

نظریه اطلاعات کوانتومی - بخش دوم

وحیدکریمی پور- دانشکده فیزیک - دانشگاه صنعتی شریف

۱۷ اردیبهشت ۱۳۹۴

۱ مقدمه

بعد از مقدماتی که در درس گذشته آموختیم، می توانیم به طرح یک سوال اساسی در نظریه اطلاعات کوانتومی بپردازیم. از خود می پرسیم که اطلاعات کوانتومی را تا چه حد می توان فشرده کرد؟ این سوال درست مشابه سوالی است که در مورد اطلاعات کلاسیک از خود پرسیدیم. نخست می بایست صورت این سوال را دقیق کنیم. فرض کنید که آلیس آزمابلی از حالت های خالص دو بعدی (کیوبیت) مثل $X = \{|\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle, \dots, |\phi_n\rangle\}$ در اختیار دارد. هر حالت $|\phi_i\rangle$ با احتمال p_i در این آزمابلی وارد شده است. هر حالت نیز در یک فضای هیلبرت d بعدی قرار گرفته است و حالت ها لزوماً برهم عمود نیستند. این آزمابلی با ماتریس چگالی زیر توصیف می شود:

$$\rho = \sum_i p_i |\phi_i\rangle \langle \phi_i|, \quad (1)$$

و آنتروپی فون نویمان آن برابر است با $S(\rho) = -\text{tr}(\rho \log \rho)$. می دانیم که $0 \leq S(\rho) \leq 1$.

اگر آلیس بخواهد یکی از این حالت ها را در جایی از یک هارد دیسک کوانتومی ذخیره کند، لازم است که آن جای بخصوص گنجایش یک فضای هیلبرت d بعدی را داشته باشد. اگر آلیس بخواهد رشته های بلندی به طول n از این آنزامل را مثل رشته های

$$|\Phi\rangle_I = |\phi_{i_1}\rangle \otimes |\phi_{i_2}\rangle \otimes |\phi_{i_3}\rangle \otimes \dots |\phi_{i_n}\rangle, \quad (2)$$

ذخیره کند، می بایست قسمتی که چنین حالتی در آن ذخیره می شود گنجایش یک فضای هیلبرت d^n بعدی را داشته باشد. همین گنجایش برای وقتی که آلیس می خواهد این حالت ها را به شخص دیگری مثلاً باب بفروشد، مورد نیاز است. حال سوال این است که آیا می توان برای ذخیره کردن یا ارسال این رشته ها از فضای هیلبرتی با بعد کمتر استفاده کرد؟ پاسخ این سوال یکی از نتایج مهم نظریه اطلاعات کوانتومی است و جالب است که این پاسخ مشابهت زیادی با قضیه اول شانون دارد. پاسخ این است که می توان رشته های n تایی از حالت ها را در حد n های بسیار بزرگ در فضای هیلبرتی با ابعاد $D = 2^{nS(\rho)}$ گنجاند. یعنی به ازای هر حالت $|\phi\rangle$ بعد فضای هیلبرتی که مورد نیاز است 2 نیست بلکه $2^{S(\rho)}$ است و می دانیم که $0 \leq S(\rho) \leq 1$. این قضیه را نخستین بار بنیامین شوماخر^۱ ثابت کرده است. اگر به جای کیوبیت ها با حالت های d بعدی سروکار داشتیم، آنگاه بجای d^n بعد، می توانستیم رشته های n بعدی را در یک فضای $D = 2^{nS(\rho)}$ فشرده کنیم. دقت کنید که در این حالت $0 \leq S(\rho) \leq \log_2(d)$ و در نتیجه $0 \leq D \leq d^n$. دقت کنید که این نتیجه مختص وقتی است که آنزامل ورودی از حالت های خالص تشکیل شده باشد. در حالت کلی می بایست اعضای آنزامل را حالت های آمیخته در نظر گرفت و این کاری است که در ادامه این درس انجام خواهیم داد. خواننده ممکن است بپرسد که ضرورت این کار چیست؟ مگر نه این است که همواره می توانیم در ورودی یک کانال حالت های خود را به صورت خالص تهیه کنیم. ولی باید توجه کرد که همواره چنین نیست که ما روی حالت های ورودی یک کانال کوانتومی کنترل داشته باشیم. به عنوان مثال اگر یک کانال C_1 بلافاصله به یک کانال C_2 متصل شده باشد، درست است که در ورودی کانال C_1 ما می توانیم حالت ها را به صورت خالص تهیه کنیم ولی در اثر خطا این حالت ها در خروجی کانال C_1 تبدیل به حالت های آمیخته می شوند و این حالت ها سپس وارد کانال C_2 می شوند؟؟ . به عنوان مثال بازهم مشخص تر می توانید فکر کنید که C_1 یک فیبر نوری است و C_2 فضای خالی بین یک آنتن و ماهواره است. ایده ی اصلی فشرده سازی در حالت کوانتومی شباهت زیادی به فشرده سازی کلاسیک دارد. در حالت کلاسیک سعی می کنیم که تنها رشته های نمونه^۲ را کد کنیم، در حالت کوانتومی نیز سعی می کنیم که تنها حالت های رشته

^۱ Benjamin Schumacher

^۲ Typical Strings

حالت های نمونه ^۳ را کد کنیم. قبل از آنکه به بحث کلی پردازیم یک مثال ساده را مطالعه می کنیم.

■ تمرین: فرض کنید که آلیس یکی از دو حالت های $|z\rangle$ یا $|x\rangle$ را در دست دارد و می خواهد آنها را برای باب بفرستد. در این جا منظور از $|z\rangle$ و $|x\rangle$ به ترتیب ویژه حالت های مثبت عملگرهای پاولی در راستای z و x هستند.

الف: اگر آلیس این حالت ها را با احتمال های مساوی برای باب بفرستد و در بین راه این حالت ها گم شوند، بهترین حالت خالصی که باب می تواند به عنوان جایگزین به کاربرد چه حالتی است. فرض کنید که باب قرار بوده که حالت دریافت شده را برای شخص ثالثی بفرستد و می خواهد به جای حالت گم شده حالتی بفرستد که کمترین اختلال را در روند محاسبه یا هر کاربرد دیگری ایجاد کند.

ب: اگر آلیس این حالت ها را با احتمالات زیر بفرستد پاسخ سوال قسمت الف چه خواهد بود؟

$$P(z) = 3/4, \quad P(x) = 1/4$$

■ تمرین: فرض کنید که آلیس یکی از دو حالت های $|z, z\rangle$ یا $|x, x\rangle$ را در دست دارد و هرکدام از آن ها را با احتمال مساوی برای باب می فرستد. اگر در بین راه این حالت ها گم شوند، بهترین حالت خالصی که باب می تواند جایگزین حالت ارسال شده بکند چه حالتی است.

۲ فشرده سازی حالت های کوانتومی: یک مثال

فرض کنید که آلیس آنزاملی از حالت های خالص به شکل زیر دارد

$$\mathcal{E} = \{|x\rangle, |z\rangle\}, \quad (۳)$$

که در آن $|x\rangle$ و $|z\rangle$ ویژه حالت های مثبت اسپین در راستاهای x و z هستند و هرکدام از این حالت ها نیز با احتمال $1/2$ در این آنزامل وارد شده اند. ماتریس چگالی یک کیوبیت برابر است با

$$\rho = \frac{1}{2}(|x\rangle\langle x| + |z\rangle\langle z|) = \frac{1}{4} \begin{pmatrix} 3 & 1 \\ 1 & 1 \end{pmatrix}. \quad (۴)$$

هرگاه از نمایش کره بلوخ استفاده کنیم این ماتریس چگالی به شکل زیر در می آید:

$$\rho = \frac{1}{2}(I + n \cdot \sigma), \quad (۵)$$

که در آن $n = \frac{1}{2}(\hat{x} + \hat{z})$. طیف ρ براحتی بدست می آید:

$$\rho|0\rangle = \lambda_0|0\rangle, \quad \rho|1\rangle = \lambda_1|1\rangle, \quad (۶)$$

که در آن

$$\lambda_0 = \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right) \equiv \cos^2 \frac{\pi}{8}, \quad \lambda_1 = \frac{1}{2}\left(1 - \frac{1}{\sqrt{2}}\right) \equiv \sin^2 \frac{\pi}{8}, \quad (۷)$$

و

$$|0\rangle \equiv |n, +\rangle = \begin{pmatrix} \cos \frac{\pi}{8} \\ \sin \frac{\pi}{8} \end{pmatrix}, \quad |1\rangle \equiv |n, -\rangle = \begin{pmatrix} \cos \frac{\pi}{8} \\ \sin \frac{\pi}{8} \end{pmatrix}. \quad (۸)$$

