ظرفیت کانال های کلاسیک

۱ مقدمه

دردرس قبل دیدیم که می توان پیام های یک منبع را که از کلمات $X = \{x_1, x_2, \cdots x_{2^n}\}$ تشکیل شده است را می توان باکدگذاری مناسب یعنی کدگذاری بلوکی چنان مخابره کرد که بجای n بیت به ازای هرکلمه، $nH(X) \leq n$ بیت مخابره کنیم. این نتایج البته درحد n های بزرگ دقیق هستند. تمام این حرف ها درصورتی بود که ازنوفه داخل کانال صرف نظرکنیم و فرض کنیم که پیام بدون هیچ نوع تغییری به مقصد می رسد. مطالب بالا محتوی قضیه شانون را درباره کدگذاری بدون نوفه تشکیل می دهند. دراین درس می خواهیم درباره کد گذاری درحضورنوفه بحث کنیم و نهایتا قضیه شانون درباره کد گذاری درحضورنوفه را بیان کنیم. دراین درس هم چنین بامفهوم مهم ظرفیت کانال آشنا خواهیم شد ودرحالت های خیلی ساده ای مقدارآن را محاسبه می کنیم.

۲ موازنه بین پایین آوردن خطا وبالابردن نرخ انتقال اطلاعات

ازاین به بعد فرض می کنیم که کلمات منبع خود را به طریق بهینه ای کدگذاری کرده ایم وتنها می خواهیم کد کلمه هارا که رشته هایی از 0 و 1 هستند مخابره کنیم. فرض می کنیم که کانالی که پیام های خود را از طریق آن ارسال می کنیم تحت تاثیرنوفه قرار می گیرد و هرعلامت 0 یا 1 که‌ارسال می کنیم بااحتمال q تبدیل به 1 یا 0 شده و با احتمال $1-q$ دست نخورده باقی می ماند. می خواهیم کاری کنیم که گیرنده پیام ها همچنان بتواند پیام های صحیح را ازپیام های دریافت شده استخراج کند.

۱.۲ یک تذکرمهم

آنچه که درمثال بالاگفته شد یک نوع کد موسوم به کد تکرار سه تایی برای تشخیص وتصحیح خطاست و باکدگذاری کلمات فرق می کند. ازاین به بعد دراین درس هروقت که مااز کلمه کدگذاری استفاده می کنیم منظورمان این نوع کدگذاری است. به عبارت دیگر فرض می کنیم که کلمات منبع X که می توانند حروف یک زبان مثل فارسی یاانگلیسی یاعلائم ریاضی باشند به نحو بهینه ای تبدیل به رشته های 0 و 1 شده اند و هدف ما مخابره این رشته ها ازدرون کانال است. درانتهای کانال رشته های دریافت شده نخست برای تعیین وتصحیح خطاها بررسی شده وپس ازاصلاح به کلمات زبان موردنظربازگشایی می شوند.

راهی که برای تعیین وتصحیح خطاباید پیش گرفت آن است عنصر تکرار را به نوعی وارد پیام های خود کنیم. به عنوان مثال می توانیم بجای مخابره‌یک 0 سه تا 0 وبجای یک 1 سه تا 1 مخابره کنیم واز گیرنده بخواهیم که با استفاده از قانون اکثریت تصمیم بگیرد که یک رشته سه تایی که دریافت کرده است درواقع چه رشته ای بوده است (جدول ??).

0	0 0 0
1	1 1 1

کد تکرار سه تایی :1

درواقع احتمال خطا که قبلاً برابربود با q اینک کمترشده است، زیرااحتمال وقوع خطا اینک برابراست بااحتمال وقوع دو برگردان و یا سه برگردان درکد سه تایی که اولی برابر است با $3q^2(1-q)$ ودومی برابراست با q^3. درنتیجه احتمال وقوع خطا برابرخواهد بود با $q^3+3q^2(1-q)$ که برای q های کوچک ازمرتبه q^2 است. البته بهایی برای این کاهش خطا پرداخت کرده ایم و آن این است که نرخ مخابره اطلاعات را پایین آورده ایم و از سه بیت برای مخابره یک بیت استفاده کرده ایم. دراین حالت نرخ مخابره اطلاعات یعنی R برابراست با $\frac{1}{3}$. درحالت کلی اگر از n بیت برای مخابره 2^k پیام استفاده کنیم (که درنبود نوفه می توانست برای مخابره 2^n پیام مورد استفاده قرارگیرد) می گوییم که نرخ مخابره اطلاعات برابراست

