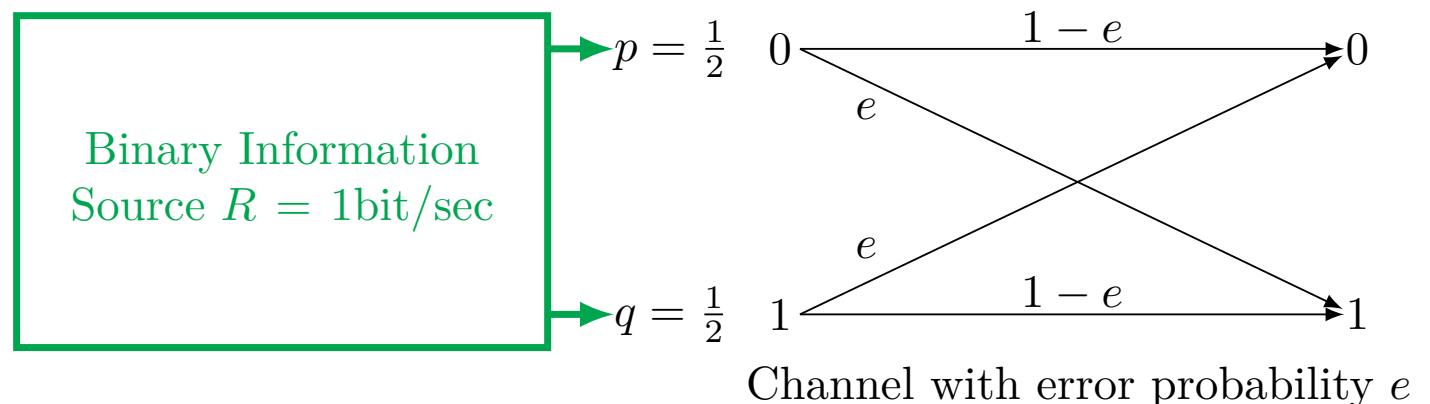
P(X, Y)	y = 0	y = 1	P(X)
x = 0	$\frac{1-e}{2}$	$\frac{e}{2}$	$\frac{1}{2}$
x = 1	$\frac{e}{2}$	$\frac{1-e}{2}$	$\frac{1}{2}$
P(Y)	$\frac{1}{2}$	$\frac{1}{2}$	1

$$\begin{aligned} H(X, Y) &= - \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} P(x, y) \log_2 P(x, y) \\ &= 1 - (1 - e) \log_2(1 - e) - e \log_2 e = 1 + H_b(e) \end{aligned}$$

تابع انتروپی دودویی (Binary Entropy Function) را هم به یاد آورید: 

$$H_b(p) = -p \log_2 p - (1 - p) \log_2(1 - p)$$

محاسبه ظرفیت برای کانال دودویی نویزدار (ادامه)



در نهایت براحتی خواهیم داشت:

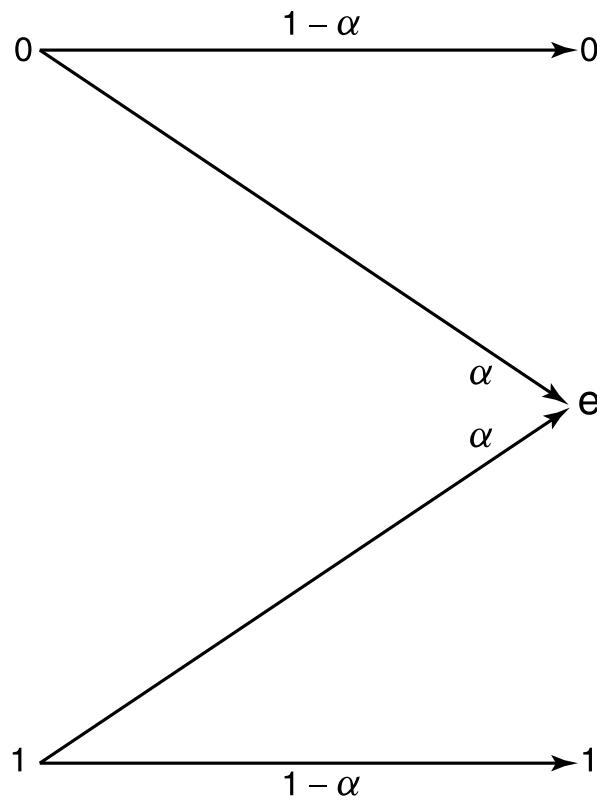
$$I(Y;X) = H(Y) + H(X) - H(X,Y) = 1 + 1 - 1 - H_b(e) = 1 - H_b(e)$$

