

آرژ اطلاعات و آرن علمی ايران  
تهيه مدارك



دانشگاه تهران  
دانشگاه تيريز  
دانشكده فيزيك

۱۳۸۲ / ۱۶ / ۱ -

پايان نامه:

جهت دريافت درجه كارشناسي ارشد در رشته فيزيك

موضوع:

## مخابرات كوانتومي دو طرفه

اساتيد راهنما:

دكتور محمدعلي جعفري زاده

دكتور منوچهر كلافي

استاد مشاور:

مهندس مريد نقش آرا

تهيه و تنظيم:

اميررضا باغبان پور

بهار ۱۳۸۲

۴۷۵۴۵

تقدیم به:

مادر

و

روح پدر درگذشته‌ام

و با تشکر از استاد محترم

استاد رهنما: دکتر محمد علی جعفری زاده - دکتر منوچهر کلافی

استاد مشاور: مهندس حمید نقش آرا

مقطع تحصیلی: کارشناسی ارشد رشته: فیزیک گرایش: نظری دانشگاه: تبریز  
 دانشکده: فیزیک تاریخ فارغ التحصیلی: تابستان ۸۲ تعداد صفحه: ۸۷

کلید واژه ها: مخبرات ، اطلاعات ، کوانتوم ، ظرفیت ، درهم تنیدگی

### چکیده:

در این پایان نامه، علم مخبرات کوانتومی را مورد بررسی قرار خواهیم داد. تعریف‌ها و کمیت‌های مورد نیاز را تعریف کرده و خواص آنها را بررسی می‌کنیم. با اینکه بعضی از تعریف‌های اولیه در تشابه با علم مخبرات کلاسیکی صورت گرفته است ولی در اینجا با مسایلی سروکار خواهیم داشت که ماهیتی کاملاً کوانتومی دارند و برای آنها معادلی در دنیای کلاسیکی نمی‌توان پیدا کرد. از جمله این خواص، عدم تشخیص‌پذیری کامل حالتها از هم و پدیده درهم تنیدگی است.

بطور کلی بحث مخبرات کوانتومی را به سه قسمت کلی می‌توانیم تقسیم کنیم: ۱- فشرده سازی اطلاعات کوانتومی، به معنی نمایش خروجی‌های یک منبع کوانتومی با کمک منابع کمتر با استفاده از مفهوم زیر فضاهای نوعی. ۲- ارسال اطلاعات کلاسیکی با کمک کانال کوانتومی. در این نوع مخبرات عدم تشخیص‌پذیری حالت‌های کوانتومی از یکدیگر باعث کاهش ظرفیت کانال می‌شود. برای اینکه از حداکثر ظرفیت کانال بتوان استفاده کرد از کدگذاری بلوکی استفاده می‌کنیم و در قسمت دکد کننده از مشاهده‌گری استفاده می‌کنیم که بطور هم‌زمان (مشاهده‌گر درهم تنیده) بر روی بلوک داده‌ها اندازه‌گیری انجام می‌دهد. با کمک درهم تنیدگی به نوع دیگری از کدگذاری به نام کدگذاری فوق فشرده خواهیم رسید. ۳- ارسال اطلاعات کوانتومی بر روی کانال کوانتومی نویز دار. در این نوع مخبرات، هدف ما ارسال یک سری حالت کوانتومی با کمترین میزان اعوجاج است. در اینجا برای اینکه به حداکثر ظرفیت کانال برسیم باید از فضاهای هیلبرت گسترش یافته استفاده کنیم و نباید حالت‌های کوانتومی دکد کننده را محدود به حالت‌های ضریبی کنیم.