$$R := \frac{k}{n}. \tag{1}$$

مسلم است که‌دراین نوع کدگذاری می توان بازهم احتمال خطا را کاهش داد و درحد ایده آل آن را به صفر نزدیک کرد ولی دراین صورت نرخ R نیزبه سمت صفرمیل خواهد کرد. حال سوالی که باآن مواجه هستیم آن است که آیا اصولاً می توان ازیک کانال نوفه دار با نرخ محدود و غیرصفر اطلاعاتی را عبورداد به نحوی که احتمال وقوع خطا لااقل درحد مجانبی (برای رشته های بزرگ) به سمت صفر میل کند؟ آیا یک نوع کدگذاری وجود دارد که این امکان را برای ما فراهم آورد؟ آیا نرخ بیشینه ای وجود دارد که هرنوع مخابره اطلاعات با بیش از آن نرخ بدون خطا غیرممکن باشد؟ این ها سوالاتی است که درقضیه دوم شانون پاسخ داده شده است. قبل از بیان قضیه کلی سعی می کنیم که دو مثال ساده را بررسی کنیم.

مثال ۱ : حالت ساده ای را درنظرمی گیریم که منبع X پیام هایی را ارسال می کند که درآنهااحتمال وقوع 0 و 1 یکسان باشد. به عبارت دیگر آنتروپی منبع دراین مثال برابراست با 1. فرض کنید که پیام خود را دررشته های n بیتی ارسال کنیم . مجموعه تمام رشته های n بیتی دارای 2^n رشته است. نقاط این فضا نقاط یک شبکه ابرمکعبی n بعدی را پرکرده اند. اگر همه این نقاط را به عنوان کدکلمه های خود به کاربریم به آسانی درطول عبوراز کانال یک کد کلمه به یکی از کد کلمه های همسایه اش یا کد کلمه های نزدیکش تبدیل می شود و گیرنده واقعاً نمی فهمد که چه کد کلمه ای برایش ارسال شده است. بنابراین راه مقابله با خطا آن است که سعی کنیم که کدکلمه هارا بافاصله کافی از یکدیگر انتخاب کنیم تااحتمال وقوع خطا پایین بیاید. درواقع وقتی که یک کدکلمه راارسال می کنیم حول آن یک کره به اندازه کافی بزرگ رسم می کنیم و هروقت نقطه ای درون این کره دریافت کنیم آن را به عنوان کد کلمه ای که درمرکز آن قراردارد تعبیر وخطاهای بوجود آمده را تصحیح می کنیم. این کاربه طورطبیعی نرخ را پایین می آورد زیرازهمه نقاط شبکه استفاده نمی کنیم. حال می پرسیم که کد کلمه هارا با چه فاصله ای انتخاب کنیم. دراین جا می بایست بین دو عامل متضاد موازنه ایجاد کنیم. اگر بخواهیم خطارا پایین بیاوریم می بایست فاصله کد کلمه هاراازیکدیگر زیادکنیم. ازطرفی این کارنرخ را پایین می آورد. خوب بیایید ببینیم به طور متوسط یک کد کلمه به چند