$$C = 1 - H_b(e) = 1 + e \log_2 e + (1 - e) \log_2(1 - e)$$

۴ چند حالت حدی

- $e = 1$ یا $e = 0$: ظرفیت کانال برابر با 1 بیت است.
- $e = \frac{1}{2}$: ظرفیت کانال برابر با صفر است.
- اگر $e = \frac{1}{4}$ باشد، آن‌گاه $C = 0.188$ خواهد شد.
از این‌که $P_e \rightarrow 0$ ، آیا منظور این است که هر بیت را شش بار تکرار کنیم، احتمال خطا $C = 0.188 = \frac{k}{n}$ 
- خیر، قطعاً روش‌هایی وجود دارد که به این نرخ دست‌یابد، اما نه به این سادگی.

مثال ۱۱ نوع دیگری از کanal دودویی متقارن که در آن برخی از بیت‌ها بجای خط‌ها در انتقال اصلاً به مقصد نمی‌رسند، کanal دودویی همراه با محوشدگی است که در شکل ۵ نمایش داده شده است.



شکل ۵: کanal دودویی همراه با محوشدگی

در این کanal بیت ارسالی با احتمال α به مقصد نرسیده و محو می‌شود و با احتمال $\alpha - 1$ ، با صحت کامل به مقصد می‌رسد. البته گیرنده می‌داند کدام بیت‌ها به مقصد نمی‌رسند، یعنی از شماره بیتی که به دست وی نرسیده است اطلاع دارد ولی از مقدار آن بی‌اطلاع خواهد بود. ظرفیت کanal دودویی همراه با محوشگی را به صورت زیر محاسبه می‌کنیم.

$$\begin{aligned} C &= \max_{p(x)} I(X; Y) \\ &= \max_{p(x)} (H(Y) - H(Y|X)) \\ &= \max_{p(x)} H(Y) - H(\alpha). \end{aligned}$$

مجموعه الفبای ورودی کanal برابر $\{0, 1\}$ و مجموعه الفبای خروجی کanal برابر $\{0, e, 1\}$ است. فرض کنید $\Pr(X = 1) = \pi$ در این صورت رابطه زیر برقرار است.

$$H(Y) = H((1 - \pi)(1 - \alpha), \alpha, \pi(1 - \alpha)) = H(\alpha) + (1 - \alpha)H(\pi).$$

$$\begin{aligned}
 C &= \max_{p(x)} H(Y) - H(\alpha) \\
 &= \max_{\pi} (1 - \alpha)H(\pi) + H(\alpha) - H(\alpha) \\
 &= \max_{\pi} (1 - \alpha)H(\pi) \\
 &= 1 - \alpha,
 \end{aligned}$$

و ظرفیت به ازای $\frac{1}{2} = \pi$ به دست می‌آید.

شهود ما از ظرفیت در کانال دودویی همراه با محوش‌گی بیان گر این است که اگر n بیت روی این کانال ارسال شود، αn بیت محو و $(1 - \alpha)n$ بیت با صحت به مقصد می‌رسند، بنابراین حداکثر تعداد بیت‌هایی که می‌توانیم بازیابی کنیم برابر $n(1 - \alpha)$ بیت، و در نتیجه ظرفیت کانال، حداکثر برابر با $n(1 - \alpha)$ است. امکان دست‌یابی به این نرخ انتقال، بدیهی نیست، ولی قضیه دوم شانون دست‌یابی به این نرخ انتقال را تضمین می‌کند.

در بسیاری از کانال‌های عملی، فرستنده، بازخوردهایی از گیرنده دریافت می‌کند و انتقال داده صرفاً یک طرفه نیست. در کانال دودویی همراه با محوشدگی دارای بازخورد، اگر گیرنده یک بیت را دریافت نکند، درخواست ارسال مجدد آن بیت را به فرستنده، به عنوان بازخورد ارسال می‌کند، و فرستنده مدامی که بیت ارسالی با صحت به دست گیرنده نرسیده باشد آن را روی کانال ارسال می‌کند. در این صورت با توجه به این که احتمال انتقال با صحت کامل برابر $\alpha - 1$ است، نرخ مؤثر انتقال برابر $\alpha - 1$ است. به این ترتیب با استفاده از بازخورد قادریم به راحتی به ظرفیت $\alpha - 1$ دست‌یابیم. ثابت می‌شود که چه با بازخورد و چه بدون آن، بیشینه نرخی که می‌توانیم به آن دست‌یابیم برابر $\alpha - 1$ است. در حقیقت بازخورد، ظرفیت یک کانال را افزایش نمی‌دهد.

