جلسه هشتم

کانال دسترسی چندگانه: مقدمات

در یک کانال دسترسی چندگانه تعدادی فرستنده بصورت همزمان با یک گیرنده صحبت میکنند. این کانال مدلی از ارتباط همزمان تلفن های همراه با برج مرکزی، و یا صحبت همزمان چند نفر با یک نفر را میتواند مدل کند.

یک کانال دسترسی چندگانه بدون حافظه با دو فرستنده با یک توزیع شرطی $\mathsf{q}(y|x_1,x_2)$ مدل میشود که در آن x_1 و x_2 در اختیار فرستنده ها بوده و خروجی y توسط گیرنده مشاهده میشود. در این جلسه ابتدا مثال هایی از یک کانال دسترسی چندگانه را بیان میکنیم. سپس تعریف دقیق یک کد برای این مساله را بیان میکنیم. نهایتا چند کران درونی و بیرونی ساده را برای این کانال ذکر میکنیم.

۱ چند مثال

در این بخش سه مثال از کانال های دسترسی چندگانه را بیان میکنیم. اهمیت این کانال ها این است که زمانی که یک گزاره در مورد کانال دسترسی چندگانه داشته باشیم و بخواهیم درستی آن را بررسی کنیم، میتوانیم آن را برای این کانال ها خاص بررسی کنیم و در صورتی که نتیجه درست بود، آنوقت سعی کنیم آن را برای تمامی کانال ها ثابت کنیم.

کانال بدون تداخل: فرض کنید که خروجی Y بشکل $Y=(Y_1,Y_2)$ باشد و

$$\mathsf{q}(y|x_1,x_2)=\mathsf{q}(y_1|x_1)\mathsf{q}(y_2|x_2)$$

در این کانال هیچ تداخلی میان دو فرستنده وجود ندارد و هرکدام روی کانال خودشان ارسال میکنند. واضح است که هر کدام از دو کاربر با نرخی برابر ظرفیت کانالشان میتوانند پیام ارسال کنند.

کانال غیرحساس نسبت به یک ورودی: فرض کنید که

$$\mathsf{q}(y|x_1,x_2)=\mathsf{q}(y|x_1)$$

در این کانال فرستنده دوم هیچ تاثیری روی خروجی ندارد. پس نرخ ارسال فرستنده دوم صفر است. نرخ ارسال فرستنده اول هم برابر ظرفیت کانال است.

کانال XOR: در اینجا ورودی های کانال باینری بوده و خروجی برابر XOR ورودی ها است.

$$\mathcal{X}_1=\mathcal{X}_2=\{0,1\},\qquad Y=X_1\oplus X_2\in\{0,1\}.$$

به عبارت دیگر گیرنده میتواند بفهمد که آیا دو فرستنده بیت یکسانی را در ورودی قرار داده اند یا نه. فرض کنید که تنها یک بار از این کانال استفاده میکنیم. در این صورت اگر X_2 را به عنوان نویز برای X_1 در نظر بگیریم کانال فوق یک کانال BSC خواهد بود. در اینجا X_2 را به عنوان نویز و X_1 را به عنوان ورودی در نظر گرفتیم. البته این تفاوت وجود دارد که در کانال BSC امکان کنترل نویز وجود ندارد، اما اینجا X_2 قابل کنترل است. مشخصا اگر فرض کنید $X_2 \sim \mathcal{B}(q)$ باشد، با تغییر q ظرفیت کانال بین X_1 و Y تغییر می‌کند.

کانال جمعی: در اینجا ورودی های کانال باینری بوده و خروجی برابر جمع حقیقی ورودی ها است.

$$\mathcal{X}_1 = \mathcal{X}_2 = \{0, 1\}, \qquad Y = X_1 + X_2 \in \{0, 1, 2\}.$$

به عبارت دیگر گیرنده میتواند بفهمد که آیا دو فرستنده بیت یکسانی را در ورودی قرار داده اند یا نه؛ علاوه بر این، در صورتی که ورودی ها یکسان باشند میفهمد که دقیقا ورودی ها چه بوده اند. فرض کنید که تنها یک بار از این کانال استفاده میکنیم. در این صورت اگر X_2 را به عنوان نویز برای X_1 در نظر بگیریم کانال فوق یک کانال BEC غیر متقارن خواهد بود. در اینجا X_2 را به عنوان نویز و X_1 را به عنوان ورودی در نظر گرفتیم. مشخصا اگر فرض کنید $X_2 \sim \mathcal{B}(q)$ باشد، آنوقت در صورتی که $X_1 = 0$ ارسال شود، بیت ارسالی با احتمال $p(X_2 = 1) = q$ در گیرنده پاک میشود، و در صورتی که که $X_1 = 1$ ارسال شود، بیت ارسالی با احتمال $p(X_2 = 0) = 1 - q$ در گیرنده پاک میشود.