برای استفاده آینده بهتر است که شباهت حالت های $|x\rangle$ و $|z\rangle$ را با حالت های $|0\rangle$ و $|1\rangle$ نیز محاسبه کنیم: یک محاسبه ساده نتیجه می دهد:

$$|\langle 0|z\rangle|^2 = |\langle 0|x\rangle|^2 = \cos^2 \frac{\pi}{8} = 0.8535,$$

$$|\langle 1|z\rangle|^2 = |\langle 1|x\rangle|^2 = \sin^2 \frac{\pi}{8} = 0.1465. \quad (9)$$

باتوجه به اینکه زاویه کوچکی است، معلوم می شود که شباهت حالت $|0\rangle$ به حالت های ارسالی خیلی بیشتر از شباهت حالت $|1\rangle$ است. در واقع می توان نشان داد که این حالت بیشترین شباهت را بین تمام حالت ها به حالت های $|x\rangle$ و $|z\rangle$ دارد. برای این کار کافی است که قرار دهیم $|0\rangle = \begin{pmatrix} \cos \theta \\ \sin \theta \end{pmatrix}$ و سپس θ را چنان بدست بیاوریم که کمیت $\langle 0|\rho|0\rangle$ بیشترین مقدار خود را اختیار کند. داریم

$$\langle 0|\rho|0\rangle = \frac{1}{4}(3\cos^2\theta + \sin^2\theta + 2\sin\theta\cos\theta) = \frac{1}{4}(2 + \cos 2\theta + \sin 2\theta) = \frac{1}{4}(2 + \sqrt{1 + \sin 4\theta}) \quad (10)$$

عبارت سمت راست وقتی بیشترین مقدار را اختیار می کند که θ برابر با $\frac{\pi}{8}$ باشد و در این نقطه مقدار سمت چپ برابر است با $\frac{1}{2}(1 + \frac{1}{\sqrt{2}}) = \cos^2 \frac{\pi}{8}$. دقت کنید که آلیس در هر بار یکی از حالت های $|x\rangle$ یا $|z\rangle$ را ارسال می کند. از آنجا که حالت های $|x\rangle$ و $|z\rangle$ برهم عمود نیستند، باب هرگز نمی تواند با قطعیت تعیین کند که آلیس کدام یک از حالت ها را برای او فرستاده است. اگر باب نداند که آلیس چه حالتی را برای او فرستاده است بهترین کار ممکن آن است که حالت $|0\rangle$ را به جای کیوبیت دریافت شده اختیار کند. حال فرض کنید که آلیس می خواهد یک رشته ۳ کیوبیتی را برای باب ارسال کند، این رشته ها هرکدام با احتمال $\frac{1}{8}$ ارسال می شوند و برابر اند با

$$\begin{aligned} &|x\rangle|x\rangle|x\rangle \\ &|x\rangle|x\rangle|z\rangle \\ &|x\rangle|z\rangle|x\rangle \\ &|x\rangle|z\rangle|z\rangle \\ &|z\rangle|x\rangle|x\rangle \\ &|z\rangle|x\rangle|z\rangle \\ &|z\rangle|z\rangle|x\rangle \\ &|z\rangle|z\rangle|z\rangle, \end{aligned} \quad (11)$$

و هرنوع اندازه گیری ای که باب روی رشته های سه تایی انجام بدهد، با ماتریس چگالی

$$\rho^{(3)} = \frac{1}{8}(|xxx\rangle\langle xxx| + \dots |zzz\rangle\langle zzz|) = \rho \otimes \rho \otimes \rho, \quad (12)$$

قابل توصیف است. ممکن است که خواننده فکر کند که کافی است که آلیس با ارسال سه بیت کلاسیک به باب بگوید که کدام یک از حالت های فوق را ارسال کرده است تا باب بتواند براحتی حالت مربوطه را در آن طرف خط تهیه کند. ولی باید دقت کرد که آلیس نمی تواند این حالت ها را از هم تشخیص دهد زیرا این حالت ها برهم عمود نیستند و تمام نکته نیز در همین جاست، این خاصیت است که تفاوت اساسی با ارسال بیت ها و اطلاعات کلاسیک دارد. اگر آلیس بتواند هر سه تا کیوبیت را برای باب بفرستد، باب ماتریس چگالی $\rho^{\otimes 3}$ را در اختیار خواهد داشت و حاصل هر نوع اندازه گیری او روی حالت دریافتی با اندازه گیری های آلیس توافق آماری کامل دارد. اما تصور کنید که آلیس امکانات ارسال ۳ تا کیوبیت را ندارد (مثلاً به دلیل گران بودن کانال کوانتومی) و فقط می تواند دو تا کیوبیت به باب بفرستد. در این صورت آلیس چه کیوبیت هایی را باید بفرستد تا حداکثر مشابهت بین ماتریس چگالی $\rho^{\otimes}$ و ماتریس چگالی باب بوجود بیاید. در وهله اول به نظر می رسد که بهترین کار آن است که آلیس تنها دو کیوبیت برای باب بفرستد و به دلیل روابط ۹، باب کیوبیت سوم را خودش $|0\rangle$ اختیار کند، زیرا $|0\rangle$ حالتی است که بیشترین شباهت را به هر کدام از حالت های ارسالی دارد. برای راحتی محاسبه یک تابع مشابهت متوسط را به صورت زیر محاسبه می کنیم:

$$\bar{F} = \frac{1}{8} \sum_i \langle |\phi_{(Alice)}^{(i)}| \phi_{(Bob)}^{(i)} \rangle|^2 \quad (13)$$

که در آن $|\phi_{Alice}^i\rangle$ حالتی است که آلیس فرستاده است و $|\phi_{Bob}^i\rangle$ حالتی است که باب دریافت کرده است. در نتیجه خواهیم داشت:

$$\bar{F} = \frac{1}{8} (|\langle xxx|xx0\rangle|^2 + |\langle xxz|xx0\rangle|^2 + |\langle xzx|xz0\rangle|^2 + \dots |\langle zzz|zz0\rangle|^2) = 0.8535. \quad (14)$$

به این ترتیب آلیس و باب می توانند تنها با مخابره ی دو کیوبیت به شباهت متوسطی برابر با 0.8535 دست پیدا کنند. بهتر است که رابطه ی 13 را به شکل زیر بنویسیم که برای روش جدیدی که در آینده پیشنهاد می کنیم نیز به کار برود، زیرا در روش جدید ممکن است که حالت در دست باب یک حالت مخلوط باشد،

$$\bar{F} = \frac{1}{8} \sum_i \langle \phi_{Alice}^{(i)} | \rho_{Bob}^{(i)} | \phi_{Alice}^{(i)} \rangle. \quad (15)$$

۱.۲ فشرده سازی شوماخر

در مثال بالا آیا راه بهتری هم برای فشرده سازی هست؟ پاسخ این سوال چنانچه خواهیم دید، مثبت است. کاری که می کنیم آن است که فضای هیلبرت یک رشته ی سه تایی را به دو زیرفضای محتمل و نامحتمل تقسیم می کنیم. می دانیم که ویژه حالت های ماتریس ρ مثل هرماتریس هرمیتی دیگری فضای یک کیویت را جاروب می کنند. با توجه به آنچه که در بالا به آن اشاره کردیم، زیرفضاهای محتمل (Λ_0) و نامحتمل (Λ_1) را چنین تعریف می کنیم:

$$\Lambda_0 = \text{Span}\{|000\rangle, |001\rangle, |010\rangle, |100\rangle\}, \quad \Lambda_1 = \Lambda_0^\perp = \text{Span}\{|111\rangle, |110\rangle, |101\rangle, |011\rangle\}. \quad (۱۶)$$

آلیس می بایست هر رشته ورودی را اندازه گیری کند و ببیند که آیا این رشته یک رشته محتمل است یا نا محتمل. به عبارت دیگر آلیس می بایست روی هر رشته ورودی که یکی از هشت حالت ورودی $\{|xxx\rangle, |xxz\rangle, \dots, |zzz\rangle\}$ است یک اندازه گیری تصویری با عملگرهای تصویری

$$\begin{aligned} P_0 &= |000\rangle\langle 000| + |001\rangle\langle 001| + |010\rangle\langle 010| + |100\rangle\langle 100|, \\ P_1 &= |111\rangle\langle 111| + |110\rangle\langle 110| + |101\rangle\langle 101| + |011\rangle\langle 011|, \end{aligned} \quad (۱۷)$$

انجام دهد و سپس با توجه به نتیجه اندازه گیری بجای یک رشته سه کیویتی یک رشته دو کیویتی برای باب بفرستد. در مقصد باب از روی این رشته دو کیویتی یک رشته سه کیویتی را چنان می سازد که بیشترین شباهت را با رشته اولیه داشته باشد. مسلم است که یک اندازه گیری با عملگرهای تصویری بالا یک اندازه گیری با دو خروجی است. یعنی اینکه تنها یک بیت می بایست اندازه گیری شود تا معلوم شود که رشته دریافت شده از کدام نوع است. این کار به این طریق انجام می شود. هر حالت سه تایی $|\phi\rangle$ (مثلاً $|xxx\rangle$) وقتی که در پایه ویژه مقدارهای ρ بسط داده می شود حالتی مثل حالت زیر است:

$$|\phi_A\rangle = x|000\rangle + y|001\rangle + z|010\rangle + w|011\rangle + x'|100\rangle + y'|101\rangle + z'|110\rangle + w'|111\rangle. \quad (۱۸)$$

