نظریه اطلاعات کوانتومی ۱ ترم پاییز ۱۳۹۱-۱۳۹۲
مدرسین: ابوالفتح بیگی و امین‌زاده گوهری نویسنده: پیام دلگشا

جلسه ۱۰

---

۱ اندازه‌گیری POVM

جلسه‌ی قبل در مورد اندازه‌گیری صحبت کردیم. در اصل اندازه‌گیری دو موضوع مهم وجود داشت: یکی اینکه نتیجه‌ی اندازه‌گیری چه توزیع احتمالی دارد و دوم اینکه بعد از اندازه‌گیری حالت سیستم چگونه تغییر می‌کند. گاهی اوقات ممکن است صرفا توزیع احتمال نتیجه‌ی اندازه‌گیری برای ما مهم باشد و علاقمند به دانستن اینکه حالت سیستم چگونه تغییر می‌کند نباشیم.

به عنوان یادآوری از جلسه‌ی قبل، یک اندازه‌گیری با عملگرهای $M_i : \mathcal{H} \to \mathcal{H}$ داده می شود که

$$\sum_i M_i^\dagger M_i = I_{\mathcal{H}}.$$

نتیجه اندازه گیری با احتمال $p_i = \langle \Psi | M_i^\dagger M_i | \Psi \rangle$ برابر i است و در این صورت حالت سیستم به

$$\frac{M_i|\Psi\rangle}{\|M_i|\Psi\rangle\|}$$

تغییر می کند. همان طور که مشاهده می‌کنیم عبارت احتمال p_i به خود M_i وابسته نیست، بلکه به $M_i^\dagger M_i$ وابسته است. به عبارت دیگر حتی اگر M_iها را نداشته باشیم اما $M_i^\dagger M_i$ را داشته باشیم، می‌توانیم پیدا کنند که نتیجه‌ی آزمایش به چه احتمالی برابر i است.

برای این منظور، زمانی که هدف صرفا تعیین احتمال نتیجه‌ی اندازه‌گیری باشد، راحت‌تر است که با عملگرهای $E_i = M_i^\dagger M_i$ کار کنیم که به آنها عملگرهای POVM[1] گفته می‌شود. دقت کنید $E_i^\dagger = M_i^\dagger M_i = E_i$ بنابراین E_i هرمیتی است. از طرفی داریم:

$$\langle v|E_i|v\rangle = \langle v|M_i^\dagger M_i|v\rangle = \|M_i|v\rangle\|^2 \geq 0,$$

بنابراین $E_i \geq 0$. از طرفی شرط کامل بودن ایجاب می‌کند که

$$\sum E_i = \sum M_i^\dagger M_i = I. \tag{۱}$$

بنابراین عملگرهای POVM دارای دو شرط $E_i \geq 0$ و $\sum E_i = I$ هستند.

[1] Positive Operator Valued Measure

تعریف ۱. عملگرهای $E_1, \ldots, E_k : \mathcal{H} \to \mathcal{H}$ را یک اندازه‌گیری $POVM$ خوانده می‌شوند هرگاه

۱. $E_i \geq 0$

۲. $\sum_i E_i = I_{\mathcal{H}}$

تا به حال نشان دادیم که برای هر اندازه‌گیری می‌توان عملگرهای POVM را تعریف نمود. سوالی که ممکن است مطرح شود این است که آیا برای هر دسته عملگر POVM (که در دو شرط $E_i \geq 0$ و $\sum E_i = I$ صدق کنند)، آیا می‌توان اندازه‌گیری پیدا نمود که متناظر با آن باشد؟جواب مثبت است، کافی است عملگر آزمایش M_i را به صورت

$$M_i = E_i^{1/2},$$

تعریف کنیم. دقت کنید $E_i \geq 0$ بنابراین جذر آن معنی دارد و

$$M_i^\dagger M_i = M_i^2 = E_i.$$

از طرفی داریم:

$$\sum_i M_i^\dagger M_i = \sum_i E_i = I.$$

بنابراین M_iها یک اندازه‌گیری تشکیل می‌دهند. به علاوه برای این اندازه‌گیری داریم

$$p_i = \langle\psi|M_i^\dagger M_i|\psi\rangle = \langle\psi|E_i|\psi\rangle.$$

بنابراین تناظری بین عملگرهای POVM و عملگرهای اندازه‌گیری وجود دارد. البته توجه کنید این تناظر یک به یک نیست، به این معنی که یک دسته عملگر POVM با چند دسته عملگر اندازه‌گیری معادل است.