اُنْتِرِپْرِی پُرْسِمْ

۔

ظرفیت کanal پیوسته

مفهوم انتروپی برای توابع پیوسته نیز تعریف می‌گردد.

$$X \quad f_X(x), \quad f_X(x) \geq 0,$$

$$\int_{-\infty}^{+\infty} f_X(x)dx = 1$$

$$F(x) = P(X \leq x) = \int_{-\infty}^x f_X(x)dx$$

$$H(x) = - \int_{-\infty}^{+\infty} f_X(x) \log_2 f_X(x)dx$$

ظرفیت کanal پیوسته (ادامه) AWGN (Additive white Gaussian noise)

در نتیجه این تلاش ظرفیت برای کanal پیوسته با نویز AWGN (قضیه Shannon-Hartley):

$$C = B \log_2 (1 + \text{SNR})$$

• می‌دانیم که:

$$\text{SNR}_{\text{dB}} = 10 \log_{10} \frac{\text{Signal Power}}{\text{Noise power}} = 10 \log_{10} \text{SNR}$$

• $\text{SNR} = 0 \text{ dB}$: یعنی قدرت سیگنال برابر با قدرت نویز است. یعنی سیگنال در نویز غرق شده است.

ظرفیت کanal پیوسته AWGN-مثال

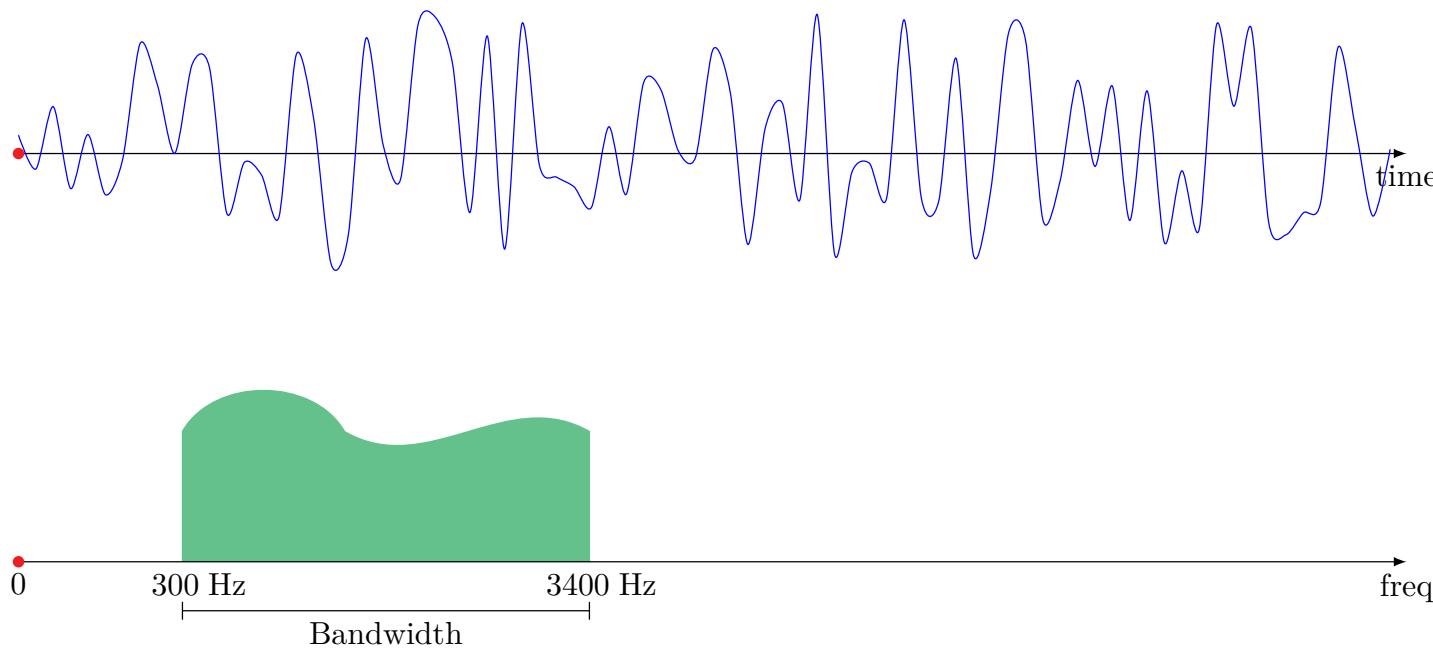
در شبکه LTE بیشینه پهنای باند (Bandwidth) مورد استفاده برابر با 20 MHz است. معمولاً بهترین SNR در شبکه LTE برابر با 12 dB است. پس خواهیم داشت:

$$\text{SNR [dB]} = 10 \log_{10} \text{SNR} \implies \text{SNR} = 10^{1.2} = 16$$

$$C = 20 \log_2(1 + 16) \approx 81.49 \text{ Mb}\odot\odot\odot$$

ولی LTE تا حد اکثر نرخ 300 مگابیت را می‌تواند پشتیبانی کند؟!