## فهرست مطالب

صفحه	عنوان
۱	مقدمه
<b>فصل ۱: بررسی منابع</b>	
۵	(۱-۱) آنتروپی شانون
۵	(۲-۱) آنتروپی شرطی
۶	(۳-۱) آنتروپی نسبی (Relative Entropy)
۷	(۴-۱) اطلاعات دوتائی (Mutual Information)
۸	(۵-۱) بررسی خواص آنتروپی
۱۰	(۶-۱) آنتروپی کوانتومی (Quantum Entropy) یا آنتروپی فون نیومن
۱۰	(۷-۱) آنتروپی نسبی کوانتومی
۱۲	(۸-۱) بررسی خواص آنتروپی فون نیومن
۱۶	(۹-۱) در هم تنیدگی (Entanglement)
۱۸	(۱۰-۱) عملیات کوانتومی (Quantum Operations)
۱۹	(۱۱-۱) نمایش‌های عملیات کوانتومی
۲۱	(۱۲-۱) فضای مرجع (Reference Space)
۲۲	(۱۳-۱) خالص‌ساز (Purification)
۲۳	(۱۴-۱) تبادل آنتروپی (Entropy Exchange)
۲۴	(۱۵-۱) وفاداری (فیدلیتی) (Fidelity)
۲۵	(۱۶-۱) وفاداری در هم تنیدگی (Entanglement Fidelity)
<b>فصل ۲: روشها</b>	
۳۰	(۱-۲) کدگذاری
۳۳	(۲-۲) کد گذاری Huffman
۳۴	(۳-۲) کدگذاری کوانتومی
۳۶	(۴-۲) فشردن سازی داده‌های کوانتومی (Quantum Data Compression)
۳۹	(۵-۲) سیستم‌های در هم تنیده (Entangled Systems)

عنوان	صفحه
۶-۲) ارسال اطلاعات کلاسیک بر روی کانال کوانتومی .....	۴۱
۷-۲) آنسابل سیگنال‌های بهینه .....	۵۱
<b>فصل ۳: نتایج و بحث</b>	
۱-۳) کدگذاری کانال نویزدار (Noisy Channel Coding) .....	۵۷
۲-۳) نامساوی کوانتومی فانو (Quantum Fano Inequality) .....	۵۸
۳-۳) اطلاعات مرتبط (Coherent Information) .....	۵۹
۴-۳) یک لم در مورد وفاداری درهم تنیدگی .....	۶۲
۵-۳) مشخصات کوانتومی اطلاعات مرتبط	
۶۳) (Quantum Characteristics of the Coherent Information) .....	۶۳
۶-۳) فرمول‌نویسی ریاضی کدگذاری کانال نویزدار .....	۶۶
۷-۳) حدهای بالا برای ظرفیت کانال .....	۶۸
۸-۳) بررسی بعضی خواص $C(N)$ .....	۷۰
۹-۳) پروتکل‌های دیگر کدگذاری .....	۷۲
۱۰-۳) کانال‌هایی که یک مشاهده‌گر کلاسیک دارند .....	۷۴
۱۱-۳) اصلاح خطا (Error Correction) .....	۷۸
نتیجه‌گیری و پیشنهادها .....	۸۳
منابع .....	۸۶

## مقدمه

برای بررسی اطلاعات، ابتدا باید آن را کمی کرد. یعنی باید گفت یک پیام (Message) چقدر اطلاعات (Information) دارد. شانون برای اندازه گیری اطلاعات مفهوم آنتروپی را پیشنهاد کرد و واحد آن را «بیت» نامید. بدین صورت که آنتروپی یک آنسابل از حالت های تصادفی که همان پیام ها می باشد، بیان می دارد که با ارسال هر پیام بطور متوسط چقدر اطلاعات منتقل می شود.

در علم اطلاعات کوانتومی، راهی که در پیش می گیریم و مفاهیمی که تعریف می کنیم از علم اطلاعات کلاسیک الهام گرفته می شود.

در فصل اول مفاهیم مورد نیاز در علم اطلاعات کلاسیک و کوانتوم را بررسی می کنیم. در این فصل مفهوم آنتروپی به عنوان معیاری از اطلاعات معرفی می شود و روابطی بین آنتروپی های مختلف بدست آورده می شود و خواص آن مورد بررسی قرار می گیرد.

عملیات کوانتومی، عملگر هایی هستند که بر روی عملگرهای کوانتومی و در حالت خاص بر روی ماتریس های چگالی اثر می کنند. پیام های ما در حالت کلی با کمک ماتریس های چگالی بیان می شوند. اثر کانال مخابراتی و محیط خارجی بر روی حالت های کوانتومی را توسط عملیات کوانتومی نشان می دهیم. در این فصل دو نوع نمایش برای عملیات کوانتومی معرفی می کنیم.