کلمه نزدیک دیگر ممکن است تبدیل شود؟ در یک کلمه n حرفی هر حرف با احتمال q ممکن است که برگردانده شود. بنابراین تعداد حرف های برگردانده شده به طور متوسط برابراست با nq. این تعداد حرف می تواند به $\binom{n}{nq} \approx 2^{nH(q)}$ طریق در رشته n حرفی قرارگیرند. درنتیجه تعداد رشته های نزدیک به این کلمه که ممکن است ازخطاهای بوجود آمده دراین کلمه ایجاد شوند برابراست با $2^{nH(q)}$. درنتیجه یک نحوه کد گذاری خوب آن است که حول هرکلمه ناحیه ای درنظربگیریم که به طور متوسط تعداد کلمات داخل آن درحدود $2^{nH(q)}$ باشد. حال اگر نرخ مبادله برابربا $R = \frac{k}{n}$ باشد معنایش این است که تعداد کل کدکلمه هابرابراست با $2^k = 2^{nR}$. چون تعدادکل کلمات ممکن برابراست با 2^n به این نتیجه می رسیم که می بایست شرط زیربرقرارباشد:

$$2^{nR}2^{nH} \leq 2^n, \tag{2}$$

یا

$$R \leq 1 - H(q) =: C. \tag{3}$$

کمیت $C := 1 - H(q)$ ظرفیت این کانال نامیده می شود واین رابطه بیان می کند که برای پرهیزازخطا نرخ مبادله اطلاعات حتما باید ازظرفیت کانال کمترباشد. حال بایک سوال اساسی مواجه می شویم و آن اینکه آیا واقعا نوعی کدگذاری وجود دارد که بتوان بااستفاده از آن نرخ مبادله اطلاعات رادرحد مجانبی $n \longrightarrow \infty$ به حداکثر ممکن یعنی به C رساند؟ پاسخ این سوال مثبت است . درواقع شانون نشان داده است که کد تصادفی این کاررا می تواند انجام دهد. البته کد تصادفی هوشمندانه ترین نحوه کد کردن کلمات نیست ولی نکته جالب آن است که این کد می تواند حد بالای نرخ مبادله را اشباع کند. تعریف کد تصادفی به این صورت است که درفضای تمام کد کلمه های ممکن که شامل 2^n تا نقطه است، $2^k \equiv 2^{nR}$ نقطه به طور تصادفی انتخاب می کنیم. حول هرکدام از این نقاط کره ای رسم می کنیم که تعداد $2^{n(H(q)+\delta)}$ تا نقطه داشته باشد. حال همان نحو کد گشایی را که دربالا توضیح دادیم بکارمی بریم.

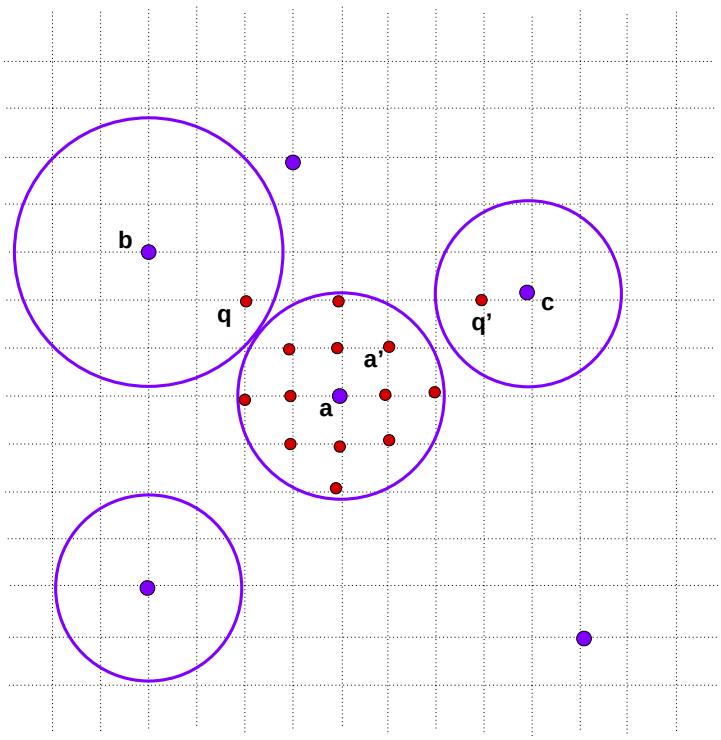
یک کد کلمه و کره اطراف آن را درنظر بگیرید. این کره کسر