آلیس نخست عملگر U را مطابق زیر می سازد:

$$U : \left\{ \begin{array}{l} |000\rangle \longrightarrow |\alpha\rangle|+\rangle, \\ |001\rangle \longrightarrow |\beta\rangle|+\rangle, \\ |010\rangle \longrightarrow |\gamma\rangle|+\rangle, \\ |100\rangle \longrightarrow |\delta\rangle|+\rangle, \\ |111\rangle \longrightarrow |\alpha\rangle|-\rangle, \\ |110\rangle \longrightarrow |\beta\rangle|-\rangle, \\ |101\rangle \longrightarrow |\gamma\rangle|-\rangle, \\ |011\rangle \longrightarrow |\delta\rangle|-\rangle, \end{array} \right. \quad (۱۹)$$

دراین رابطه $|\alpha\rangle, |\beta\rangle, |\gamma\rangle, |\delta\rangle$ چهار حالت متعامد برای دو کیوبیت اول و $|+\rangle$ و $|-\rangle$ دو حالت متعامد برای کیوبیت سوم است. بعد از اعمال عملگر U حالتی که در دست آلیس است به صورت زیر در می آید:

$$U|\phi_A\rangle = (x|\alpha\rangle + y|\beta\rangle + z|\gamma\rangle + w|\delta\rangle) \otimes |+\rangle + (x'|\alpha\rangle + y'|\beta\rangle + z'|\gamma\rangle + w'|\delta\rangle) \otimes |-\rangle. \quad (۲۰)$$

بعد از اعمال این عملگریکانی آلیس تنها کیوبیت سوم را اندازه می گیرد. نتیجه ی $+$ و $-$ به این معنا هستند که حالت $|\phi_A\rangle$ به زیر فضای Λ_0 و Λ_1 تصویر شده اند.

بنابراین حالت دو کیوبیت اول عبارت خواهند بود از:

$$\left\{ \begin{array}{ll} |\phi_A^+\rangle = \frac{1}{\sqrt{x^2+y^2+z^2+w^2}}(x|\alpha\rangle + y|\beta\rangle + z|\gamma\rangle + w|\delta\rangle) & if \quad + \\ |\phi_A^-\rangle = \frac{1}{\sqrt{x'^2+y'^2+z'^2+w'^2}}(x'|\alpha\rangle + y'|\beta\rangle + z'|\gamma\rangle + w'|\delta\rangle) & if \quad - \end{array} \right. \quad (۲۱)$$

دقت کنید که آلیس حالت های بالا را با احتمالات زیر بدست می آورد:

$$\begin{cases} P(+) = x^2 + y^2 + z^2 + w^2 \\ P(-) = x'^2 + y'^2 + z'^2 + w'^2 \end{cases} \quad (22)$$

حال اگر آلیس نتیجه + را بدست آورد حالت $|\phi_A^+\rangle$ را برای باب ارسال می کند. با توجه به شکل Λ_0 این حالت شباهت خیلی زیادی با رشته حالت اولیه ای دارد که آلیس دریافت کرده است. در مقصد پس از دریافت این حالت باب یک کیویت $|+\rangle$ را به این حالت اضافه کرده و سپس عملگر U^{-1} را به آن اعمال می کند. بنابراین در این صورت باب حالت زیر را خواهد ساخت:

$$|\phi^+\rangle_{Bob} \equiv U^{-1}|\phi_A^+\rangle|+\rangle = \frac{1}{\sqrt{x^2 + y^2 + z^2 + w^2}}(x|000\rangle + y|001\rangle + z|010\rangle + w|100\rangle) \quad (23)$$

که می توان آن را به صورت زیر نیز نوشت:

$$|\phi^+\rangle_{Bob} = \frac{1}{\sqrt{\langle\phi_A|P_0|\phi_A\rangle}}P_0|\phi_A\rangle. \quad (24)$$

وقتی که آلیس نتیجه - بدست می آورد چه باید بکند؟ چه حالتی را می بایست به باب بفرستد؟ در مثال حاضر منطقی ترین پاسخ این است که حالتی را بفرستد که بعد از عمل باب (یعنی اتصال یک حالت $|+\rangle$ و اعمال عملگر U^{-1} حالتی حاصل شود که بیشترین شباهت را با حالت اولیه داشته باشد. این حالت می بایست رشته $|000\rangle$ باشد. پس در این صورت آلیس حالت $|\alpha\rangle$ را به باب می فرستد. این حالت با احتمال $1 - \langle\phi_A|P_0|\phi_A\rangle$ ارسال می شود. بنابراین حالت نهایی در دست باب حالت زیر است:

$$\rho_{Bob} = \langle\phi_A|P_0|\phi_A\rangle|\phi_A^+\rangle\langle\phi_A^+| + (1 - \langle\phi_A|P_0|\phi_A\rangle)|000\rangle\langle 000|. \quad (25)$$

و در نتیجه مشابهت متوسط برابر خواهد بود با

$$\bar{F} = \frac{1}{8} \sum_{\phi} \langle\phi_{Alice}|\rho_{Bob}|\phi_A\rangle = \frac{1}{8} \sum_{|\phi\rangle} [\langle\phi_A|P_0|\phi_A\rangle\langle\phi_A|P_0|\phi_A\rangle + \langle\phi_A|1 - P_0|\phi_A\rangle\langle\phi|000\rangle\langle 000|\phi\rangle]. \quad (26)$$

در عبارت بالا روی همه حالت های $|\phi\rangle \in \{|xxx\rangle, |xxz\rangle, \dots |zzz\rangle\}$ جمع زده می شود. می دانیم که

$$\begin{aligned}\langle\phi_A|P_0|\phi_A\rangle &= \cos^6\frac{\pi}{8} + 3\cos^4\frac{\pi}{8}\sin^2\frac{\pi}{8} = 0.8535^3 + 3 \times 0.8535^2 \times 0.1465 = 0.9419, \\ \langle\phi_A|1 - P_0|\phi_A\rangle &= 0.0581, \\ \langle\phi_A|000\rangle\langle 000|\phi_A\rangle &= 0.8535^3 = 0.6274.\end{aligned}\tag{۲۷}$$

بنابراین بدست می آوریم

$$\overline{F} = 0.9236.\tag{۲۸}$$

بدین ترتیب آلیس توانسته است تنها با ارسال ۲ کیوبیت به مشابهتی به اندازه 0.9236 دست پیدا کند. در قسمت بعد نشان خواهیم داد که آلیس واقعاً می تواند با ارسال رشته کیوبیت های طولانی به مشابهت های به اندازه کافی نزدیک به یک دست پیدا کند. البته بحث خود را به صورت کلی و نه در قالب این مثال خاص دنبال خواهیم کرد.

■ تمرین: فرض کنید که آلیس از همین آزمایلی که تا کنون مطالعه کرده ایم کیوبیت های 5 تایی دریافت کند ولی تنها بتواند رشته های 3 کیوبیتی برای باب بفرستد.

الف: بهترین استراتژی آلیس و باب در این صورت چه خواهد بود. فیدلیته متوسط حالت هایی که به دست باب می رسد با حالت های اولیه ای که آلیس دریافت کرده است چقدر است؟

ب: اگر طول رشته های دریافتی 7 باشد و آلیس تنها بتواند 5 کیوبیت برای باب بفرستد پاسخ سوال الف چه خواهد بود.