ظرفیت کanal پیوسته AWGN-مثال



می‌دانیم که پهنه‌ای باند صدای انسان برای انتقال در شبکه (PSTN) (Public Switched Telephone Network) میزان SNR حدوداً برابر با 35 dB است. در صورتی که در خطوط تلفنی میزان SNR برابر با 4 kHz شانون ظرفیت به صورت زیر محاسبه می‌شود.

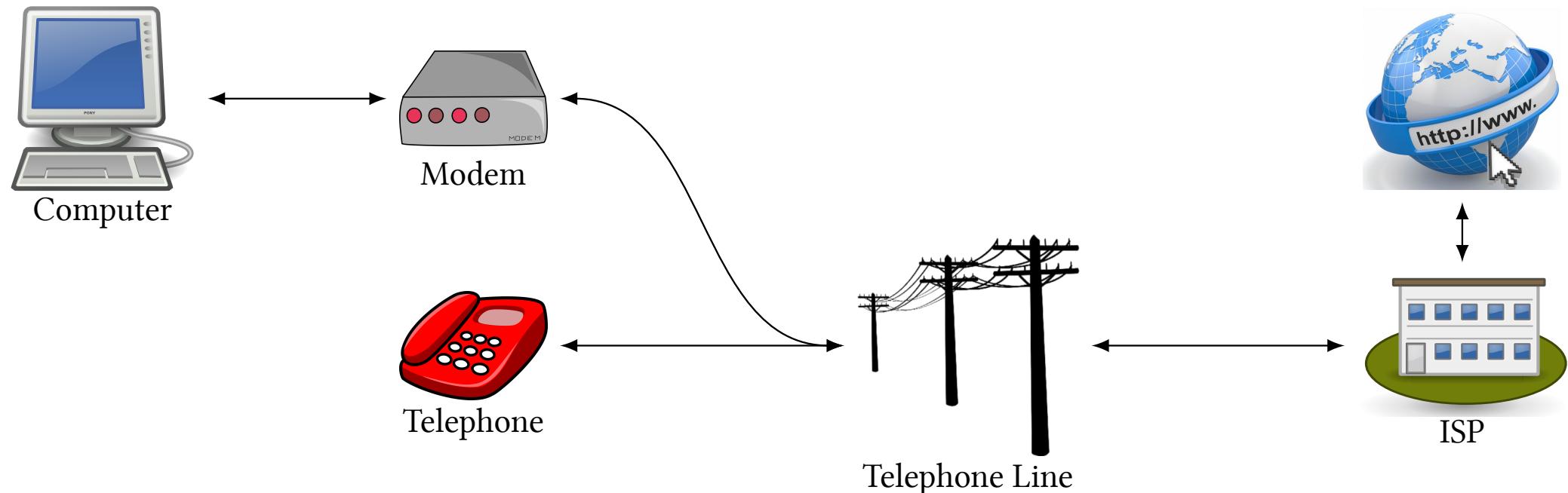
$$C = 4000 \log_2(1 + 10^{3.5}) \approx? \text{ Kb}$$

شبکه دسترسی Dial-up

استفاده از بستر PSTN برای انتقال اینترنت از دهه ۱۹۸۰ میلادی.

مزیت: فرآگیر بودن و بدون نیاز به بستر خاص.

برای سرعت بسیار پایین حداقل ۵۶ کیلوبیت بر ثانیه و اشغال شدن خط تلفن.



شبکه دسترسی Dial-up

حداکثر نرخ Dial-up به صورت تئوری برابر با $\frac{kb}{s}$ ۵۶ بود؟!