کانال اینترنت ایران: فرض کنید که برای اینترنت یک شیر در نظر بگیریم که با آن می توان قطع یا وصل بودن اینترنت را کنترل کرد. این شیر را به عنوان یک ورودی در نظر میگیریم. این کانال را هم میتوان به عنوان یک کانال دسترسی چندگانه در نظر گرفت:

$$Y = \begin{cases} X_1, & \text{اگر } X_2 = 0 \\ \text{خفه شده}, & \text{اگر } X_2 = 1 \end{cases}$$

به این معنی که اگر شیر بسته باشد ورودی هر چه باشد، در خروجی کانال اطلاعاتی دریافت نمی شود و سیگنال "خفه بودن"دریافت می شود. اگر شیر باز باشد ورودی در خروجی نمایش داده می شود. فرض کنید که تنها یک بار از این کانال استفاده میکنیم. در این صورت اگر X_2 را به عنوان نویز برای X_1 در نظر بگیریم کانال فوق یک کانال BEC خواهد بود. در اینجا X_2 را به عنوان نویز و X_1 را به عنوان ورودی در نظر گرفتیم. مشخصا اگر فرض کنید $X_2 \sim \mathcal{B}(q)$ باشد، آنوقت ورودی با احتمال q پاک میشود.

۲ تعریف کد

یک کد برای انتقال پیام های مستقل شخصی روی یک کانال دسترسی چندگانه متشکل است از:

۱. توابع کدگذار:

$$\mathcal{E}_1 : \{1, \cdots, 2^{nR_1}\} \mapsto \mathcal{X}_1^n,$$

$$\mathcal{E}_2 : \{1, \cdots, 2^{nR_2}\} \mapsto \mathcal{X}_2^n.$$

با فرض اینکه کدگذار اول پیام M_1 را دارد، کلمه کد ارسالی فرستنده اول $\mathcal{E}_1(M_1)$ خواهد بود. مشابها کلمه کد فرستنده دوم $\mathcal{E}_2(M_2)$ خواهد بود. مشخص کردن توابع کدگذار معادل مشخص کردن یک کتاب کد برای هر فرستنده است. هر کدگذار یک کتاب کد معین دارد و به کمک آن عمل کدگذاری را انجام می‌دهد.

۲. تابع کدگشا:

$$\mathcal{D} : \mathcal{Y}^n \mapsto \{1, \cdots, 2^{nR_1}\} \times \{1, \cdots, 2^{nR_2}\}.$$

با فرض اینکه کدگشا دنباله Y^n را در خروجی دریافت کند، بازسازی زیر را از پیام های ورودی انجام میدهد:

$$(\hat{M}_1, \hat{M}_2) = \mathcal{D}(Y^n).$$

بنابراین هر کد با ۶ - تایی $(n, R_1, R_2, \mathcal{E}_1, \mathcal{E}_2, \mathcal{D})$ بطور کامل معرفی می‌شود.

تعریف ۱ احتمال خطا در صورت ارسال پیام های $M_1 = m_1, M_2 = m_2$ اینگونه محاسبه میشود:

$$p(E|M_1 = m_1, M_2 = m_2) = \sum_{y^n : \mathcal{D}(y^n) \neq (m_1, m_2)} p\big(y^n | x_1^n = \mathcal{E}_1(m_1), x_2^n = \mathcal{E}_1(m_2)\big),$$

که در آن

$$p(y^n | x_1^n, x_2^n) = \prod_{i=1}^{n} \mathsf{q}(y_i | x_{1i}, x_{2i}).$$

احتمال خطای متوسط یک کد اینگونه تعریف میشود:

$$\begin{aligned} p(E) &= \sum_{m_1, m_2} p(M_1 = m_1, M_2 = m_2) p(E|M_1 = m_1, M_2 = m_2) \\ &= 2^{-n(R_1 + R_2)} \sum_{m_1, m_2} p(E|M_1 = m_1, M_2 = m_2). \end{aligned}$$