۳ فشرده سازی برای حالت های خالص

فرض می کنیم که آلیس یک آنزامل از حالت های خالص از کیویت ها به صورت $\{|\phi_i\rangle, p_i, i = 1, 2, \dots, k\}$ در اختیار دارد. این آنزامل در واقع حکم یک الفبا را برای وی دارد با این تفاوت که حروف الفبا الزاماً از هم تمیز پذیر نیستند. ماتریس چگالی یک حرف عبارت است از:

$$\rho = \sum_i p_i |\phi_i\rangle \langle \phi_i|. \quad (29)$$

بعد ماتریس ρ برابر است با 2. رشته های n حرفی، حالت هایی هستند به صورت زیر:

$$|\Phi_x\rangle := |\phi_{x_1}\rangle |\phi_{x_2}\rangle |\phi_{x_3}\rangle \cdots |\phi_{x_n}\rangle, \quad x_i \in \{1, 2, \dots, k\}. \quad (30)$$

این رشته ها نیز از هم تمیز ناپذیرند. چنین رشته ای با احتمال $P_x := p_{x_1} p_{x_2} \cdots p_{x_n}$ ارسال می شود و ماتریس چگالی این رشته ها برابر است با

$$\rho^{(n)} = \sum_x P_x |\Phi_x\rangle \langle \Phi_x| = \rho^{\otimes n}. \quad (31)$$

بعد این ماتریس برابر است با 2^n . (یک بار که مسئله را برای کیویت ها بفهمیم فهم حالت کلی آسان خواهد بود.) حال نشان می دهیم که آلیس می تواند بجای این رشته های بلند، رشته هایی از $nS(\rho)$ کیویت برای باب ارسال کند و در حد مجانبی (n های خیلی بزرگ) به مشابهتی هرچقدر نزدیک به 1 دست پیدا کند. برای این کار آلیس به ترتیب زیر عمل می کند و تمام این اعمال چیزی نیستند جز تعمیم سراسر است آنچه که در مثال بخش قبلی دیدیم. ماتریس چگالی ρ دارای دو ویژه مقدار $|0\rangle$ و $|1\rangle$ است.

$$\rho|0\rangle = \lambda_0|0\rangle, \quad \rho|1\rangle = \lambda_1|1\rangle. \quad (32)$$

اگر ماتریس چگالی ρ را در پایه های خودش اندازه گیری کنیم با احتمال $\lambda_0 = \langle 0|\rho|0\rangle$ مقدار 0 و با احتمال $\lambda_1 = \langle 1|\rho|1\rangle$ مقدار 1 بدست خواهد آمد. هم چنین ویژه مقدارها و ویژه بردارهای $\rho^{(n)}$ عبارتند از:

$$\rho^{(n)}|s_1 s_2 \cdots s_n\rangle = \lambda_{s_1} \lambda_{s_2} \cdots \lambda_{s_n} |s_1 s_2 \cdots s_n\rangle, \quad s_i \in \{0, 1\}. \quad (33)$$

اگر $\rho^{(n)}$ را در پایه های خودش اندازه گیری کنیم احتمال بدست آوردن رشته ی $|s_1 s_2 \cdots s_n\rangle$ برابر است با $\lambda_{s_1} \lambda_{s_2} \cdots \lambda_{s_n}$. در چنین رشته ای متوسط تعداد 0 ها را با n_0 و تعداد 1 ها را با n_1 نشان می دهیم. واضح است که متوسط این مقادیر برابر است

با $\overline{n_0} = n\lambda_0$ و $\overline{n_1} = n\lambda_1$. بنابراین در تقریب صفر می توانیم بگوییم که زیرفضای محتمل آن زیرفضایی است که توسط آن دسته از ویژه بردارهای $|s_1 s_2 \cdots s_n\rangle$ جاروب می شود که تعداد 0 ها و 1 هایشان به ترتیب برابرند با $n\lambda_0$ و $n\lambda_1$. یعنی قرار دهیم

$$\Lambda_{typical} := Span\{|s_1 s_2 \cdots s_n\rangle, \quad n_0 = n\lambda_0, \quad n_1 = n\lambda_1\}. \quad (34)$$

تعداد چنین بردارهایی یعنی بعد این زیرفضای محتمل چقدر است؟ پاسخ آن برابر است با

$$Dim(\Lambda_{typical}) = \binom{n}{n\lambda_0} = 2^{nS(\rho)}, \quad (35)$$

که در آن از تقریب استرلینگ و رابطه‌ی

$$S(\rho) = -\lambda_0 \log_2 \lambda_0 - \lambda_1 \log_2 \lambda_1, \quad (36)$$

استفاده کرده‌ایم. اگر یک بردار متعلق به زیرفضای نمونه یعنی $\Lambda_{typical}$ را در نظر بگیریم، ویژه مقدار آن برای عملگر چگالی چقدر است؟ پاسخ برابر است با

$$\rho|v\rangle = \lambda_0^{n\lambda_0} \lambda_1^{n\lambda_1} |v\rangle = 2^{n\lambda_0 \log \lambda_0 + n\lambda_1 \log \lambda_1} |v\rangle = 2^{-nS(\rho)} |v\rangle. \quad (37)$$

بنابراین می توانیم زیر فضای نمونه را به این صورت تعریف کنیم که زیرفضایی است که توسط تمام بردارهای با ویژه مقدار $2^{-nS(\rho)}$ جاروب می شود. عملگر تصویر روی فضای $\Lambda_{typical}$ را با E نشان می دهیم ، یعنی

$$E := \sum_{v \in \Lambda_{typical}} |v\rangle\langle v|. \quad (38)$$

با چنین تعریفی احتمال این که اندازه گیری یک حالت آن را به زیر فضای نمونه یعنی $\Lambda_{typical}$ تصویر کند برابر خواهد بود با

$$P_{typical} = tr(\rho E) = \sum_{i \in typical} \lambda_i = 2^{nS(\rho)} \times 2^{-nS(\rho)} = 1, \quad (39)$$

که به این معناست که هر نوع اندازه گیری با احتمال یک حتماً حالت یک رشته را به زیر فضای نمونه تصویر خواهد کرد. البته این نتیجه در حد n های بسیار بزرگ درست است و هم چندی ناشی از تعریف خیلی محدود ما از زیر فضای نمونه است.

ولی به همان دلیل و ترتیبی که در حالت کلاسیک رشته‌های نمونه را با کمی تحمل تعریف کردیم، در این جا هم می توانیم تعریف زیر فضای نمونه را با کمی تحمل تعریف کنیم به این ترتیب که:

$$\Lambda_{typical} := Span\{|v\rangle \mid 2^{-n(S(\rho)+\delta)} < \lambda(v) < 2^{-n(S(\rho)-\delta)}\} \quad (40)$$

با این تعریف رابطه‌ی ^۴ به صورت زیر تعدیل می شود

$$1 - \epsilon \leq tr(\rho E) \leq 1. \quad (41)$$

با بزرگ تر گرفتن n می توانیم مقدار ϵ را هرچقدر که می خواهیم کوچک اختیار کنیم . (در این قسمت از درس ما از جاده استدلال خیلی دقیق کمی دور افتاده‌ایم ولی مطالبی را که می گوئیم، خواننده‌ی علاقمند می تواند به طور دقیق اثبات کند. برای این کار کافی است که به اثبات نامساوی هایی که در درس نظریه اطلاعات کلاسیک بدست آوردیم رجوع کند.)

حال مطابق با مثالی که در قسمت قبلی دیدیم آلیس برای کد کردن یک رشته دلخواه مثل $|\Phi_x\rangle$ به ترتیب زیر عمل می کند. نخست وی یک اندازه گیری با تصویرگرهای $\{E, 1-E\}$ انجام می دهد. وقتی که وی نتیجه E را بدست می آورد، حالت وی با احتمال $\langle \Phi_x | E | \Phi_x \rangle$ روی زیر فضای نمونه تصویر می شود. بعد این زیر فضا برابر است با $2^{NS(\rho)}$. سپس وی می تواند از یک عملگریکانی مثل U استفاده کند که حالت های این فضا را به طرز مناسبی بچرخاند به نحوی که :

$$U : |\Phi_x\rangle \longrightarrow |\phi_x\rangle \otimes |0\rangle^{\otimes n(1-S(\rho))}, \quad \text{if } |\psi\rangle \in \Lambda_{typical}. \quad (42)$$

دقت کنید که $|\phi_x\rangle$ یک حالت در فضای $nS(\rho)$ کیوبیتی است. پس از این کار آلیس تنها حالت $|\phi_x\rangle$ را به باب می فرستد. سپس باب حالت $|0\rangle^{\otimes N(1-S(\rho))}$ را به حالت دریافت شده اضافه کرده و عملگر U^{-1} را به حالت ایجاد شده اعمال می کند تا حالت $|\Phi_x\rangle$ را بدست بیاورد. اما وقتی که آلیس نتیجه $1-E$ بدست می آورد، آلیس و باب می توانند هر کار دیگری انجام دهند. در این مورد که با احتمال خیلی کم $tr(\rho^{\otimes N}(1-E))$ رخ می دهد، فرض کنید که نتیجه روش آلیس و باب این است که یک حالت دلخواه مثل $|\chi_x\rangle$ به دست باب می رسد. بنابراین نتیجه کلی این است که

$$\rho_x^{Bob} = E|\Phi_x\rangle\langle\Phi_x|E + \langle\Phi_x|I-E|\Phi_x\rangle|\chi_x\rangle\langle\chi_x|. \quad (43)$$

ptyp^۴

■ تمرین: درستی رابطه بالا را ثابت کنید.