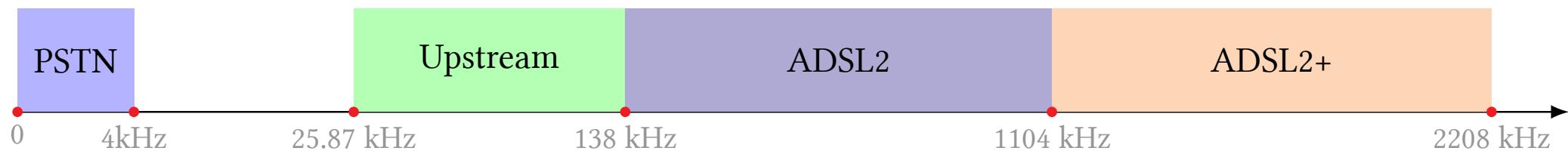
خطوط تلفن به مانند یک هواپیمای ۲۰۰ نفره است که ما در Dial-up و تلفن فقط از دو ظرفیت آن استفاده کردیم.



DSL خانواده‌ای از فناوری‌ها است برای انتقال داده از طریق خط تلفن، به HDSL (High bit-rate Digital Subscriber Line)، ADSL (Asymmetric Digital Subscriber Line) و VDSL (Very-high-bit-rate Digital Subscriber Line) مانند (High bit-rate Digital Subscriber Line) مانند (Asymmetric Digital Subscriber Line) و (Very-high-bit-rate Digital Subscriber Line) در (Asymmetric Digital Subscriber Line) از پهنه‌ای باند باقی‌مانده استفاده می‌شود.

تفاوت ADSL و ADSL2+ در تفاوت پهنه‌ای باند DownStream است.

واژه ADSL در Asymmetric Digital Subscriber Line ناظر به عدم تقارن بین UpStream و DownStream است.



☞ حداقل سرعت ADSL2+ به صورت تئوری:

0/3km در فاصله $25Mb/s$ •

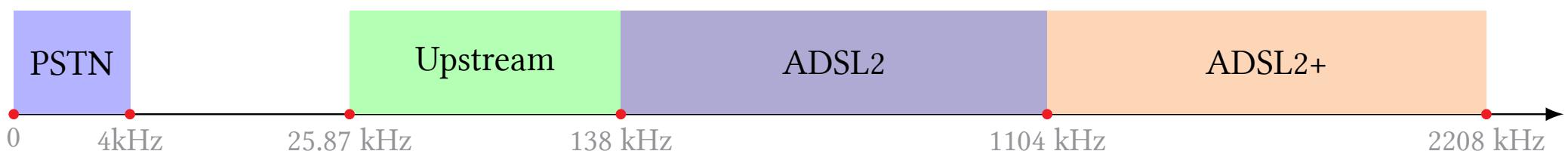
0/9km در فاصله $23Mb/s$ •

1/2km در فاصله $21Mb/s$ •

2/1km در فاصله $16Mb/s$ •

3km در فاصله $8Mb/s$ •

5/2km در فاصله $1/5Mb/s$ •



مثال ۱۲ اگر یک سیگنال در بازه بین سه تا چهار مگاهرتز به ارسال داده بپردازد، با در نظر گرفتن SNR برابر با ۲۴dB، مقدار ظرفیت کanal چقدر خواهد شد؟

پاسخ: نخست در نظر بگیرید که وقتی گفته می‌شود سیگنال در بازه بین سه تا چهار مگاهرتز به ارسال اطلاعات می‌پردازد، یعنی پهنای باند (Bandwidth) برابر با یک مگاهرتز است. در ضمن باید ۲۴dB را نیز به واحد مطلق تبدیل کنید. بدینسان داریم:

$$C = B \log_2(1 + SNR) = 1 \log_2(1 + 10^{2.4}) = 7.97 \text{ Mbps}$$

سوال اول اگر X منبعی با خروجی های (a, b, c, d) با احتمالات به ترتیب $(\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{8})$ باشد، الف آنتروپی X را بیابید.

ب اگر این احتمالات متناظر برای خروجی های (b, a, d, c) بود جواب چه تغییری می کرد؟
ج از این تمرین چه نتیجه ای می گیریم؟

سوال دوم اگر (X, Y) دارای توزیع مشترک زیر باشند:

$Y \setminus X$	1	2	3	4	$P(Y)$
X	$\frac{1}{8}$	$\frac{1}{16}$	$\frac{1}{32}$	$\frac{1}{32}$	
Y	$\frac{1}{16}$	$\frac{1}{8}$	$\frac{1}{32}$	$\frac{1}{32}$	
3	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	
4	$\frac{1}{4}$	0	0	0	
$P(X)$					

الف $H(Y|X)$ و $H(X|Y)$ را حساب کنید.