$$f = \frac{2^{n(H(q)+\delta)}}{2^n} = 2^{-n(C-\delta)} \tag{4}$$

ازنقاط را دربردارد. اگر کد کلمه واقع درمرکزاین کره درطول انتقال به نقطه ای درون همین کره تبدیل شده باشد، خطا محسوب نمی شود. خطا وقتی بوجود می آید که کدکلمه های کرات دیگر درون این کره بیفتند. احتمال این اتفاق برابراست با f . چون درکل 2^{nR} کلمه داریم احتمال وقوع خطا برابرمی شود با:

$$P = f2^{nR} = 2^{-n(C-R-\delta)} \tag{5}$$

حال چون مجازیم δ را هرمقدارمثبتی بگیریم به این نتیجه می رسیم که می توانیم R را هرچقدرکه می خواهیم به C نزدیک کنیم و P همچنان درحد $n \longrightarrow \infty$ به سمت صفر میل می کند.



شکل ۱: هرگاه کد کلمه a دچارخطای کوچک شود و تبدیل به a' شود خطای بوجود آمده قابل تصحیح است. خطا وقتی بوجود می آید که a تبدیل به نقاط درون دیگر کره ها شود.

۳ تعریف ظرفیت درحالت کلی

دربخش قبل خود را به منبع پیامی محدودکردیم که دارای آنتروپی بیشینه بود زیرا دراین منبع حرف 0 وحرف 1 هردو بااحتمال $\frac{1}{2}$ رخ می دادند وبنابراین داشتیم $H(X) = H(\frac{1}{2}) = 1$. دراین بخش حالت کلی را درنظرمی گیریم که درآن آنتروپی منبع دلخواه است . فرض می کنیم که منبع حرف 0 را با احتمال p و حرف 1 را بااحتمال $1-p$ تولید کند. درنتیجه آنتروپی منبع برابراست با

$$H(X) = p\log\frac{1}{p} + (1-p)\log\frac{1}{1-p}. \tag{6}$$

حال می خواهیم ببینیم که پیام های این منبع را حداکثر با چه نرخی می توانیم مخابره کنیم. فرض کنید که رشته $y = (y_1, y_2, \cdots y_n)$ رادریافت کنیم. فرض اساسی ما آن است که حروف کلمه های ارسالی و هم چنین خطاهای ایجاد شده درآنها هیچ نوع همبستگی بایکدیگر ندارند. بنابراین احتمال وقوع 0 در همه مکان هابرابربا p است. تعدادرشته های متعارف x ای که می توانسته اند دراثر خطا منجربه این رشته y شوند برابراست با $2^{nH(X|y)}$. بنابراین حول این y می توانیم کره ای رسم کنیم که تعداد $2^{nH(X|y)}$ نقطه داشته باشد. به طورمتوسط کره هایی که حول نقاط مختلف رسم می کنیم دارای $2^{nH(X|Y)}$ نقطه

هستند. اگرتعدادکل نقاط را $2^k = 2^{nR}$ بگیریم می بایست داشته باشیم

$$2^{nH(X|Y)} \times 2^{nR} \leq 2^{nH(X)} \tag{7}$$

ودرنتیجه

$$R \leq H(X) - H(X|Y). \tag{8}$$

بنابراین ظرفیت کانال رامی توانیم به شکل زیرتعریف کنیم:

$$C = max_X I(X;Y) = max_X \left(H(X) - H(X|Y)\right). \tag{9}$$

ودرنتیجه نشان دادیم که امکان مخابره اطلاعات باهرنرخ R که کمترازظرفیت کانال باشد امکان پذیراست. به همان ترتیب که درموردمثال اول عمل کردیم دراین حالت کلی نیز می توان استدلال کردکه نرخ خطارامی توان درحد n های بزرگ به سمت صفر میل داد. یک رشته معین یعنی یک نقطه معین درابرشبکه را درنظربگیرید. تعدادنقاط درون کره ای که دوراین نقطه رسم کرده ایم برابر با$2^{n(H(X|Y)+\delta)}$. این نقاط کسر f ازکل نقاط راتشکیل می دهد که درآن

$$f = \frac{2^{n(H(X|Y)+\delta)}}{2^{nH(X)}} = 2^{-n(H(X)-H(X|Y)-\delta)} \tag{10}$$