مثال ۲. مجموعه عملگرهای

$$\{E_0 = |0\rangle\langle 0|, E_1 = |1\rangle\langle 1|\}$$

را برای یک کیوبیت در نظر بگیرید. اگر تعریف کنیم

$$\{M_0 = |0\rangle\langle 0|, M_1 = |1\rangle\langle 1|\}, \quad \{N_0 = |+\rangle\langle 0|, N_1 = |-\rangle\langle 1|\},$$

که در آن $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ می بینیم که

$$E_i = M_i^\dagger M_i = N_i^\dagger N_i.$$

بنابر این به یک مجموعه از $\{E_i\}$ها می‌توان $\{M_i\}$ های مختلفی را نسبت داد. به طور کلی $\{M_i\}$ و $\{U_i M_i\}$ که در آن $\{U_i\}$ ها ماتریس‌های یکانی دلخواه هستند، به یک مجموعه از عملگرهای POVM منجر می شوند.

تمرین ۳. فرض کنید یک اندازه‌گیری با عملگرهای M_m متناظر شده است. نشان دهید عملگرهای یکانی U_m وجود دارند به طوری که $M_m = U_m\sqrt{E_m}$ که در آن E_m عملگرهای POVM متناظر هستند.

مثال ۴ (تمیز دادن حالات کوانتمی). فرض کنید یک سیستم فیزیکی به طور تصادفی و با توزیع یکنواخت در یکی از حالات $|\psi_1\rangle, \dots, |\psi_k\rangle$ قرار داده شده است و ما می‌خواهیم تشخیص دهیم در کدام حالت است. برای این کار می‌توانیم روی سیستم یک اندازه‌گیری انجام دهیم به طوری که حاصل اندازه‌گیری یک اندیس $1 \leq i \leq k$ باشد، که در این صورت حدس می‌زنیم که حالت سیستم $|\psi_i\rangle$ بوده است. حال سؤال این است که چه اندازه‌گیریی انجام دهیم که احتمال درست حدس زدن ما بیشینه شود.

توجه کنید که در این مسأله تغییر حالت سیستم بعد از اندازه‌گیری برای ما مهم نیست. لذا بهتر است که از فرمول بندی POVM استفاده کنیم. پس عملگرهای $E_1, \dots, E_k$ را با خواص $E_i \geq 0$ و $\sum_i E_i = I$ می‌گیریم و سیستم را با این POVM اندازه می‌گیریم. حاصل اندازه گیری i معادل حدس $|\psi_i\rangle$ است. پس احتمال حدس درست را می‌توان محاسبه کرد:

$$\begin{aligned} Pr[\text{ حدس درست }] &= \sum_{i=1}^{k} Pr[\text{ حالت سیستم } |\psi_i\rangle \text{ باشد }] \cdot Pr[\text{ حدس درست } | \text{ حالت سیستم } |\psi_i\rangle \text{ باشد }] \\ &= \sum_{i=1}^{k} \frac{1}{k} Pr[\text{ حدس درست } | \text{ حالت سیستم } |\psi_i\rangle \text{ باشد }]. \end{aligned}$$

حال توجه کنید که اگر حالت سیستم $|\psi_i\rangle$ باشد، حدس درست معادل این است که حاصل اندازه‌گیری i باشد که این با احتمال $\langle\psi_i|E_i|\psi_i\rangle$ اتفاق می‌افتد. در نتیجه داریم

$$Pr[\text{ حدس درست }] = \frac{1}{k} \sum_{i=1}^{k} \langle\psi_i|E_i|\psi_i\rangle.$$

بنابراین برای بیشینه کردن احتمال حدس درست باید

$$\max \frac{1}{k} \sum_{i} \langle\psi_i|E_i|\psi_i\rangle$$

را با شرایط $E_i \geq 0$ و $\sum_{i=1}^{k} E_i = I$ حساب کنیم. جواب این مساله در حالت کلی فرم بسته ندارد.