ب اگر انتروپی، میزان ابهام باشد، نتیجه خود را از بند الف به صورت شهودی در دو سطر بیان کنید؟

ج $H(X, Y)$ و $H(X), H(Y)$ را حساب کنید.

د با توجه با نتیجه محاسبات بند الف و ج، رابطه آنتروپی مشترک را به صورت شهودی در دو سطر بیان کنید؟

۵ صحت رابطه زیر را در مورد این مساله نشان دهید.

$$H(X_1, X_2, \dots, X_n) \leq \sum_{i=1}^n H(X_i)$$

و اطلاعات متقابل را حساب کنید.

ز اگر X و Y را مولفه های ورودی و خروجی کانالی ارتباطی در نظر بگیریم، ظرفیت این کanal چقدر است؟

ح اگر بخواهیم اطلاعات متقابل حداقل شود(معادل اینکه ظرفیت کمینه شود)، جدول توزیع مشترک را به شرط

داشتن احتمالات حاشیه ای مشابه جدول قبل، مجددا پر کنید.

$Y \setminus X$	1	2	3	4	$P(Y)$
1					$\frac{1}{4}$
2					$\frac{1}{4}$
3					$\frac{1}{4}$
4					$\frac{1}{4}$
P(X)	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{8}$	$\frac{1}{8}$	

ط اگر هدف بیشینه کردن آنتروپی مشترک بود، جواب قسمت قبل به چه صورت تغییر می کرد؟

ی نتیجه خود از دو قسمت قبل را با توجه به یکی از تعاریف اطلاعات متقابل که به صورت فاصله دو توزیع $P(x, y)$

و $P(x)P(y)$ بیان می شود در حداکثر دو سطر بیان کنید.

$$I(X, Y) = D(P(x, y) || P(x)P(y)) = \sum_{x,y} P(x, y) \log \frac{P(x, y)}{P(x)P(y)}$$

ک اگر بخواهیم هم آنتروپی X و هم آنتروپی مشترک حداکثر شود، جدول توزیع مشترک را به شرط داشتن احتمال حاشیه‌ای مشابه برای Y ، جدول را مجدداً پر کنید.

$Y \setminus X$	1	2	3	4	$P(Y)$
1					$\frac{1}{4}$
2					$\frac{1}{4}$
3					$\frac{1}{4}$
4					$\frac{1}{4}$
$P(X)$					

ل برای جدول پر شده قسمت قبل $H(X, Y)$ و $H(X)$, $H(Y)$ را محاسبه کنید و با مقدار اولیه محاسبه شده در بند ج مقایسه کنید.

سوال سوم یک تاس را پرتاب می کنیم. اگر خروجی جزء پیشامد $A = \{1, 2, 3, 4\}$ باشد، یک سکه سالم را یک بار می اندازیم. اگر جزء پیشامد $B = \{5, 6\}$ باشد، سکه سالمی را دو بار می اندازیم. اطلاعات متقابل عدد خوانده شده از پرتاب تاس و تعداد خط آمدن سکه را بدست آورید.

سوال چهارم

- الف ظرفیت کانالی با پهناهی باند ۱۰ مگاهرتز و $SNR = 5\text{dB}$ چقدر است؟
- ب اگر بخواهیم به ظرفیت 50Mbps بررسیم چه مقدار SNR نیاز است؟

پروژه اول

در این پروژه از شما خواسته شده است که یک فایل صوتی را وارد نرم افزار MATLAB کرده، و سپس انترپوی آن را محاسبه کنید. بدین سان گام های زیر را برای اجرای این پروژه بردارید:

☞ **گام اول:** نرم افزار MATLAB را نصب بر روی سیستم عامل خود نصب کنید. دقت کنید که این نرم افزار را براحتی می توانید در انواع سیستم عامل ها از Windows گرفته تا macOS و Linux نصب کنید. سعی کنید نسخه جدید این نرم افزار را نصب کنید و یا حداقل نسخه MATLAB 2018b

۵ گام دوم: یک فایل Wav را با این نرم افزار بخوانید. دقیق کنید که Help این نرم افزار واقعاً کامل و جامع است. اما برای استفاده از Help آن به صورت برخط (Online) باید فیلترشکن نصب کنید و یا از [شکن](#) استفاده کنید. به عنوان مثال [این صفحه](#) را نگاه کنید. من به صورت نمونه در کد زیر این کار را انجام داده‌ام:

```
% Initialization
clc
clear

% Create WAV file in current folder .
load handel.mat
audiowrite('handel.wav',y,Fs)
clear y Fs

% Read the data back into MATLAB , and listen to audio .
[y, Fs] = audioread('handel.wav');

% Play wav file
player = audioplayer(y,Fs);
play(player);
```

