به نام خدا

جلسه بیست و هفتم

فرض کنیم کانالی با تابع تبدیل Φ داریم.

$$\rho_{XA} = \sum P(x)|x >< x| \otimes \rho_x^A$$

$$\rho_x^A \to \sigma_x^B$$

$$\rho_{XB} = \sum P(x)|x >< x| \otimes \sigma_x^B$$

نرخ قابل حصول: I(X;B)

مانند حالت کلاسیک کلمه-کدهای $x^n(1), x^n(2), \ldots, x^n(2^{nR})$ را تولید می کنیم. به طوری که P(x) یک i.i.d. باشد.

$$\rho_{x^n(m)}^{A^n} = \rho_{x_1(m)}^{A_1} \otimes \rho_{x_2(m)}^{A_2} \otimes$$

در گیرنده $\rho_{x_1(m)}^{A_1}$ تبدیل به $\sigma_{x^n(m)}^{B^n}$ می شود.

$$tr(\prod_{\delta}^{B^n|x^n(m)} \sigma_{x^n(m)}^{B^n}) \ \geq 1 - \varepsilon$$

$$tr(\prod \sigma_{x^n(m)}^{B^n}) \geq 1 - \varepsilon$$

عملگر E_m را تعریف می کنیم:

$$E_m = \prod^{\sigma^n} \prod^{B^n|x^n(m)} \prod^{\sigma^n}$$

ادعا می کنیم:

$$tr\left(E_m \sigma_{x^n(m)}^{B^n}\right) \geq 1 - \varepsilon$$

فرض کنیم $x^n(m)$ را به اشتباه $x^n(\acute{m})$ انتخاب کنیم:

$$E\{\, tr\left(E_{\acute{m}} \sigma_{x^n(m)}^{B^n}\right)\} = E\{tr(\prod_{\delta} \prod^{B^n|x^n(m)} \prod_{\delta} \sigma_{x^n(m)}^{B^n}$$

$$E_{x^n(\acute{m})} tr(\prod_{\delta} \prod^{B^n|x^n(m)} \prod_{\delta} \sum P(\, x^n(m)) \sigma_{x^n(m)}^{B^n})$$
$$= E\{tr\left(\prod_{\delta} \prod^{B^n|x^n(m)} \prod_{\delta} \sigma^{B^n}\right\} (I)$$

و چون می دانیم:

$$\frac{1}{1-\varepsilon}2^{-n(H(B)+\varepsilon)}\prod_{\delta} \leq \prod_{\delta}^{\sigma^{B^n}} \prod_{\delta} \leq\ 2^{-n(H(B)+\varepsilon)}\prod_{\delta}$$

بنابراین:

$$(I) \leq E\{tr(\prod^{B^n|x^n(m)} 2^{-n(H(B)+\varepsilon)}\prod_{\delta})\}^{(1)} \leq E\{tr(\prod^{B^n|x^n(m)} 2^{-n(H(B)-\varepsilon)}$$
$$\leq 2^{-n(H(B)-\varepsilon)}2^{-n(H(B|X)-\varepsilon)} = 2^{-n(I(B;X)-2\varepsilon)}$$

(1) برقرار است چون:

$$tr(AB) \leq tr(AC)$$

وقتی:

$$B \leq C$$

می خواهیم یک اندازه گیزی تعریف کنیم که در صورتی که m=1 باشد بعد از اندازه گیری با احتمال زیاد 1 و با احتمال کم سایر اعداد دریافت شود.

برای ترکیب چند اندازه گیری:

$$\acute{E}_m = (\sum E_i)^{1/2}E_m(\sum E_i)^{-1/2}$$

$$\sum \acute{E}_i = \mathrm{I}$$

$$I-(S+T)^{-\frac{1}{2}}S(S+T)^{\frac{1}{2}} \leq 2(I-S)+4T$$

$$I-\acute{E}_m \leq 2(I-E_m)+4\sum_{m\neq m'}\acute{E}_m$$

احتمال خطا:

$$E\{P_e(1)\} = E\{tr\big(I-\acute{E}_1\big)\sigma_{x^n(1)}^{B^n}\} \leq 2E\{tr(I-E_1)\sigma_{x^n(1)}^{B^n}\} + 4E\{\sum_{m\neq 1} tr(\acute{E}_{m\prime})\,\sigma_{x^n(1)}^{B^n}$$

چون داریم

$$tr(\acute{E}_{m\prime}) = 2^{-nI(B;X)}$$

و بنابراین:

$$E\left\{\sum_{m\neq 1} tr(\acute{E}_{m'})\,\sigma_{x^n(1)}^{B^n}\right\} = 2^{-n(R-I(B;X))}$$

و چون R<I(X;B) عبارت دوم سمت راست تساوی (II) به صفر میل می کند.