نهایتا احتمال خطای بیشینه یک کد اینگونه تعریف میشود:

$$\max_{m_1, m_2} p(E|M_1 = m_1, M_2 = m_2)$$

تعریف ۲ زوج نرخ (R_1, R_2) را قابل حصول گویند چنانچه دنباله‌ای از کدها $(n_i, R_1, R_2, \mathcal{E}_{1i}, \mathcal{E}_{2i}, \mathcal{D}_i)$ با نرخ های داده شده وجود داشته باشد بطوریکه $n_i \to \infty$ و همچنین حد احتمال خطا روی این دنباله به سمت صفر میل کند. در اینجا میتوان از تعریف احتمال خطای بیشینه یا متوسط استفاده کرد و این موضوع میتواند تعاریف متفاوتی از ناحیه ظرفیت را بدست بدهد.

معادلا زوج نرخ قابل حصول را میتوان اینگونه نیز تعریف کرد: زوج نرخ (R_1, R_2) را قابل حصول گویند چنانچه برای هر $\epsilon > 0$ و هر $N \in \mathbb{N}$ به دلخواه بزرگ، کدی با طول $n > N$ و با نرخ های (R_1, R_2) وجود داشته باشد بطوریکه احتمال خطای این کد کمتر از ϵ باشد.

۳ یک کران درونی ساده

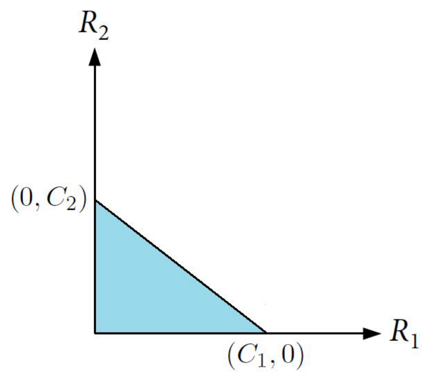
برای یک کانال دسترسی چندگانه C_1 و C_2 را ماکزیمم نرخ قابل ارسال برای فرستنده اول و دوم تعریف میکنیم. کانال XOR را در نظر بگیرید. اگر $X_2 = 0$ آنگاه یک کانال بدون نویز دراختیار X_1 قرار می‌گیرد. در این حالت X_1 می‌تواند با حداکثر نرخ ممکن خود یعنی $C_1 = 1$ ارسال را انجام دهد. اگر $X_1 = 0$ آنگاه یک کانال بدون نویز دراختیار X_2 قرار می‌گیرد. در این حالت X_2 می‌تواند با حداکثر نرخ خود یعنی $C_2 = 1$ ارسال را انجام دهد. در مورد کانال اینترنت ایران، فرستنده اول زمانی ماکزیمم نرخ ارسال را خواهد داشت که فرستنده دوم همواره $X_2 = 0$ را انتخاب کرده باشد. بصورت کلی تر برای یک کانال دسترسی چندگانه C_1 و C_2 به شکل زیر بدست می آیند:

$$C_1 = \max_{x_2} \max_{p(x_1)} I(X_1; Y | X_2 = x_2),$$

$$C_2 = \max_{x_1} \max_{p(x_2)} I(X_2; Y | X_1 = x_1).$$

اثبات این روابط را بعدا خواهیم دید. اما بصورت شهودی برای ماکزیمم کردن نرخ ارسال گیرنده اول، گیرنده دوم ورودی اش را بصورتی انتخاب میکند که ظرفیت کانال میان فرستنده اول و گیرنده ماکزیمم شود. فرستنده دوم ورودی تصادفی انتخاب نمیکند زیرا انجام چنین کاری ممکن است ابهامی ناخواسته در خروجی ایجاد کند و به کدگشایی گیرنده آسیب وارد کند.

دیدیم که $(C_1, 0)$ و $(0, C_2)$ داخل ناحیه ظرفیت هستند. ادعا میکنیم که نقاط روی خط واصل بین دو نقطه‌ی $(C_1, 0)$ و $(0, C_2)$ و زیر آن نیز قابل حصول هستند. این ناحیه در شکل زیر نشان داده شده است.



جهت اثبات توجه کنید که کافی است که ثابت کنیم که نقاط روی خط واصل دو نقطه‌ی $(C_1, 0)$ و $(0, C_2)$ قابل حصول هستند، زیرا هر اگر یک زوج نرخ (R_1, R_2) قابل حصول باشد، آنوقت تمامی زوج نرخ های (R_1', R_2') بطوریکه $R_1' \leq R_1$ و $R_2' \leq R_2$ نیز قابل حصول خواهند بود. دلیل این موضوع این است که فرستنده ها میتوانند بیت های زائد (آشغال) بین بیت های اطلاعات قرار دهند تا نرخ ارسالی را بصورت مجازی زیاد کنند. گیرنده این بیت های زائد را کدبرداری کرده و بدور می ریزد.