گام سوم: به سوالات زیر پاسخ دهید:

- الفبای منبع در حالت ذکر شده چیست؟ و چه تعداد است؟ راهنمایی: شما باید بگویید سمبول‌های تولید شده (y) چگونه هستند، یعنی مثلا عدد هستند، صحیح هستند یا اعشاری، اگر صحیح هستند چند بیتی هستند اگر اعشاری هستند با چه دقیقی (۷ رقم اعشار یا ۱۵ رقم اعشار).
 - سرعت تولید سمبول در منبع ذکر شده چه مقدار است؟ سپس توسط آن کل زمان (کل زمانی که شما صدا را می‌شنوید) را محاسبه بکنید. راهنمایی: خروجی F_s نشان‌دهنده مقدار سرعت منبع اطلاعات است. با داشتن تعداد سمبول‌ها و همچنین مقدار F_s به سادگی می‌توانید مقدار زمان را بدست آورید.
- بیان شد که تمام سیگنال‌هایی که در طبیعت وجود دارند سیگنال‌های آنالوگ می‌باشند. به نظر شما سرچشممه همین فایل handel که در بالا آن را فراخوانی کردیم، از کجا است؟ احتمالا در ارکسرسی این موسیقی تولید شده و مثلاً فردی به نام X آن را با یک mp3 player ضبط می‌نماید. سیگنال‌های آنالوگ تولید شده توسط ادوات ارکسر به صفحه میکروفون آفای X برخورد می‌کند. این برخورد موجب ایجاد ارتعاشاتی می‌شود و

این ارتعاشات نیز خود تبدیل به تغیرات ولتاژ می‌شود. تغییر ولتاژ را می‌توان به صورت یک سیگنال در نظر گرفت. تا اینجا احتمالاً قبول می‌کنید که با یک سیگنال آنالوگ مواجه هستم.

اگر من این سیگنال آنالوگ را توسط دستگاه ضبط صدا بر روی یک نوار کاست ضبط کنم، یک سیگنال آنالوگ را به صورت آنالوگ ذخیره نمودم. اگر نوار کاست را درون یک دستگاه پخش نوار کاست بگذارم، می‌توانم آن را پخش کنم. پس دستگاه پخش نوار کاست یک منبع اطلاعات آنالوگ هست. اما در مورد mp3 player این قضايا برقرار نیست. من نمی‌توانم مانند نوار کاست اطلاعات را به طور پیوسته ضبط کنم. چرا که در هنگام ضبط صدا در نوار کاست، نوار به صورت پیوسته می‌چرخد و اطلاعات در آن ذخیره می‌شود. پس راه کار چیست؟ راه کار این است که mp3 player تنها نمونه‌هایی از سیگنال آنالوگ را در حافظه خود ذخیره کند. در هنگام پخش صدا در mp3 player، در هر زمان‌های مشخصی نمونه‌های ذخیره شده به سمت بلندگو ارسال می‌شوند و صفحه بلندگو را تحریک می‌کنند.

با توجه به مطالب بیان شده، احتمالاً این سوال بوجود می‌آید که به نظر می‌رسد که mp3 player در زمان‌های

مشخصی اقدام به ارسال یک نمونه به سمت بلندگو برای پخش می‌کند. به نظر باید گوش ما یک لحظه صدا را بشنود و تا زمانی که نمونه بعدی می‌آید هیچ چیز نشنود. اما اگر به همان فایل handel گوش کنید شما چنین قطعی در صدانمی یابید. چرا؟ چرا در هنگام تماشای یک فایل ویدئویی با این که تنها ۲۰ تا ۳۰ فریم در ثانیه پخش می‌شود، ولی شما هیچ‌گونه گستاخی در فیلم مشاهده نمی‌کنید؟

۴ گام چهارم: فرض کنید که سمبل‌های منبع از یکدیگر مستقل هستند. هیستوگرام فایل صوتی handel را رسم کنید.

- هیستوگرام نشان‌دهنده این است که هر سمبل با چه احتمالی در فایل رخ داده است.
- در ضمن با استفاده از روابط بیان شده انتروپی این منبع را بدست آورید.
- با استفاده از قضیه اول شانون بگویید که این فایل را حداقل تا چه میزان می‌توان فشرده کرد؟
- به نظر شما نتیجه بدست آمده معقول است؟ اگر نیست چرا؟ تحقیق کنید و ببینید آیا می‌توان به مرزهای واقعی‌تری برای فشرده‌سازی دست یافت.