حال مشابهت متوسط را محاسبه می کنیم:

$$\begin{aligned}\bar{F} &= \sum_x P_x \langle \Phi_x | \rho_x^{Bob} | \Phi_x \rangle \\ &= \sum_x P_x \langle \Phi_x | E | \Phi_x \rangle \langle \Phi_x | E | \Phi_x \rangle + \sum_x P_x \langle \Phi_x | 1 - E | \Phi_x \rangle |\chi_x\rangle \langle \chi_x| \\ &\geq \sum_x P_x ||E|\Phi_x\rangle||^4.\end{aligned}\quad (44)$$

اما با استفاده از نامساوی $(x-1)^2 \geq 0$ یا $x^2 \geq 2x-1$ نتیجه می گیریم که

$$\bar{F} \geq \sum_x P_x (2||E|\Phi_x\rangle||^2 - 1) = \sum_x 2P_x \langle \Phi_x | E | \Phi_x \rangle - 1 = 2tr(E\rho) - 1 \geq 2(1-\epsilon) - 1 = 1 - 2\epsilon. \quad (45)$$

به این ترتیب نشان داده ایم که با ارسال تنها $nS(\rho)$ کیبیت می توان اطلاعات موجود در رشته های n کیبیتی از آزمابل $\rho^{\otimes n}$ را با مشابهت هرچقدر نزدیک به 1 ارسال کرد. این نتیجه تعمیم قضیه اول شانون به حالت کوانتومی است. به عبارت بهتر این قضیه می گوید که اطلاعات موجود در رشته های n کیبیتی که از این آزمابل یا الفبای کوانتومی ساخته می شوند، به اندازه $nS(\rho)$ کیبیت است. باید تاکید کنیم که این نتیجه تنها برای آزمابلی از حالت های خالص صحیح است. در بخش بعدی به بحث در باره آزمابل حالت های ناخالص می پردازیم.

۴ فشرده سازی برای حالت های آمیخته

فرض کنید که آلیس آزمابلی از حالت های آمیخته دارد که می خواهد آن را برای باب ارسال کند. آزمابل را با $\mathcal{E} = \{\sigma_x, p_x\}$ نشان می دهیم. ماتریس چگالی این آزمابل یعنی ماتریس چگالی ای که نتایج تمام اندازه گیری ها روی این آزمابل را نشان می دهد برابر است با

$$\rho = \sum_x p_x \sigma_x. \quad (46)$$

یک رشته حالت به طول n عبارت است از:

$$\sigma_{x_1} \otimes \sigma_{x_2} \otimes \cdots \sigma_{x_n}, \quad (47)$$

که با احتمال $p_{x_1} p_{x_2} \cdots p_{x_n}$ ارسال می شود. آیا بازهم پاسخ مسئله فشرده سازی این است که آلیس می تواند با مشابهت نزدیک به ۱، و تنها با مصرف $nS(\rho)$ کیبیت رشته حالت های n تایی از حالت ها را ارسال کند؟ آیا آن کمیتی که حد فشرده سازی را تعیین می کند بازهم $S(\rho)$ است؟ مسلم است که پاسخ این سوال منفی است. برای فهم این موضوع فرض کنید که آزمایلی که در دست آلیس است تماماً از یک حالت مشخص مثل σ درست شده باشد، یعنی $\mathcal{E} = \{\sigma, p(\sigma) = 1\}$. در این صورت همه رشته های n کیبیتی عین هم هستند و آلیس برای آنکه بگوید که کدام رشته ای n کیبیتی مخابره شده است احتیاج به ارسال هیچ کیبیتی ندارد. به عبارت دیگر اطلاعات موجود در این رشته ها صفر است. اما می دانیم که $S(\rho) = S(\sigma)$ و بسته به نوع حالت σ ، $S(\rho)$ می تواند هر مقداری بین صفر و یک را اختیار کند. پس در مورد حالت های آمیخته پاسخ سوال فوق $S(\rho)$ نیست. از طرف دیگر ما می توانیم به دو حالت حدی نگاه کنیم و بفهمیم که کمیت مورد نظر چه رفتار حدی ای می بایست داشته باشد. این کمیت را با $\chi(\mathcal{E})$ نشان می دهیم. به عنوان دو حالت حدی موارد زیر را نگاه می کنیم:

الف: آزمایلی $\mathcal{E} = \{|\phi_x\rangle, p_x\}$ از حالت های خالص ولی نامتعامل تشکیل شده است. این مورد را در بخش قبلی مطالعه کرده ایم و می دانیم که میزان اطلاعات موجود در آن $S(\rho)$ بر حالت است که در آن $\rho = \sum_x |\phi_x\rangle\langle\phi_x|$. بنابراین می بایست کمیت $\chi(\mathcal{E})$ در این حد تبدیل شود به $S(\rho)$.

ب: آزمایلی $\mathcal{E} = \{\sigma_x, p_x\}$ از حالت های ناخالص ولی متعامل تشکیل شده است. در این صورت چون همه ی حالت های σ_x تمیز پذیرند، کوانتومی بودن حالت ها اهمیت ندارد و آلیس می تواند بجای هر حالت σ_x خود رشته ی کلاسیک x را مخابره کند و ما از درس قبل می دانیم که اطلاعات موجود در این آزمایلی برابر است با $H(X)$ بیت بر حرف یا حالت که در آن $H(X) = -\sum_i p_i \log p_i$. پس کمیت $\chi(\mathcal{E})$ می بایست در این حد میل کند به $H(X)$.

حال سوال این است که آیا چنین کمیتی وجود دارد؟ و آیا به فرض وجود دارای خاصیت های مورد انتظار هست یا نه؟ این

کمیت به کمیت هولو *Holevo* موسوم است ^۵ و به شکل زیر تعریف می شود:

$$\chi(\mathcal{E}) = S\left(\sum_i p_i \sigma_i\right) - \sum_i p_i S(\sigma_i). \quad (48)$$

■ تمرین: یک آنزامل از حالت ها به صورت زیر است:

$$\mathcal{E} = \left\{ \frac{1}{2}(I + \mathbf{r} \cdot \boldsymbol{\sigma})(p_1), \quad \frac{1}{2}(I + \mathbf{s} \cdot \boldsymbol{\sigma})(p_2) \right\} \quad (49)$$

که در آن $\mathbf{r}$ و $\mathbf{s}$ دو بردار دلخواه در کره بلوخ هستند و اعداد داخل پرانتز نیز احتمالات مربوط به هر حالت را نشان می دهند. کمیت *Holevo* را برای این آنزامل حساب کنید. الف: هرگاه این بردارها ثابت باشند به ازای کدام احتمالات کمیت هولو و مقدار بیشینه را اختیار می کند.

ب: هرگاه احتمالات ثابت باشند، به ازای کدام بردارها کمیت هولو و بیشترین مقدار را پیدا می کند؟

واضح است که برای آنزاملی از حالت های خالص (یعنی برای $\sigma_i = |\phi_i\rangle\langle\phi_i|$) این کمیت تبدیل می شود به $S(\rho)$. برای آنکه نشان دهیم که در حد دیگر نیز این کمیت رفتار مورد انتظار ما را دارد به ترتیب زیر عمل می کنیم: از آنجا که σ_i ها برهم عمودند، پس پایه ^۶ آنها در فضاهای عمود برهم قرار گرفته است و بنابراین ماتریس چگالی $\rho = \sum_i p_i \sigma_i$ چنین قیافه ای دارد:

$$\rho = \begin{pmatrix} p_1 \tilde{\sigma}_1 & & & \\ & p_2 \tilde{\sigma}_2 & & \\ & & \dots & \\ & & & p_n \tilde{\sigma}_n \end{pmatrix}, \quad (50)$$

که در آن منظور از $\tilde{\sigma}$ تحدید σ به زیر فضای پایه خودش است یعنی به زیر فضای ویژه مقدارهای غیرصفرخودش. بنابراین با قطری کردن ماتریس فوق خواهیم داشت

$$S(\rho) \equiv S\left(\sum_i p_i \sigma_i\right) = - \sum_i \text{tr}(p_i \sigma_i \log(p_i \sigma_i))$$

^۵ به خاطر *Alexander Holevo* که نخستین بار آن را مطرح کرده است.

^۶ Support

$$\begin{aligned}
&= - \sum_i \text{tr}(p_i \sigma_i \log p_i) - \sum_i \text{tr}(p_i \sigma_i \log \sigma_i) \\
&= - \sum_i p_i \log p_i - \sum_i p_i \text{tr}(\sigma_i \log \sigma_i) = H(X) + \sum_i p_i S(\sigma_i).
\end{aligned} \tag{51}$$

بنابراین بدست می آوریم که برای یک آنزامل از حالت های آمیخته‌ی متعامد،

$$\chi(\mathcal{E}) \equiv S(\sum_i p_i \sigma_i) - \sum_i p_i S(\sigma_i) = H(X) \equiv - \sum_i p_i \log p_i. \tag{52}$$

حال که دیدیم کمیت هولو رفتار حدّی درستی دارد، سوال این است که آیا واقعاً می توان اطلاعات یک آنزامل از حالت های آمیخته‌ی دلخواه را تا حدّ $\chi(\mathcal{E})$ کیویت بر حالت فشرده کرد؟ پاسخ این سوال منفی است. خواننده برای اثبات این قضیه می بایست به نوشتارهای تخصصی در این مورد مراجعه کند. هم چنین برای یافتن پاسخ به این سوال که آیا واقعا مثل حالت کلاسیک یک روش کدگذاری مشخص مثلاً کد گذاری تصادفی وجود دارد که حد هولو وو را اشباع کند یا خیر، خواننده می تواند به نوشتارهای تخصصی مراجعه کند.