در بحث اطلاعات و مخابرات همواره یک سوال اساسی داریم: اطلاعات بعد از ارسال چقدر دست نخورده باقی مانده است؟ در مورد اطلاعات کلاسیکی این مساله با بررسی احتمال خطا در دریافت پیام دیگری به جای پیام ارسال شده بررسی می شود. در حالت کوانتومی میزان یکسان بودن یا همپوشانی حالت های ارسالی با حالت های دریافت شده مد نظر می باشد. این یکسان بودن خروجی با ورودی با کمیتی به نام «وفاداری» (Fidelity) بیان می شود [16]. وفاداری آخرین موضوعی است که در این فصل مورد بررسی قرار می گیرد. در این قسمت سه نوع وفاداری یعنی: وفاداری، وفاداری درهم تنیدگی و وفاداری زیر فضا را معرفی می کنیم و خواص آنها را بیان می کنیم.

در فصل دوم مساله اطلاعات و ارتباطات کوانتومی را از نزدیکتر بررسی می‌کنیم. دو مساله اساسی که توسط شانون مطرح شدند به این قرار بود:

۱- یک پیام، به چه مقداری می‌تواند فشرده شود؟ (قضیه کدگذاری بدون نویز، Noiseless Coding Theorem)

۲- بر روی یک کانال نویزدار با چه میزانی می‌توان تبادل اطلاعات کرد؟ (قضیه کدگذاری کانال نویزدار، Noisy Channel Coding Theorem)

برای حالتی که اطلاعات کوانتومی هستند، مساله اول را در این فصل و مساله دوم را در فصل سوم بیان می‌کنیم.

فشرده سازی اطلاعات به معنی نمایش حالت‌های کوانتومی با کمک منابع کمتر می‌باشد. به این کار کد گذاری می‌گوییم.

یکی از حالت‌هایی که در مورد کد گذاری بررسی خواهیم کرد، حالتی است که سیستم مورد نظر که می‌خواهیم آنرا فشرده کنیم، با سیستم دیگری درهم تنیده باشد. خواهیم دید که بعد از کد و سپس دکد کردن سیستم مورد نظر باز هم می‌توانیم درهم تنیدگی را به میزان زیادی حفظ کنیم.

موضوع دیگری که در این فصل به آن خواهیم پرداخت ارسال اطلاعات کلاسیکی با کمک کانال‌های کوانتومی است. در اینجا هر حالت کوانتومی نماینده یک حالت کلاسیکی است. در این قسمت مفهومی به نام ظرفیت کلاسیکی کانال کوانتومی را معرفی می‌کنیم. ظرفیت یک کانال به ما می‌گوید که در هر بار استفاده از کانال کوانتومی حداکثر چند بیت کلاسیکی می‌توانیم منتقل کنیم. در این بخش با معرفی یک نوع کد گذاری بلوکی و دکد کننده‌ای که یک مشاهده پذیر درهم تنیده است به ظرفیت کانالی برابر با آنتروپی ماتریس چگالی واحد در فضایی با ابعاد حالت کوانتومی ارسالی می‌رسیم.

همانطور که می‌دانید یکی از منابعی که در علم اطلاعات کوانتومی در دسترس داریم، درهم تنیدگی است. استفاده از پدیده درهم تنیدگی در ارسال اطلاعات کلاسیکی با کمک کانال‌های

کوانتومی، منجر به نوع خاصی از کد گذاری می‌شود که به «کد گذاری فوق فشرده» موسوم است. در این نوع کد گذاری دو ذره کوانتومی داریم که در حالت درهم تنیده قرار دارند، یکی از آن دو در نزد فرستنده و دیگری در نزد گیرنده می‌باشد.

در ارسال اطلاعات کلاسیکی، برای اینکه بتوانیم از حداکثر ظرفیت کانال استفاده کنیم باید به دو مورد توجه کنیم، یکی انتخاب مشاهده پذیر دزد کننده و دیگری انتخاب آنسابل حالتهای کوانتومی ارسالی یا به عبارتی آنسابل بهینه. در انتهای این فصل خواص آنسابل بهینه را مورد بررسی قرار می‌دهیم.

در فصل آخر به بررسی ظرفیت کانال کوانتومی برای ارسال حالتهای کوانتومی می‌پردازیم. در این فصل کمیتی به نام اطلاعات مرتبط (Coherent Information) را تعریف می‌کنیم. این کمیت معادل کوانتومی کمیت کلاسیکی اطلاعات دوتایی (Mutual Information) است، که در تعریف ظرفیت کانال های کلاسیکی و یا ظرفیت کلاسیکی کانال های کوانتومی به کار می‌رود. این معادل بودن حداقل در دو مورد نقض می‌شود. یکی از این دو مورد به علت وجود خاصیت درهم تنیدگی در سیستم های کوانتومی است.