تمرین ۵. نشان دهید که اگر در اندازه‌گیری بالا، حالتی را هم برای خطا در اعلام حالت یا $E_{k+1} = E_{\text{error}}$ در نظر می‌گرفتیم، ماکسیمم احتمال کدگشایی درست تغییری نمی‌کرد.

تمرین ۶. مساله‌ی بهینه‌سازی فوق را برای حالت خاص $\psi_1 = |0\rangle$ و $\psi_2 = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ در فضای $\mathbb{C}^2$ حل کنید.

تمرین ۷. نشان دهید احتمال حدس درست برابر یک است اگر و تنها اگر $|\psi_i\rangle$ها دوبدو بر هم عمود باشند.

تمرین ۸. نشان دهید هر اندازه‌گیری که در آن عملگرهای اندازه‌گیری با عملگرهای POVM یکی باشند، اندازه‌گیری تصویری است.

۲ اصل عدم قطعیت هایزنبرگ

در این بخش کمی به این موضوع می‌پردازیم که مطالبی که تا به حال بررسی کرده‌ایم، در فیزیک به چه صورت بیان می‌شوند و چه نتایجی در مکانیک کوانتومی دارند.

تعریف ۹. در فیزیک هر کمیت فیزیکی با یک عملگر هرمیتی مانند A متناظر است که میانگین آن کمیت برابر است با $\langle\psi|A|\psi\rangle$.

حال ارتباط این موضوع را با مطالبی که تا به حال بیان کردیم بررسی می‌کنیم. چون عملگر A هرمیتی است، در یک پایه‌ی متعامد یکه‌ای مثل $|v_0\rangle, \ldots, |v_{d-1}\rangle$ قطری می‌شود:

$$A = \sum_{i=0}^{d-1} \lambda_i |v_i\rangle\langle v_i| \qquad\qquad \lambda_i \in \mathbb{R},$$

حال چون $|v_i\rangle$ها متعامد یکه هستند، می‌توان یک اندازه‌گیری در این پایه تعریف کرد که درواقع

$$M_i = |v_i\rangle\langle v_i|,$$

و اگر حاصل اندازه‌گیری i بود، کمیت فیزیکی را برابر λ_i تعریف می‌کنیم. بنابراین متوسط این کمیت فیزیکی برابر است با

$$\begin{aligned}\mathbb{E}\left[\text{کمیت فیزیکی}\right] &= \sum Pr\left[\text{حاصل اندازه‌گیری} = i\right] \times \lambda_i \\ &\overset{(a)}{=} \sum \langle\psi|M_i|\psi\rangle\lambda_i \\ &= \langle\psi|\left(\sum \lambda_i M_i\right)|\psi\rangle \\ &= \langle\psi|A|\psi\rangle,\end{aligned}$$

که همان چیزی است که در تعریف گفته شده بود. دقت کنید (a) به این دلیل درست است که $M_i^\dagger M_i = M_i^2 = M_i$ چراکه M_i عملگر تصویری است.

همان طور که میانگین کمیت را حساب کردیم، انحراف معیار آن را نیز می‌توانیم محاسبه کنیم. ابتدا دقت کنید که میانگین و انحراف معیار هردو به حالت سیستم وابسته هستند، بنابراین انحراف معیار کمیت را با $\Delta(A)_{|\psi\rangle}$ نشان می‌دهیم. اگر متغیر تصادفی را با λ نشان دهیم داریم:

$$\begin{aligned}\mathbb{E}\left[\lambda^2\right] &= \sum \langle\psi|M_i|\psi\rangle\lambda_i^2 \\ &= \langle\psi|\left(\sum \lambda_i^2 M_i\right)|\psi\rangle,\end{aligned}$$

حال ادعا می‌کنیم که $\sum \lambda_i^2 M_i = A^2$. دقت کنید M_iها عملگر تصویری هستند بنابراین $M_i^2 = M_i$ ضمنا چون $|v_i\rangle$ها بر هم عمود هستند، برای $i \neq j$ داریم $M_i M_j = |v_i\rangle\langle v_i||v_j\rangle\langle v_j| = 0$ بنابراین

$$\begin{aligned}A^2 = \left(\sum \lambda_i M_i\right)^2 &= \sum_{i,j} \lambda_i\lambda_j M_i M_j \\ &= \sum_i \lambda_i^2 M_i^2 + \sum_{i\neq j} \lambda_i\lambda_j M_i M_j \\ &= \sum \lambda_i^2 M_i,\end{aligned}$$

بنابراین
$$\Delta(A)_{|\psi\rangle} = \left(\mathbb{E}\left[\lambda^2\right] - \mathbb{E}\left[\lambda\right]^2\right)^{1/2} = \left(\langle\psi|A^2|\psi\rangle - \langle\psi|A|\psi\rangle^2\right)^{1/2}.$$
حال می‌توانیم اصل عدم قطعیت هایزنبرگ را بیان نماییم.