۵ میزان اطلاعات قابل حصول

کمیت هولو برای یک آنزامل یک خصلت مهم و بنیادین دیگر نیز دارد و دراین بخش می خواهیم این خصلت بنیادین را معرفی کنیم. فرض کنید که آلیس یک آنزامل از حالت ها مثل $\mathcal{E} = \{\sigma_x, p_x\}$ در اختیار دارد. وی حالت های σ_x را با احتمالات p_x برای باب می فرستد. باب با یک $POVM$ مثل مجموعه $\{E_y\}$ اندازه گیری انجام می دهد. هدف باب این است که تشخیص دهد آلیس کدام حالت را برای او فرستاده است. اگر حالت هایی که آلیس می فرستد متعامد باشند، باب می تواند با یک $POVM = \{|\phi_y\rangle\langle\phi_y|\}$ حالت ها را با اطمینان تشخیص دهد. ولی اگر حالت ها متعامد نباشند هیچگاه اطمینان و قطعیت برای باب حاصل نمی شود و وی تنها می تواند با اندازه گیری هوشمندانه میزان اطلاعات خود را افزایش دهد. احتمال اینکه باب نتیجه‌ی y را بدست بیاورد مشروط بر اینکه آلیس حالت σ_x را ارسال کرده باشد برابر است با:

$$P(y|x) = \text{tr}(\sigma_x F_y). \tag{53}$$

بنابراین احتمال اینکه آلیس حالت σ_x را ارسال کند و باب نتیجه‌ی y را بدست بیاورد، برابر است با

$$p(y, x) = p(y|x)p_x = \text{tr}(\sigma_x F_y)p_x$$

. هم چنین خواهیم داشت

$$p_y = \sum_x p(y, x) = \sum_x p(y|x)p_x = \sum_x \text{tr}(\sigma_x F_y)p_x. \quad (54)$$

هدف باب آن است که با اندازه‌گیری مناسب میزان اطلاعات متقابل بین متغیرتصادفی X و Y را بیشینه کند. این مقدار را اطلاعات قابل حصول از آنزامل $\mathcal{E}$ می‌نامیم، و آن را با $Acc(\mathcal{E})$ نشان می‌دهیم، یعنی

$$Acc(\mathcal{E}) := \max_{F_y} I(Y : X) = \max_{F_y} (H(X) + H(Y) - H(X, Y)). \quad (55)$$

در ادامه به چند خاصیت مهم کمیت هوله و اشاره می‌کنیم. از این خواص تنها یکی از آنها را اثبات می‌کنیم ولی باید توجه کنیم که بیش از اثبات این روابط آنچه که مهم است فهم دقیق صورت این خواص است. این خواص به صورت زیر هستند:

■ خاصیت اول: هیچ رابطه فشرده و کلی‌ای برای $Acc(\mathcal{E})$ وجود ندارد یا لااقل تا کنون بدست نیامده است.

■ خاصیت دوم: علیرغم خاصیت اول برای اطلاعات قابل حصول حد بالا بدست آمده است. به این معنا که

$$\begin{aligned} Acc(\mathcal{E}) &\leq S(\rho), & \text{for an ensemble of pure states,} \\ Acc(\mathcal{E}) &\leq \chi(\mathcal{E}), & \text{for an ensemble of mixed states.} \end{aligned} \quad (56)$$

■ خاصیت سوم: اگر آلیس حالت‌ها را به صورت بسته‌های n تایی بفرستد و باب نیز روی بسته‌های n تایی اندازه‌گیری

های جمعی انجام دهد آنگاه در حد $n \rightarrow \infty$ حدهای بالا اشباع خواهند شد، یعنی این که :

$$\lim_{n \rightarrow \infty} \frac{Acc(\mathcal{E}^{(n)})}{n} = S(\rho), \quad \text{for an ensemble of pure states,}$$

Accessible Information^Y

$$\lim_{n \rightarrow \infty} \frac{Acc(\mathcal{E}^{(n)})}{n} = \chi(\mathcal{E}), \quad \text{for an ensemble of mixed states.} \quad (57)$$

پس از این نتایج که خواننده را دعوت می کنیم معنای آنها را به روشنی به خاطر بسپارد، می توانیم به اثبات خاصیت اول می پردازیم. به عبارت دیگر نشان می دهیم که میزان اطلاعات قابل حصول هرگز نمی تواند از $\chi(\mathcal{E})$ بیشتر باشد، یعنی اینکه نشان می دهیم

$$Acc(\mathcal{E}) \leq \chi(\mathcal{E}).$$

■ تمرین: آلیس آزمایلی از حالت ها را با احتمالات داده شده در زیر برای باب می فرستد:

$$\mathcal{E} = \{|0\rangle\langle 0|(\frac{1}{2}), \quad |+\rangle\langle +|(\frac{1}{2})\}. \quad (58)$$

باب یک اندازه گیری متعامد و دو حالت با تصویرگرهای $P_+ = |n, +\rangle\langle n, +|$ و $P_- = |n, -\rangle\langle n, -|$ روی حالت های دریافتی انجام می دهد. میزان اطلاعات قابل حصول برای باب را به عنوان تابعی از جهت n بدست آورید. به ازای کدام جهت این اطلاعات بیشینه می شود. تحقیق کنید که آیا این اطلاعات از کمیت هولده و کمتر است؟

برای اثبات این نامساوی ناچاریم از قضیه زیر جمع پذیری قوی ^۸ استفاده کنیم. ضمناً فعلاً برای سادگی فرض می کنیم که اندازه گیری ما یک اندازه گیری تصویری است یعنی اینکه $F_y F'_y = \delta_{y,y'} F_y$. برای این منظور ماتریس چگالی زیر را برای سه سیستم X, Y و Q تشکیل می دهیم:

$$\rho_{XQY} = \sum_x p_x |x\rangle\langle x| \otimes \sigma_x \otimes |0\rangle\langle 0|. \quad (59)$$

وقتی که باب روی حالت هایی که دریافت می کند اندازه گیری می کند، می توان گفت که عملگریکانی زیر را روی فضای $Q \otimes Y$ انجام می دهد:

$$U_{QY} : |\phi\rangle \otimes |0\rangle \longrightarrow \sum_y F_y |\phi\rangle \otimes |y\rangle. \quad (60)$$

تحت چنین عملگریکانی ای حالت ρ_{XQY} تبدیل می شود به

$$\rho'_{XQY} = \sum_{x,y,y'} p_x |x\rangle\langle x| \otimes F_y \sigma_x F_{y'} \otimes |y\rangle\langle y'|. \quad (61)$$

^۸ Strong Subadditivity Theorem

حال از قضیه زیرجمع پذیری قوی استفاده می کنیم که به موجب آن

$$S(\rho'_{XQY}) + S(\rho'_Y) \leq S(\rho'_{XY}) + S(\rho'_{QY}). \quad (62)$$

آنچه که باقی مانده است این است که هرکدام از ماتریس های چگالی فوق را تعیین کرده و آنتروپی فون نویمان را برای آنها حساب کنیم. داریم

$$\begin{aligned} \rho'_Y &= \text{tr}_{XQ}(S(\rho'_{XQY})) = \sum_{x,y} p_x \text{tr}(F_y \sigma_x) \otimes |y\rangle\langle y| = \sum_y p_y |y\rangle\langle y| \\ \rho'_{XY} &= \text{tr}_Q(S(\rho'_{XQY})) = \sum_{x,y} p_x |x\rangle\langle x| \otimes |y\rangle\langle y| \text{tr}(F_y \sigma_x) = \sum_{x,y} p(x,y) |x,y\rangle\langle x,y|. \end{aligned} \quad (63)$$

با توجه به این روابط بدست می آوریم

$$\begin{aligned} S(\rho'_Y) &= H(Y), \\ S(\rho'_{XY}) &= H(X, Y). \end{aligned} \quad (64)$$

حال دقت می کنیم که با توجه به این که ρ_{XQY} از اثر عملگر یکانی U_{QY} روی حالت ρ_{XQY} بدست آمده، مطمئن هستیم که

$$\begin{aligned} S(\rho'_{XQY}) &= S(\rho_{XQY}) = H(X) + \sum_x p_x S(\sigma_x), \\ S(\rho'_{QY}) &= S(\rho_{QY}) = S(\sum_x p_x \sigma_x \otimes |0\rangle\langle 0|) = S(\sum_x p_x \sigma_x). \end{aligned} \quad (65)$$

با جایگذاری این نتایج در رابطه ی ۶۲ بدست می آوریم:

$$H(X) + \sum_x p_x S(\sigma_x) + H(Y) \leq H(X, Y) + S(\sum_x p_x \sigma_x) \quad (66)$$

و یا

$$I(X : Y) \leq \chi(\mathcal{E}). \quad (67)$$

این نامساوی به حد هولو^۹ مشهور است. می توان نشان داد^{۱۰} که میزان اطلاعات قابل حصول برای آزمابلی از حالت های خالص و آمیخته در حد مجانبی به شرح زیر است:

^۹ Holevo Bound

^{۱۰} خواننده ی علاقمند می تواند به کتاب پرسکیل، فصل پنجم مراجعه کند

الف: برای آزمابلی از حالت های خالص: میزان اطلاعات قابل حصول در حد مجانبی برابر است با $S(\rho)$ بریت که در آن $\rho = \sum_x p_x |\phi_x\rangle\langle\phi_x|$. منظور دقیقی این قضیه این است که اگر آلیس رشته های n تایی از حالت هایی را به باب ارسال کند که هر حالت آن از آزمابل $\{|\phi_x\rangle, p_x\}$ انتخاب شده اند، و باب بهترین اندازه گیری ها را انجام دهد، آنگاه میزان اطلاعات متقابل بین آلیس و باب را می توان با مصرف $nS(\rho)$ بیت کلاسیک در جایی ذخیره کرد یا به جایی ارسال کرد.