در این فصل چند نوع ظرفیت کوانتومی معرفی می‌کنیم: ظرفیت کانال برای کد کننده های یکایی، ظرفیت کانال برای کد کننده های کلی و ظرفیت کانال برای کانال هایی که یک مشاهده گر کلاسیکی دارند. در نوع اخیر مشاهده گر می‌تواند بر روی کانال، محیط، و یا هر دو اندازه گیری انجام دهد. ظرفیت کانال برای کانال هایی که یک مشاهده گر کلاسیکی دارند بزرگتر از ظرفیت کانال های مشاهده نشده می‌باشد، بطوری که می‌توان مواردی یافت که ظرفیت کانال مشاهده نشده برابر با صفر بوده ولی ظرفیت همان کانال در حالتی که یک مشاهده کننده کلاسیکی داریم مخالف صفر و برابر با عدد بزرگی می‌باشد.

در پایان این فصل نیز قضیه بی مطرح می‌کنیم که شرط لازم و کافی برای وجود یک کد اصلاح خطای کامل را بیان می‌کند.



## بررسی منابع

## ۱-۱) آنتروپی شانون

همانطور که در مقدمه اشاره شد، برای بررسی اطلاعات ابتدا باید آنرا کمی کنیم.

فرض کنیم کسی به ما می‌گوید که مقدار متغیر  $X$ ، ۵ است، در اینجا چقدر اطلاعات کسب کرده‌ایم؟ پاسخ این سؤال بستگی به میزان دانش قبلی ما در مورد متغیر  $X$  دارد. یعنی: اگر ما از قبل مقدار متغیر  $X$  را می‌دانستیم با شنیدن دوباره مقدار آن هیچ اطلاعات جدیدی کسب نکرده‌ایم. ولی اگر مقدار آنرا از قبل ندانیم و فقط بدانیم که  $X$ ، نتیجه خروجی پرتاب یک تاس است. میزان اطلاعاتی که از شنیدن مقدار آن دریافت کرده‌ایم، دیگر صفر نیست. در واقع می‌توانیم اطلاعات بدست آمده را معادل یا عدم قطعیت در مورد یک حادثه بدانیم.

اگر  $X$ ، یک متغیر تصادفی باشد که مقدار  $x$  را با احتمال  $P(x)$  بگیرد، محتوی اطلاعات  $X$  را بصورت زیر تعریف می‌کنیم:

$$H(X) = -\sum_x p(x) \log_2 p(x)$$

$H(X)$  را می‌توانیم به عنوان مقدار اطلاعاتی که بطور متوسط از دانستن  $X$  بدست می‌آوریم، بدانیم.  $H(X)$  را آنتروپی شانون می‌نامیم. واحد آنتروپی شانون، بیت است.

مثال: فرض کنید یک پیام می‌تواند، یکی از سمبل‌های  $a$ ،  $b$  یا  $c$  باشد.  $a$  با احتمال  $1/2$ ،  $b$  با احتمال  $3/8$  و  $c$  با احتمال  $1/8$  رخ می‌دهد. اگر سمبل دریافتی ما  $a$  باشد

$$-\log_2 P_a = -\log_2 1/2 = 1$$

۱ بیت، اطلاعات کسب کرده‌ایم، اگر  $b$  باشد

$$-\log_2 P_b = -\log_2 3/8 \cong 1.41$$

تقریباً 1.41 بیت و اگر  $c$  باشد

$$-\log_2 P_c = -\log_2 1/8 = 3$$

۳ بیت اطلاعات کسب کرده‌ایم. بطور متوسط با دریافت هر سمبل،

$$H(X) = -1/2 \log_2 1/2 - 3/8 \log_2 3/8 - 1/8 \log_2 1/8 \cong 1.40$$

1.40 بیت اطلاعات کسب می‌کنیم.