حال احتمال اینکه یکی ازنقاط دیگر به اشتباه درون این کره بیفتد ومادر بازگشایی این رشته مرتکب خطا شویم برابراست با f. احتمال وقوع خطادربازگشایی کل رشته ها برابراست با f ضرب در تعدادکل رشته هایعنی

$$P = f \times 2^{nR} = 2^{-n(H(X)-H(X|Y)-\delta)} \times 2^{nR} = 2^{-n(C-R-\delta)}. \tag{11}$$

حال می توانیم هرقدرکه بخواهیم R را به C نزدیک کنیم و δ را چنان اختیارکنیم که همچنان $C - R - \delta > 0$ باشد ودرنتیجه P درحد n های بزرگ به سمت صفر میل کند. به عبارت بهتر به ازای هر $\epsilon > 0$ و هر$\delta > 0$ می توان n را آنقدر بزرگ گرفت که هردو شرط زیربرقرارباشند:

$$R < C - \delta, \qquad P < \epsilon, \tag{12}$$

واین نشان دهنده این است که می توانیم هرچقدرکه بخواهیم نرخ مخابره را به C نزدیک کرده ودرعین حال خطارا هرچقدرکه بخواهیم کوچک کنیم. دراین جانکته ای مطرح است وآن اینکه خطای محاسبه شده درواقع یک خطای متوسط است یعنی خطای بوجودآمده برای تمام کد کلمه ها متوسط گیری شده است. درواقع اگر خطای ایجادشده برای کدکلمه i را با P_i نشان دهیم آنچه که نشان داده ایم آن است که

$$\frac{1}{2^{nR}} \sum_{i=1}^{2^{nR}} P_i < \epsilon. \tag{13}$$

می توان باحذف کردن بعضی از کد کلمه ها ودرواقع خلوت کردن فضای شبکه ابرمکعبی ازنقاط فاصله بین کد کلمه هارازیادترکرد طوریکه خطای ایجادشده برای هر کد کلمه از یک مقداربی نهایت کوچک ترشود. می خواهیم ببینیم که چه مقدارازکلمات را باید دوربریزیم واین کارچقدرنرخ را پایین خواهد آورد. فرض کنید که تعداد کل کد کلمه هایی که خطای آنهااز 2ϵ بیشترباشد را با $N_{2\epsilon}$ نشان دهیم. دراین صورت نامساوی بالا نشان می دهد که

$$\frac{1}{2^{nR}} N_{2\epsilon} 2\epsilon < \epsilon, \tag{14}$$

که ازآن نتیجه می گیریم

$$N_{2\epsilon} < 2^{nR-1}. \tag{15}$$

بنابراین حداکثر می بایست به تعداد 2^{nR-1} یعنی نصف کدکلمه هارادورریخت تا فاصله بین کد کلمه ها آنقدرزیاد شود که خطای هرکد کلمه به زیر2ϵ رسد. دراین صورت نرخ تبدیل می شودبه:

$$R' = \frac{k'}{n} = \frac{nR-1}{n} = R - \frac{1}{n}, \tag{16}$$

که درحد n های بزرگ دوباره با R برابراست.

آنچه که دراین فصل نشان دادیم محتوی قضیه دوم شانون بودیعنی می توان ازیک کانال نوفه دار برای مخابره بدون خطای اطلاعات استفاده کرد مشروط براینکه نرخ مخابره را زیریک حد که ظرفیت کانال نامیده می شود نگاه داشت. می توان هرقدرکه بخواهیم نرخ را به ظرفیت کانال نزدیک کردوهمچنان خطارا کوچک نگاه داشت وبرای این کارمی بایست از کدهایی باطول بلندتراستفاده کرد.