ب: برای آزمابلی از حالت های آمیخته: میزان اطلاعات قابل حصول در حد مجانبی برابر است با $\chi(\mathcal{E})$ بریت که در آن $\chi(\mathcal{E}) = S(\sum p_x \sigma_x - \sum p_x S(\sigma_x))$. منظور دقیقی این قضیه این است که اگر آلیس رشته های n تایی از حالت هایی را به باب ارسال کند که هر حالت آن از آزمابل $\{\sigma_x, p_x\}$ انتخاب شده اند، و باب بهترین اندازه گیری ها را انجام دهد، آنگاه میزان اطلاعات متقابل بین آلیس و باب را می توان با مصرف $n\chi(\mathcal{E})$ بیت کلاسیک در جایی ذخیره کرد یا به جایی ارسال کرد.

۶ آتروپی فون نویمان به عنوان اندازه درهم تنیدگی

کدام یک از حالت های زیر درهم تنیدگی بیشتری دارند؟

$$|\phi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\psi\rangle = \sqrt{0.85}|00\rangle + \sqrt{0.15}|11\rangle. \quad (68)$$

به صورت کیفی می توانیم بگوییم درهم تنیدگی حالت $|\phi_+\rangle$ بیشتر است زیرا بیشترین فاصله کیفی را از یک حالت ضربی دارد. این پاسخ می تواند قانع کننده باشد ولی نمی گوید که درهم تنیدگی این حالت چقدر از درهم تنیدگی حالت دیگر بیشتر است؟ اصلا معلوم نیست که آیا سوال «چقدر؟» می تواند برای درهم تنیدگی با معنا باشد. ما می توانیم طول دو خط کش یا وزن دو قطعه فلز را با هم مقایسه کنیم ولی معلوم نیست بتوانیم مقدار درهم تنیدگی را اصلا معنا کنیم. برای آنکه شک و تردید خود را درباره معنا دار بودن این سوال زیاد تر کنیم می توانیم از خود بپرسیم که درهم تنیدگی حالت $|\phi_+\rangle$ بیشتر است یا حالت زیر

$$|\chi\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)? \quad (69)$$

خوشبختانه نه تنها می توان نشان داد که این سوال با معناست و می توان درهم تنیدگی هر سه حالت بالا را با هم مقایسه کرد بلکه می توان نشان داد که میزان درهم تنیدگی این سه حالت را به صورت ساده ای می توان اندازه گرفت . در واقع میزان درهم تنیدگی یک حالت خالص دو بخشی برابر است با

$$\mathcal{E}(|\psi\rangle_{AB}) := S(\rho_A) = S(\rho_B), \quad (70)$$

که در آن S آنتروپی فون نویمان و ρ_A و ρ_B ماتریس های چگالی کاهش یافته هستند. بدیهی است که این دو ماتریس چگالی با هم مساوی نیستند ولی هر چه که باشند آنتروپی فون نویمان آنها باهم برابر است. به این ترتیب مقدار درهم تنیدگی این سه حالت به صورت زیر است:

$$\mathcal{E}(|\phi_+\rangle) = 1, \quad \mathcal{E}(|\psi\rangle) = 0.6, \quad \mathcal{E}(|\chi\rangle) = \log_2 3 = 1.58. \quad (71)$$

ولی این اعداد چه معنایی دارند؟ و چرا این اعداد را می توانیم به عنوان اندازه درهم تنیدگی تلقی کنیم؟ در این بخش پاسخ این سوال ها را خواهیم یافت.

برای پاسخ به این سوال ها نخست توجه می کنیم که اگر بین دو آزمایشگاه تعداد 100 تا زوج بل وجود داشته باشد منطقی است که بگوییم به اندازه 100 واحد درهم تنیدگی بین این دو آزمایشگاه به اشتراک گذاشته شده است زیرا این دو آزمایشگاه با این زوج ها می توانند روی 100 تا کیوبیت اعمال غیرکلاسیکی مثل فرابرد کوانتومی انجام دهند. حال اگر بین این دو آزمایشگاه 100 تا حالت از نوع

$$|\phi\rangle = \sqrt{0.85}|00\rangle + \sqrt{0.15}|11\rangle$$

وجود داشته باشد، آنگاه منطقی است که ببینیم این دو آزمایشگاه با انجام اعمال موضعی روی این حالت ها چه تعداد زوج بل می توانند درست کنند. هرگاه بتوانند تعداد 60 تا زوج درهم تنیده درست کنند می توانیم بگوییم که ارزش درهم تنیدگی هر کدام از حالت هایشان به اندازه 0.6 واحد است. در واقع برخورد ما با اندازه درهم تنیدگی درست شبیه به مبادله پول و سرمایه است. از آنجا که همه اعمال موضعی که ما انجام می دهیم نتایج احتمالاتی دارند این تبدیل حالت و مبادله ارزش درهم تنیدگی می بایست در حد مجانبی تعریف شود. یعنی اینکه اگر بین دو آزمایشگاه تعداد N تا حالت درهم تنیده $|\phi\rangle$ به اشتراک گذاشته شده باشد و بتوان از این حالت ها تعداد k تا حالت بل درست کرد آنگاه می گوییم

$$N\mathcal{E}(|\phi\rangle) = k\mathcal{E}(|\phi_+\rangle) = k \times 1 = k, \quad (72)$$

و یا

$$\mathcal{E}(|\phi\rangle) := \lim_{N \rightarrow \infty} \frac{k}{N}. \quad (73)$$

در زیر نشان می دهیم که با دنبال کردن این تعریف دقیقاً به این نتیجه می رسیم که اندازه درهم تنیدگی برابر است با آنتروپی فون نویمان ماتریس چگالی کاهش یافته به ترتیبی که در بالا تعریف کرده ایم. دقت کنید که این نتیجه برای هر بعدی برقرار است یعنی اگر بین دو آزمایشگاه تعداد 100 تا حالت $|\chi\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)$ به اشتراک گذاشته باشد آنها می توانند از این حالت ها تعداد تقریبی 158 تا حالت بل درست کنند.

■ تمرین: حالت زیر را در نظر بگیرید:

$$|\psi\rangle_{AB} = \sqrt{1-p}|00\rangle + \sqrt{p}|11\rangle, \quad p \leq 0.5. \quad (74)$$

آیس یک اندازه گیری غیر متعامد با عملگرهای زیر روی کیویت خودش انجام می دهد:

$$A := \begin{pmatrix} \sqrt{\lambda p} & 0 \\ 0 & \sqrt{\lambda(1-p)} \end{pmatrix}, \quad B := \begin{pmatrix} \sqrt{1-\lambda p} & 0 \\ 0 & \sqrt{1-\lambda(1-p)} \end{pmatrix}. \quad (75)$$

با این اندازه گیری اگر آیس نتیجه A را بدست بیاورد حالت $|\psi_{AB}\rangle$ به یک حالت بل تبدیل می شود. این احتمال را بدست بیاورید. احتمال را بیشینه کنید و بگویید که اگر آیس تعداد 1000 تا از این حالت ها داشته باشد تقریباً چند تا حالت بل می تواند درست کند. با روشی که به کار برده اید چه ارزش درهم تنیدگی ای به حالت $|\psi\rangle_{AB}$ نسبت می دهید؟

مسئله ای که حل کردیم یک روش برای تقطیر درهم تنیدگی است. اما این روش الزاماً بهترین روش نیست چرا که آیس فقط روی یک کیویت اندازه گیری می کند و حال آنکه اگر تعداد زیادی از این حالت ها بین آیس و باب به اشتراک گذاشته شده باشد، آیس می تواند روی دسته های آنها یا حتی همه کیویت هایی که در اختیار دارد اندازه گیری جمعی انجام دهد. در واقع بهترین روش همانطور که نشان خواهیم داد متکی بر مفهوم رشته های نمونه است که در واقع از ابتدا تا کنون تم هماهنگ کننده همه نتایج مربوط به آنتروپی شان و آنتروپی فون نویمان بوده است. برای درک این موضوع فرض کنید که آیس و