## ۱-۲) آنتروپی شرطی

فرض کنیم دو متغیر تصادفی  $X$  و  $Y$  داریم آنتروپی شرطی را بصورت زیر تعریف می‌کنیم:

$$H(X|Y) = -\sum_x p(x|y) \log_2 p(x|y)$$

آنتروپی شرطی متوسط می‌شود

$$H(X|Y) = \sum_y p(y) H(X|y)$$

با جایگذاری بدست می‌آوریم

$$H(X|Y) = -\sum_{x,y} p(x,y) \log_2 p(x|y)$$

همین‌طور خواهیم داشت

$$\begin{aligned} H(X|Y) &= -\sum_{x,y} p(x,y) \log_2 p(x|y) = -\sum_{x,y} p(x,y) \log_2 \frac{p(x,y)}{p(y)} \\ &= -\sum_{x,y} p(x,y) \log_2 p(x,y) + \sum_{x,y} Y(x,y) \log_2 p(y) \\ &= H(X,Y) - H(Y) \end{aligned}$$

نتیجه: با توجه به تعریف آنتروپی، می‌دانیم که مقدار آن همواره غیرمنفی است بنابراین

$$H(X|Y) \geq 0 \rightarrow H(X,Y) \geq H(Y)$$

در روابط بالا،  $H(X,Y)$  آنتروپی مشترک (Joint Entropy) نامیده می‌شود.

### ۳-۱) آنتروپی نسبی (Relative Entropy):

این آنتروپی به خودی خود سودمند نیست ولی در اثبات روابط دیگر برای آنتروپی که حالت

خاصی از این آنتروپی می‌شوند بسیار مفید است این آنتروپی بصورت زیر تعریف می‌شود

$$H(p(x) \| q(x)) \equiv \sum_x p(x) \log_2 \frac{p(x)}{q(x)}$$

$p(x)$  و  $q(x)$  دو توزیع تصادفی برای مجموعه اندیس‌های  $x$  هستند.

در محاسبه مقدار بالا تعریف می‌کنیم  $-0 \log_2 0 \equiv 0$  و  $-P(x) \log_2 0 \equiv +\infty$

قضیه: ثابت کنید آنتروپی نسبی غیرمنفی است.

برای  $x$ های مثبت داریم:  $\ln x \leq x - 1$ . اگر و تنها اگر  $x=1$  باشد، نامساوی به تساوی تبدیل

می‌شود. بنابراین

$$\begin{aligned}
 H(p(x) \| q(x)) &= -\sum p(x) \log_2 \frac{q(x)}{p(x)} \geq -\frac{1}{\ln 2} \sum_x p(x) \left(1 - \frac{q(x)}{p(x)}\right) \\
 &= \frac{1}{\ln 2} \sum_x (p(x) - q(x)) = \frac{1}{\ln 2} (1 - 1) = 0 \\
 \Rightarrow H(p(x) \| q(x)) &\geq 0
 \end{aligned}$$

تساوی وقتی و فقط وقتی است که برای تمام  $x$  ها  $\frac{p(x)}{q(x)} = 1$  باشد. یعنی هر دو توزیع یکسان باشند.

قضیه: اگر  $X$  یک متغیر تصادفی با  $d$  حالت ممکن باشد ثابت کنید:  $H(X) \leq \log_2 d$

$$q(x) \equiv \frac{1}{d}$$

$$H(p(x) \| q(x)) = H(p(x) \| \frac{1}{d}) = -H(X) - \sum p(x) \log \frac{1}{d}$$

$$= \log d - H(X) \geq 0$$

$$\Rightarrow H(X) \leq \log_2 d$$

#### (۴-۱) اطلاعات دوتائی (Mutual Information)

این کمیت نشان می‌دهد که  $X$  و  $Y$  با هم چه مقدار اطلاعات دارند یا به تعبیری دیگر، اگر  $X$  اطلاعات ارسال شده و  $Y$  اطلاعات دریافت شده باشد این کمیت به ما می‌گوید که چه مقدار اطلاعات در مورد  $X$  از طریق کانال نویزدار دریافت شده است.

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

ورودی کانال  $x_i$  ها با احتمال  $p(x_i)$  هستند و خروجی کانال  $y_k$  ها با احتمال  $p(y_k)$  هستند.