برای اثبات قابل حصول بودن نقاط روی خط واصل از روش اثباتی به نام تقسیم زمانی [1] استفاده میکنیم. هدف ما

[1] Time-Sharing

اثبات این گزاره کلی است که اگر دو نقطه (R_1, R_2) و (R'_1, R'_2) قابل حصول باشند، آنوقت نقطه

$$(\lambda R_1 + (1-\lambda)R'_1, \lambda R_2 + (1-\lambda)R'_2)$$

نیز قابل حصول است. از آنجایی که (R_1, R_2) و (R'_1, R'_2) قابل حصول هستند، پس برای هر احتمال خطای ϵ داده شده متناظر با این دو نرخ کد های (n_1, ϵ) و (n_2, ϵ) وجود دارد. ایده اثبات استفاده متوالی از این دو کد با فرکانس متناسب با λ و $1-\lambda$ است. تقسیم بندی زمانی به این معنی است که در بخشی از زمان یکی از کدها فعال باشد و در باقی زمان ها کد دیگر.

برای سادگی فرض کنید: $n_1 = n_2$. حال یک کد جدید به این شکل میسازیم: فرض کنید که K یک عدد ثابت اما خیلی بزرگ باشد. یک کد به طول $\lfloor K\lambda \rfloor n + \lfloor K(1-\lambda) \rfloor n$ اینگونه میسازیم: از کد اول به تعداد $\lfloor K\lambda \rfloor$ بار برای انتقال پیام، و از کد دوم به تعداد $\lfloor K(1-\lambda) \rfloor$ بار برای انتقال پیام استفاده میکنیم. در نتیجه این استفاده تعداد بیت های ارسالی از فرستنده اول برابر خواهد بود با

$$\lfloor K\lambda \rfloor nR_1 + \lfloor K(1-\lambda) \rfloor nR'_1$$

و تعداد بیت های ارسالی از فرستنده دوم برابر خواهد بود با

$$\lfloor K\lambda \rfloor nR_2 + \lfloor K(1-\lambda) \rfloor nR'_2.$$

پس نرخ بدست آمده برای کد جدید برابر خواهد بود با نسبت بیت های ارسال کل به تعداد استفاده کل از کانال:

$$\tilde{R}_1 = \frac{\lfloor K\lambda \rfloor nR_1 + \lfloor K(1-\lambda) \rfloor nR'_1}{\lfloor K\lambda \rfloor n + \lfloor K(1-\lambda) \rfloor n} \approx \lambda R_1 + (1-\lambda)R'_1,$$

$$\tilde{R}_2 = \frac{\lfloor K\lambda \rfloor nR_2 + \lfloor K(1-\lambda) \rfloor nR'_2}{\lfloor K\lambda \rfloor n + \lfloor K(1-\lambda) \rfloor n} \approx \lambda R_2 + (1-\lambda)R'_2.$$

احتمال خطای کد جدید برابر است با احتمال خطای اینکه در هر کدام از استفاده ها از کد اول یا دوم خطا داشته باشیم. با استفاده از باند اجتماع احتمال خطا را میتوان با جمع احتمال خطاهای تک تک کد ها کران بالا زد:

$$P(E) \leq \lfloor K\lambda \rfloor \epsilon + \lfloor K(1-\lambda) \rfloor \epsilon \leq K\epsilon.$$

چون K عددی ثابت (هر چند بزرگ) بود، میتوان ϵ را به اندازه کافی کوچک گرفت تا $K\epsilon$ به میزان لازم کوچک باشد.

۱.۳ کران درونی برای کانال های خاص

در کانال بدون تداخل، کران درونی با ناحیه ظرفیت مساوی نخواهد بود زیرا بصورت همزمان میتوان به نرخ

$$(R_1 = C_1, R_2 = C_2)$$

رسید، و ناحیه ظرفیت یک مستطیل است.