باب تعداد خیلی زیادی از رشته های $|\psi\rangle_{AB}$ را در اختیار دارند. این تعداد رشته را N بگیرد. بنابراین حالتی که در دست آنهاست این است:

$$|\Psi(N)\rangle = |\psi\rangle_{AB}^{\otimes N} = (\sqrt{1-p}|00\rangle + \sqrt{p}|11\rangle)^{\otimes N} \quad (۷۶)$$

برای سادگی فرض کنید که $N = 3$ باشد. در این صورت بسط حالت بالا به شکل زیر در می آید:

$$\begin{aligned} |\Psi(3)\rangle_{a_1 b_1, a_2 b_2, a_3 b_3} &= \sqrt{1-p}^3 |00, 00, 00\rangle + \sqrt{1-p}^2 \sqrt{p} (|00, 00, 11\rangle + |00, 11, 00\rangle + |11, 00, 00\rangle) \\ &+ \sqrt{1-p} \sqrt{p}^2 (|11, 11, 00\rangle + |11, 00, 11\rangle + |00, 11, 11\rangle) + \sqrt{p}^3 |11, 11, 11\rangle. \end{aligned} \quad (۷۷)$$

اندیس های این حالت نشان می دهد که کدام کیوبیت ها در دست آلیس و کدام در دست باب هستند. می توان این حالت را به صورت زیر بازنویسی کرد:

$$\begin{aligned} |\Psi(3)\rangle_{a_1 a_2 a_3; b_1 b_2 b_3} &= \sqrt{1-p}^3 |000, 000\rangle + \sqrt{1-p}^2 \sqrt{p} (|001, 001\rangle + |010, 010\rangle + |100, 100\rangle) \\ &+ \sqrt{1-p} \sqrt{p}^2 (|110, 110\rangle + |101, 101\rangle + |011, 011\rangle) + \sqrt{p}^3 |111, 111\rangle. \end{aligned} \quad (۷۸)$$

حال آلیس می تواند روی سه کیوبیتی که در دست دارد اندازه گیری جمعی انجام دهد و به اصطلاح اسپین کل آنها را اندازه بگیرد. در این صورت آلیس چهار نتیجه متفاوت هرکدام با یک احتمال بدست می آورد و حالت دست او و هم چنین دست باب به یکی از حالت های زیر تصویر می شود:

$$\begin{aligned} |\Psi_0(3)\rangle &= |000, 000\rangle & Pr(0) &= (1-p)^3, \\ |\Psi_1(3)\rangle &= \frac{1}{\sqrt{3}} (|001, 001\rangle + |010, 010\rangle + |100, 100\rangle) & Pr(1) &= (1-p)^2 p \\ |\Psi_2(3)\rangle &= \frac{1}{\sqrt{3}} (|110, 110\rangle + |101, 101\rangle + |011, 011\rangle) & Pr(2) &= (1-p) p^2 \\ |\Psi_3(3)\rangle &= |111, 111\rangle & Pr(3) &= p^3. \end{aligned} \quad (۷۹)$$

نکته مهم این است که حالت دست آلیس و باب همواره به یک حالت که ترکیبی یکنواخت با ضرایب یکسان از حالت های مختلف است تصویر می شود. این نکته چنانکه در آینده خواهیم دید اهمیت دارد. حال که خواننده با حالت $N = 3$ آشنا شده است می تواند حالت کلی را برای خود تجزیه و تحلیل کند و آن را براحتی بفهمد. می توانیم بگوییم که وقتی در حالت کلی آلیس روی N تا اسپین خود این اندازه گیری جمعی را انجام می دهد حالت در دست او و باب به یکی از حالت های زیر

تصویر می شود:

$$|\Psi_k(N)\rangle_{a_1 a_2 \dots a_N; b_1 b_2 \dots b_N} = \frac{1}{\sqrt{\binom{N}{k}}} \sum'_{s_1, s_2 \dots s_N=0,1} |s_1 s_2 \dots s_N; s_1 s_2 \dots s_N\rangle \quad (۸۰)$$

که در آن جمع $\sum'$ روی تمام رشته هایی است که دارای k تا 1 و $N-k$ تا 0 هستند. دقت کنید که تعداد حالت های $|s_1 s_2 \dots s_N; s_1 s_2 \dots s_N\rangle$ برابر است با $\binom{N}{k}$. احتمال اینکه حالت اولیه به یک حالت $|\Psi_k(N)\rangle$ تصویر شود برابر است با

$$Pr(k) = \binom{N}{k} \times (1-p)^k p^{N-k}$$

. حال آن چه را که در باره رشته های نمونه دیده بودیم به یاد می آوریم و آن اینکه محتمل ترین رشته ها آنهایی هستند که تعداد 1 های آنها برابر است با $N(1-p)$ و تعداد 0 های آنها برابر است با Np . از خود می پرسیم که احتمال تصویر شدن حالت اولیه به حالتی که شامل رشته های نوعی باشد چقدر است ؟ یعنی احتمال تصویر شدن حالت اولیه به حالتی نزدیک به حالت $|\Psi_{Np}(N)\rangle$ ؟ این احتمال تقریباً برابر است با:

$$Pr(k = Np) = \binom{N}{Np} \times (1-p)^{Np} p^{N(1-p)} \quad (۸۱)$$

اما می دانیم که در حد N های بزرگ این احتمال برابر خواهد بود با

$$Pr(k = Np) \approx 2^{NH(p)} \times 2^{-NH(p)} \approx 1 \quad (۸۲)$$

که در آن

$$H(p) = -p \log p - (1-p) \log(1-p) = S(\rho_A). \quad (۸۳)$$

معنای این حرف این است که در این اندازه گیری تقریباً به طور قطع حالت آلیس و باب به حالت $|\Psi_{Np}(N)\rangle$ تصویر می شود و این حالت چیزی نیست جز ترکیب یکنواختی از رشته های نوعی که تعداد آن ها نه 2^N تا بلکه $2^{NS(\rho)}$ تا است. حال می توانیم با یک عملگر یکانی این حالت را به یک حالت تبدیل کنیم که نشان دهنده ضرب تانسوری تعداد $N(S(\rho))$ تا حالت بل باشد. برای فهمیدن بهتر این قضیه به مثال زیر توجه می کنیم: فرض کنید که $N=4$ و $p=\frac{1}{4}$ است. در این صورت حالت $|\Psi_1(4)\rangle$ برابر است با :

$$|\Psi_1(4)\rangle = \frac{1}{\sqrt{4}} (|1000, 1000\rangle + |0100, 0100\rangle + |0010, 0010\rangle + |0001, 0001\rangle)_{a_1 a_2 a_3 a_4; b_1 b_2 b_3 b_4}. \quad (۸۴)$$

آلیس و باب می توانند هر کدام یک عملگر یکانی روی حالت خود اعمال کنند که تبدیل زیر را انجام دهد:

$$\begin{aligned} |1000\rangle &\longrightarrow |00\rangle \otimes |00\rangle, \\ |0100\rangle &\longrightarrow |01\rangle \otimes |00\rangle, \\ |0010\rangle &\longrightarrow |10\rangle \otimes |00\rangle, \\ |0001\rangle &\longrightarrow |11\rangle \otimes |00\rangle. \end{aligned} \quad (۸۵)$$

در این صورت حالت بالا تبدیل می شود به

$$|\Phi\rangle = \frac{1}{\sqrt{4}} (|00, 00\rangle + |01, 01\rangle + |10, 10\rangle + |11, 11\rangle)_{a_1 a_2; b_1 b_2} \otimes |00\rangle_{a_3 a_4} \otimes |00\rangle_{b_3 b_4}. \quad (۸۶)$$

سپس آنها می توانند کیوبیت های 3, 4 را برای کار دیگری ذخیره کنند و به کیوبیت های 1, 2 توجه کنند. حالت این کیوبیت ها برابر است با

$$|\chi\rangle_{a_1 b_1; a_2 b_2} = \frac{1}{\sqrt{4}} (|00, 00\rangle + |00, 11\rangle + |11, 00\rangle + |11, 11\rangle)_{a_1 b_1; a_2 b_2}. \quad (۸۷)$$

اما حالت آخر چیزی نیست جز

$$|\chi\rangle_{a_1 b_1; a_2 b_2} = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)_{a_1 b_1} \otimes \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)_{a_2 b_2}, \quad (۸۸)$$

یعنی دو تا حالت کامل بل که در دست آلیس و باب باقی مانده است. حال با دیدن این مثال می توانیم به حالت کلی باز گردیم و خودمان را قانع کنیم که آلیس و باب می توانند در حد مجانبی یعنی وقتی که N خیلی زیاد است، از تعداد N تا حالت $|\phi\rangle = \sqrt{1-p}|00\rangle + \sqrt{p}|11\rangle$ که در دست دارند، تعداد $NS(\rho)$ تا حالت بل درست کنند.