خواص کانال توسط احتمال شرطی  $p(y_k|x_i)$  مشخص می‌شود. اگر  $X$  کاملاً مستقل از  $Y$  باشد، یعنی

اگر ورودی و خروجی کانال از هم مستقل باشند بطور شهودی متوجه می‌شویم که هیچ اطلاعاتی

منتقل نشده است. بطور ریاضی، در این حالت داریم

$$H(X|Y) = H(X) \rightarrow H(X:Y) = H(X) - H(X|Y) = H(X) - H(X) = 0$$

اگر با دانستن  $Y$ ،  $X$  کاملاً مشخص شود، تمام اطلاعات ورودی به خروجی منتقل شده است

در روابط  $H(X:Y)$  داریم

$$H(X|Y) = 0$$

یعنی هیچ ابهامی در مورد  $X$  با دانستن  $Y$  باقی نمانده است.

$$H(X:Y) = H(X) - H(X|Y) = H(X) - 0 = H(X)$$

(۵-۱) بررسی خواص آنتروپی

:Subadditivity

$$H(X, Y) \leq H(X) + H(Y) \quad (۱-۵-۱)$$

برای اثبات این نامساوی، ابتدا نامساوی زیر را ثابت می‌کنیم

$$\sum_K p_K \log_2 q_K \leq \sum_K p_K \log_2 p_K \quad (۲-۵-۱)$$

می‌دانیم برای  $x > 0$ :

$$\ln x \leq x - 1$$

$$x = \frac{q_K}{p_K} \rightarrow \ln \frac{q_K}{p_K} \leq \frac{q_K}{p_K} - 1$$

$$\sum_K p_K \log_2 \frac{q_K}{p_K} = \frac{1}{\ln 2} \sum_K p_K \ln \frac{q_K}{p_K} \leq \frac{1}{\ln 2} \sum_K p_K \left( \frac{q_K}{p_K} - 1 \right) = \frac{1}{\ln 2} \sum_K (q_K - p_K) = 0$$

$$\sum_K p_K \log_2 \frac{q_K}{p_K} \leq 0 \Rightarrow \sum_K p_K \log_2 q_K \leq \sum_K p_K \log_2 p_K$$

اثبات رابطه subadditivity:

$$q(x, y) = p(x)p(y)$$

با کمک رابطه‌ای که در بالا بدست آوردیم

$$\sum_{x,y} p(x, y) \log q(x, y) \leq \sum_{x,y} p(x, y) \log p(x, y)$$

$$\sum_{x,y} p(x, y) \log(p(x)p(y)) \leq \sum_{x,y} p(x, y) \log p(x, y)$$

$$\sum_{x,y} p(x, y) \log p(x) + \sum_{x,y} p(x, y) \log p(y) \leq \sum_{x,y} p(x, y) \log p(x, y)$$

$$\sum_x p(x) \log p(x) + \sum_y p(y) \log p(y) \leq \sum_{x,y} p(x, y) \log p(x, y)$$

$$-\sum_x p(x) \log p(x) + \sum_y p(y) \log p(y) \geq -\sum_{x,y} p(x, y) \log p(x, y)$$

$$H(X) + H(Y) \geq H(X, Y)$$

نتیجه: تساوی فقط و فقط وقتی رخ می‌دهد که  $p(x, y) = q(x, y)$  باشد یعنی  $p(x, y) = p(x)p(y)$  باشد

و این یعنی  $X$  و  $Y$  از هم مستقل باشند.

با استفاده از رابطه Subadditivity:

$$H(X, Y) \leq H(X) + H(Y) \rightarrow H(X, Y) - H(Y) \leq H(X) \\ \Rightarrow H(X|Y) \leq H(X)$$

**: Strong Subadditivity (۲-۵-۱)**

$$H(X, Y, Z) + H(X) \leq H(X, Y) + H(X, Z) \quad (۳-۵-۱)$$

اثبات این رابطه از subadditivity آنتروپی شرطی نتیجه می‌شود. بنابراین ابتدا آن را اثبات می‌کنیم

$$q(x, y, z) = p(y|x) p(z|x), p(x, y, z) = p((y, z)|x)$$

با کمک رابطه (۲-۵-۱) داریم

$$\sum_{y,z} p((y, z)|x) \log p((y, z)|x) \geq \sum_{y,z} p((y, z)|x) \log p(y|x) p(z|x) \\ = \sum_{y,z} p((y, z)|x) (\log p(y|x) + \log p(z|x)) = \sum_{y,z} p((y, z)|x) \log p(y|x) + \\ \sum_{y,z} p((y, z)|x) \log p(z|x) = \sum_y p(y|x) \log p(y|x) + \sum_z p(z|x) \log p(z|x) \\ \Rightarrow H((Y, Z)|X) \leq H(Y|X) + H(Z|X) \\ \Rightarrow H((Y, Z)|X) \leq H(Y|X) + H(Z|X)$$