جهت ماکزیمم کردن C_1 برای کانال های XOR و جمعی گیرنده دوم باید عددی ثابت را انتخاب کند. در این صورت محاسبه ای ساده نشان میدهد که

$$C_1 = C_2 = 1.$$

پس کران درونی در هر دو حالت یک مثلث است که رئوس آن $(0,0), (0,1), (1,0)$ میباشد یعنی ناحیه بشکل زیر است:

$$\{(R_1, R_2) : \quad R_1 \geq 0, \ \ R_2 \geq 0, \ \ R_1 + R_2 \leq 1\}.$$

بصورت شهودی برای کانال XOR این ناحیه همان ناحیه ظرفیت است زیرا از آنجایی که خروجی Y دودویی است، بیش از یک بیت در هر استفاده از کانال دریافت نمیکند. بنابراین $R_1 + R_2$ نمیتواند از یک بزرگتر باشد. از طرفی تمامی نقاطی که $R_1 + R_2$ آنها کمتر مساوی یک است، قابل حصول میباشند. پس ناحیه ظرفیت بر کران درونی منطبق خواهد بود.

تمرین ۳ مقادیر C_1 و C_2 را برای کانال اینترنت ایران بیابید. توجه کنید که کسی شیر اینترنت را کنترل میکند می تواند با باز و بسته کردن شیر در زمان های مختلف اطلاعات منتقل کند.

در مورد کانال جمعی کران درونی با ناحیه ظرفیت مساوی نخواهد بود. برای این کانال نشان میدهیم که دو نقطه ی $(0.5, 1)$ و $(1, 0.5)$ قابل دستیابی هستند. جهت دستیابی به این نقطه $(1, 0.5)$ فرض کنید که نفر اول بیت هایش را (که از توزیع یکنواخت $\mathcal{B}(\frac{1}{2})$ انتخاب شده اند) بدون کدگذاری و بطور مستقیم روی کانال قرار دهد. همانطور که قبلا بحث کردیم از دید فرستنده دوم، کانال میان او و گیرنده یک کانال BEC با پارامتر $\frac{1}{2}$ خواهد بود. بنابراین فرستنده دوم میتواند با کدگذاری مناسب $\frac{1}{2}$ بیت را منتقل کند. گیرنده ابتدا نفر اول را به عنوان نویز فرض کرده و پیام نفر دوم را کدگشایی میکند. پس از یافتن دنباله ارسالی نفر دوم، آن را از خروجی کم کرده تا دنباله ارسالی نفر اول (که همان پیام او است) را دریافت کند.

۴ یک کران بیرونی ساده

سوالی که مطرح میشود آن است که آیا کران درونی داده شده در بخش قبل با ناحیه ظرفیت برابر است، و اگر نیست چقدر با آن فاصله دارد؟ مثلا آیا میتوان با نرخ مجموع $R_1 + R_2 = C_1 + C_2$ بیت فرستاد؟ برای جواب دادن به این سؤال باید به دنبال یک کران بیرونی گشت که محدوده بیرونی ای برای ناحیه ظرفیت مشخص کند. اولین نکته ای که میدانیم این است که R_1 نمیتواند از C_1 بزرگتر شود. مشابها R_2 نمیتواند از C_2 بزرگتر شود. پس قطعا نامساوی های زیر الزامی هستند:

$$R_1 \leq C_1, \qquad R_2 \leq C_2.$$

اما چگونه میتوان کران بیرونی روی نرخ-مجموع $R_1 + R_2$ یافت؟ در مساله کانال دسترسی چندگانه، فرستنده ها از پیام همدیگر مطلع نیستند. در صورتی که آنها را از پیام هم مطلع کنیم، آنوقت توانایی های فرستنده ها را بیشتر کرده ایم. پس اگر حتی در این حالت قوی تر نتوان به نرخ های خاصی دست یافت، در حالت ضعیف تر هم قطعا نمیتوان این کار را انجام داد. مطلع کردن فرستنده ها از پیام همدیگر معادل ادغام کردن دو ورودی کانال و در نظر گرفتن یک کانال