از طرفی می دانیم:

$$E\{tr(I-E_1)\sigma_{x^n(1)}^{B^n}\} \leq \varepsilon$$

در معادله

$$\rho_{XA} = \sum P(x)|x><x|\otimes\rho_x^A$$

می توان ρ_x^A را pure در نظر گرفت.

مثال:

فرض کنید کانالی داریم که در آن:

$$\epsilon(|\Psi\times\Psi|) = P|\Psi\times\Psi| + \bar{P}\left(\frac{1}{2}I\right)$$

می خواهیم مقدار mutual information را حساب کنیم.

$$H(B)-H(B|X) \leq \sum H(B|X=x)\,P(x) = h\left(\frac{1+p}{2}\right)$$

$$H(B)-H(B|X) \leq 1-h\left(\frac{1+p}{2}\right)$$

که برابر با ظرفیت کانال است. عدد 1 به این دلیل در فرمول قرار گرفت که کیوبیت دوحالتی است.

اگر یک کانال Cq داشته باشیم در آن صورت نرخ قابل حصول به صورت C=max{I(X;B)} برای توزیع P(x) خواهد بود.

وارون آن هم مثل حالت کلاسیک خواهد بود:

$$X = x \rightarrow \sigma_x^B$$

$$M \xrightarrow{Mapping} X^n \xrightarrow{Sending} B^n \xrightarrow{Measuring} \widehat{M}$$

$$H(M) \approx I\left(MX^n;\widehat{M}\right) \leq I(MX^n;B^n) = I(X^n;B^n) + I(M;B^n|X^n) \quad (II)$$

چون:

$$\rho_{X^n MB} = \sum_{x^n m} P(mx^n)|m \times m| \otimes |x^n \times x^n| \otimes \sigma_{x_n}^{B^n} = \sum_{x^n} P(x^n)[\sum_{m} P(m|x^n)|m \times m| \otimes \sigma_{x_n}^{B^n}$$

بنابراین عبارت دوم (II) برابر با صفر خواهد بود.

$$(II) = H(B^n) - H(B^n|x^n) \leq \sum H\,(B_i) - \sum P(x^n)\,H(B^n|x^n) \quad (III)$$

چون سیستم .i.i.d است:

$$H(B^n..x^n) = \sigma_{x_1}^{B^1} \otimes \sigma_{x_2}^{B^2} \ldots = \sigma_{x_n}^{B^n}$$

بنابراین آنتروپی مجموع برابر جمع آنتروپی‌هاست. پس:

$$(\mathrm{III})\,^{*} = \sum H(B_i) - \underbrace{\sum_{i} \sum_{x^n} P(x^n) H(B_i\,|x_i)}_{\sum_i H(B_i|x_i)}$$

(*) برقرار است چون:

$$\sum P(x^n)\,H(B_i|X_i = x_i) = \sum_{x_i} \sum_{i_{1:i-1} x_{i+1:n}} P(x_i) P(x_{1:i-1}, x_{i+1:n}|x_i)\,H(B_i|X_i = x_i)$$
$$= \sum_{x_i} P(x_i) H(B_i|X_i = x_i) \underbrace{\sum_{x_{1:i-1} x_{i+1:n}} P(\ldots\ldots x_i)}_{=1}$$

فرض کنید یک کانال کلاسیک و یک پیام کلاسیک دارید که قصد انتقال این پیام را از این کانال دارید.

فرض کنید Shared-Randomness بین A و B داریم.

یک اندازه‌گیری که A روی M انجام می‌دهد:

$$\varepsilon_m(A) = A^n$$

$$D_{y^n(B)} = \widehat{M}$$

در زمان نوشتن converse تنها متغیرهایی را که در یک لحظه زمانی وجود دارد، در نظر می گیریم. مثلاً $I(A;Y^n)$ معنایی ندارد چون A از بین می‌رود و x^n را تولید می‌کند و تا x^n تولید نشود Y^n معنی ندارد.

$$\begin{aligned} I(M,\widehat{M}) &\le I(M;BY^n) \le I(MX^n,BY^n) = \overbrace{I(M;B)}^{=0} + I(M;Y^n|B) \le I(MBX^n;Y^n) \\ &= I(X^n;Y^n) + \overbrace{I(MB;Y^n|X^n)}^{=0} \end{aligned}$$

ادعا می‌کنیم $(MB;Y^n|X^n)$ صفر است چون اگر X^n را بدانیم Y^n مشخص می‌شود.

$$\begin{aligned} \rho_{X^nMY^nB} &= \sum_{x^n y^n m} P(x^n\, x)|x\times m|\otimes|x^n\times x^n|\rho^B_{mx^n}P(y^n|x^n)|y^n\times y^n| \\ &= \sum_{x^n}\Big(\sum_{x} P(x|x^n)\,|m\times m|\otimes|x^n\times x^n|\otimes\rho_m B^n_{x^n}\Big)\otimes\Big(\sum_{y^n} P(y^n|x^n)|y^n\times y^n|\Big) \end{aligned}$$