۵ گام پنجم: کدکننده هافمن یکی از انواع کدکننده‌های منبع بدون اتلاف است. در این قسمت می‌خواهیم

توسط نرم‌افزار MATLAB یک کدکننده هافمن به خروجی منبع اطلاعات خود اعمال کنیم. این کار را بر روی فایل صوتی اعمال کنید. راهنمایی: MATLAB ابزارهای مفیدی برای این کار در اختیار شما قرار داده است.

- محاسبه کنید که چه مقدار فضای ذخیره فایل صوتی نیاز است؟ (لطفاً محاسبه کنید و با مقدار size اصلی سیگنال مقایسه کنید.)
- محاسبه کنید که برای انتقال این فایل در یک لینک مخابراتی با سرعت 64 kbit/s چه مقدار زمان لازم است؟

نکته ۲ ما برای انتقال اطلاعات معمولاً نیازمند فشرده‌سازی بیشتری می‌باشیم. لذا مجبور هستیم که به سراغ کدکننده‌های با اتلاف برویم.

چند نکته تكميلی:

- محتواي فايل‌هاي پروژه:

الف فايل صوتی اصلی به همراه فايل صوتی فشرده شده.

ب کدهای MATLAB

ج یک گزارش تفصیلی که در آن به تمامی سوالات مطرح شده پاسخ داده شده باشد.

- به کسانی که گزارش تحويلی آن‌ها با LATEX باشد نمره اضافی تعلق می‌گیرد.

- حتما فايل صوای انتخابی دانشجویان با یکدیگر متفاوت باشد. حداکثر طول فايل صوتی سی ثانیه باشد.

- محل بارگذاری تمرین نیز در سایت quera.ir است که پیوند ارتباطی آن در گروه قرار داده خواهد شد.

- تقریباً یک هفته بعد از تحويل، از برخی از دانشجویان خواسته خواهد شد که به صورت Skype پروژه را تحويل برخط (Online) نیز دهند.

- [1] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. John Wiley & Sons, 2 ed. , 2012.

فهرست اختصارات

A

ADSL Asymmetric Digital Subscriber Line

AWGN Additive white Gaussian noise

D

DMC Discrete Memoryless Channel

DSL Digital subscriber line

H

HDSL High bit-rate Digital Subscriber Line

L

LTE Long Term Evolution

P

PSTN Public Switched Telephone Network

S

SNR Signal Noise Ratio

V

VDSL Very-high-bit-rate Digital Subscriber Line

واژه‌نامه انگلیسی به فارسی

C

Conditional Entropy انتروپی شرطی پهنه‌ای باند

Cryptography رمزگاری تابع انتروپی دودویی

Binary Erasure کanal دودویی همراه با محوشدن .

D

Demodulator وامدوله ساز Binomial Distribution توزیع دوجمله‌ای

Detector آشکارساز

Channel

کanal گسته بدون حافظه . Discrete Memoryless

I

Channel

Idle Mode مُد بیکار

Information Source منبع اطلاعات .. E

Information Theory نظریه اطلاعات .. Event پیشامد ..

Encoding کدگذاری ..

J Entropy انتروپی ..

Joint Entropy انتروپی توام ..

G

Gray Scale Image تصویر خاکستری ..

R

Random Variable متغير تصادفى بى حافظگى

اطلاعات متقابل Mutual Information

S

Source Coding کدگذار منبع

Stochastic Process فرایند تصادفى

مدولاسیون Modulation

مدوله کننده Modulator

O

U

User کاربر

برخط Online

سیستم عامل Operating System

واژه‌نامه فارسی به انگلیسی

۱

ب

Online آشکارساز	Detector برشط
Memoryless اطلاعات متقابل	بی‌حافظگی Mutual Information
	Entropy انتروپی
	Joint Entropy انتروپی توام
	Conditional Entropy انتروپی شرطی
Bandwidth پهنای باند	
Event پیشامد	

ت

تابع انتروپی دودویی

ف

تصویر خاکستری

Stochastic Process

فرایند تصادفی

توزیع دو جمله‌ای

ک

User

کاربر

رمزنگاری

Binary Erasure

Channel

کanal گسته بدون حافظه .

س

سیستم عامل

کدگذار منبع ن Source Coding

کدگذاری Encoding نظریه اطلاعات Information Theory

م و

متغیر تصادفی Random Variable وامدوله ساز Demodulator

مُد بیکار Idle Mode

مدولاسیون Modulation

مدوله کننده Modulator

منبع اطلاعات Information Source