نقطه به نقطه با ورودی $X' = (X_1, X_2)$ و خروجی $Y' = Y$ میباشد که روی آن میخواهیم پیام های M_1 و M_2 را منتقل کنیم. در این حالت پیامی با نرخ معادل $R_1 + R_2$ منتقل شده است و این نرخ باید کمتر از ظرفیت کانال نقطه به نقطه معادل باشد:

$$R_1 + R_2 \leq \max_{p(x_1,x_2)} I(X_1, X_2; Y).$$

کران بالا را با فرض اینکه دو فرستنده از پیام هم مطلع هستند، بدست آوردیم. اما در مساله ما دو فرستنده این قابلیت را ندارند. در کران بالا روی تمامی توزیع های $p(x_1, x_2)$ اجتماع میگیریم، اما از آنجایی که فرستنده ها پیام های مستقل دارند، توزیع ورودی های آنها در هر بار استفاده از کانال باید مستقل باشند. ادعا میکنیم که حتی به کران بیرونی بهتر زیر هم میتوان رسید:

$$R_1 + R_2 \leq \max_{p(x_1)p(x_2)} I(X_1, X_2; Y).$$

هر زمانی که از یک اثبات دیگر (اینجا اثبات وارون نقطه به نقطه) استفاده میکنیم، نگاه کردن به روابطی که در درون اثبات آن وجود دارد ممکن است به ما کمک کند که کران بهتری برای مساله خاص خودمان بدست بیاوریم. اثبات نقطه به نقطه را برای $X = (X_1, X_2)$ و Y مینویسیم:

$$n(R_1 + R_2) = H(M_1 M_2) \leq \cdots \leq I(X_1^n X_2^n; Y^n) \leq \cdots \leq \sum_{i=1}^{n} I(X_{1i} X_{2i}; Y_i).$$

در اثبات نقطه به نقطه هر جمله $I(X_{1i} X_{2i}; Y_i)$ را با $\max_{p(x_1,x_2)} I(X_1, X_2; Y)$ از بالا کران میزنیم. اما میتوانیم در مرحله آخر بجای گرفتن ماکزیمم روی همه توزیع ها، ماکزیمم را روی توزیع های مستقل بگیریم (ورودی های دو فرستنده تنها تابعی از پیام هایشان است، و چون پیام ها از هم مستقلند پس ورودی ها هم از هم مستقلند). پس میتوان به نامساوی قوی تر زیر بر روی نرخ مجموع رسید:

$$R_1 + R_2 \leq C_{12},$$

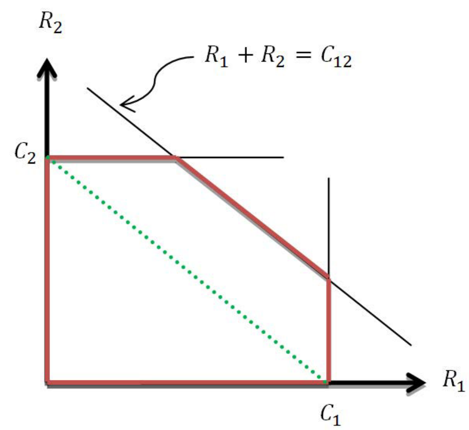
که در آن

$$C_{12} = \max_{p(x_1)p(x_2)} I(X_1, X_2; Y).$$

پس کران بیرونی به این شکل خواهد بود:

$$\begin{aligned}\{(R_1, R_2) \in \mathbb{R}^2 : \quad & 0 \leq R_1 \leq C_1 \\ & 0 \leq R_2 \leq C_2 \\ & R_1 + R_2 \leq C_{12}\}.\end{aligned}$$

این ناحیه یک پنج ضلعی است. پس ناحیه ظرفیت حتما در پنج ضلعی با مرز قرمز زیر قرار خواهد گرفت. از طرف دیگر تمام نقاط درون و روی مرز مثلث قابل دستیابی است . ناحیه واقعی ناحیه ای است که شامل مثلث است، و داخل پنج ضلعی نیز هست.



در حالت کلی هیچکدام از کران درونی و بیرونی ذکر شده در بالا با ناحیه ظرفیت یکی نیستند، اما برای برخی کانال های خاص، یکی یا هر دوی این کران ها بر ناحیه ظرفیت منطبق می شوند.

تمرین ۴ برای کانال بدون تداخل نشان دهید:

$$C_{12} = C_1 + C_2.$$

برای کانال XOR نشان دهید:

$$C_{12} = C_1 = C_2 = 1.$$

برای کانال جمعی نشان دهید که برای محاسبه C_{12}، ماکزیمم در نقطه $p(x_1), p(x_2) \sim \mathcal{B}(\frac{1}{2})$ رخ میدهد و در نتیجه آن داریم:

$$C_{12} = 1.5, \quad C_1 = C_2 = 1.$$

سپس با توجه به بحث قبلی در مورد ناحیه قابل حصول این کانال، نشان دهید که کران بیرونی با ناحیه ظرفیت انطباق دارد.