حال با کمک این رابطه Strong subadditivity را اثبات می‌کنیم:

$$H(Y, Z, X) - H(X) \leq H(Y, X) - H(X) + H(Z, X) - H(X) \\ \Rightarrow H(X, Y, Z) + H(X) \leq H(X, Y) + H(X, Z)$$

**۳-۵-۱) نامساوی "پردازش داده" Data Processing Inequality**

فرض کنیم،  $X \rightarrow Y \rightarrow Z$  یک زنجیره مارکوف است. یعنی  $Z$  فقط به متغیر تصادفی قبل از

$$p(z|y, x) = p(z|y)$$

خود وابسته است:

بنابراین خواهیم داشت:

$$H(X) \geq H(X: Y) \geq H(X: Z) \quad (۴-۵-۱)$$

به این نامساوی، نامساوی پردازش داده می‌گوئیم.

اثبات:

$$H(X: Y) = H(X) - H(X|Y), H(X|Y) \geq 0 \\ \Rightarrow H(X) \geq H(X: Y)$$

قسمت دوم نامساوی:

برای اثبات این قسمت باید ثابت کنیم اگر  $X \rightarrow Y \rightarrow Z$  یک فرآیند مارکوف باشد،

$Z \rightarrow Y \rightarrow X$  هم یک فرآیند مارکوف است:

$$Z \rightarrow Y \rightarrow X$$

$$p(x|y,z) = \frac{p(x,y,z)}{p(y,z)} = \frac{p(z|x,y)p(x,y)}{p(z|y)p(y)} = \frac{p(z|y)p(x,y)}{p(z|y)p(y)} = p(x|y)$$

ادامه اثبات قسمت دوم نامساوی پردازش داده:

قسمت دوم نامساوی به  $H(X|Y) \leq H(X|Z)$  تبدیل می‌شود. همانطور که گفتیم  $Z \rightarrow Y \rightarrow X$  یک

فرآیند مارکوف می‌شود، بنابراین  $H(X|Y) = H(X|Y,Z)$  پس باید ثابت کنیم  $H(X|Y,Z) \leq H(X|Z)$

$$H(X,Y,Z) - H(Y,Z) = H(X|Y,Z) \leq H(X|Z) = H(X,Z) - H(Z)$$

یعنی باید ثابت کنیم:

$$H(X,Y,Z) + H(Z) \leq H(X,Z) + H(Y,Z)$$

این رابطه همان رابطه Strong subadditivity است که قبلاً ثابت شده است.

## ۶-۱) آنتروپی کوانتومی (Quantum Entropy) یا آنتروپی فون نیومن

سیستم  $Q$  را در حالت  $\rho^Q$  در نظر بگیرید. آنتروپی فون نیومن را بصورت زیر تعریف می‌کنیم

$$S(\rho^Q) \equiv -\text{tr} \rho^Q \log_2 \rho^Q$$

اگر  $\lambda_i > 0$  ویژه حالت‌های  $\rho^Q$  با ویژه مقادیر  $\lambda_i$  باشد

$$S(\rho^Q) = -\sum \lambda_i \log_2 \lambda_i = H(\bar{\lambda})$$

بنابراین اگر  $\dim H^Q = d$  باشد

$$\Rightarrow 0 \leq S(\rho^Q) \leq \log d$$

$S(\rho^Q) = 0$  اگر و تنها اگر  $\rho^Q$  حالت خالص (Pure) باشد. زیرا اگر  $\rho^Q$  خالص باشد، فقط

یک ویژه مقدار مخالف صفر دارد و آنتروپی شانون یک عدد تنها، صفر می‌شود و اگر  $S(\rho^Q) = 0$

باشد، نتیجه می‌گیریم  $\rho^Q$  تنها، یک ویژه مقدار مخالف صفر دارد بنابراین یک حالت خالص است.

## ۷-۱) آنتروپی نسبی کوانتومی

مرکز اطلاعات مدرک علمی ایران  
تمت مدرک