اصل (عدم قطعیت هایزنبرگ). برای کمیت‌های فیزیکی (عملگرهای هرمیتی) A و B داریم
$$\Delta(A)_\psi \Delta(B)_\psi \geq \frac{1}{2}\left|\langle\psi|[A,B]|\psi\rangle\right| \tag{۲}$$
که در آن $[A,B] = AB - BA$ جابجاگر A و B هستند.

درواقع این اصل بیان می‌کند که اگر دو عملگر داشته باشیم که با هم جابجا نشوند، یعنی $AB \neq BA$ طرف راست (۲) احتمالا صفر نیست[۲] و بنابراین طرف چپ نمی‌تواند صفر باشد. به عبارت دیگر اگر $\Delta(A)_{|\psi\rangle}$ بسیار کوچک باشد (کمیت A را بتوان با دقت زیادی اندازه‌گیری نمود) $\Delta(B)_{|\psi\rangle}$ نمی‌تواند خیلی کوچک باشد. در دنیای کلاسیک تمام عملگرها با هم جابجا می‌شوند (و قطری هستند) بنابراین طرف راست صفر است و این اصل نتیجه‌ای ندارد. اما در دنیای کوانتوم چنین نیست. مثلا اگر A عملگر مکان باشد و B عملگر تکانه باشد داریم $AB - BA = i\hbar I$ و این دو عملگر با هم جابجا نمی‌شوند.[۳] اصل عدم قطعیت هایزنبرگ می‌گوید $\Delta(A)_\psi\Delta(B)_\psi \geq \frac{\hbar}{2}$. بنابراین نمی‌توان هم مکان و هم تکانه‌ی یک سیستم را با دقت داشته باشیم. یا به عبارتی دقت و قطعیت در یکی باعث عدم قطعیت در دیگری می‌شود.

۳ اصل سوم: تحول زمانی

در این بخش این موضوع را بررسی می‌کنیم که حالت یک سیستم کوانتمی در طول زمان چگونه تغییر می‌کند. برای این منظور اصل تحول زمانی بیان می‌کند که:

اصل (تحول زمانی). تحول زمانی یک سیستم «بسته» با یک عملگر یکانی که روی فضای هیلبرت عمل می کند بیان می شود. یعنی اگر حالت سیستم در زمان t_0 ، $|\psi\rangle$ باشد و در زمان t_1، $|\psi'\rangle$ باشد، آنگاه $U : \mathcal{H} \to \mathcal{H}$ یکانی وجود دارد که $U|\psi\rangle = |\psi'\rangle$. U مستقل از $|\psi\rangle$ و $|\psi'\rangle$ است و فقط به t_0 و t_1 بستگی دارد.

دقت کنید حالت سیستم در لحظه‌ی t_2 باید با نرم واحد باشد که این خاصیت برقرار است چون عملگرهای یکانی طول را حفظ می‌کنند.

این اصل در واقع فرمول‌بندی دیگری از «معادله‌ی شرودینگر» است. این معادله تحول زمانی یک سیستم کوانتمی را به صورت زیر بیان می‌کند:
$$i\hbar\frac{d}{dt}|\psi(t)\rangle = H|\psi(t)\rangle,$$
که در آن $H : \mathcal{H} \to \mathcal{H}$ یک عملگر هرمیتی (در حالت کلی دلخواه) است که به آن «همیلتونی» گفته می‌شود. اگر H مستقل از زمان باشد، جواب این معادله‌ی دیفرانسیل به صورت زیر است:
$$|\psi(t)\rangle = e^{-\frac{it}{\hbar}H}|\psi(0)\rangle.$$

[۲] می‌گوییم احتمالا صفر نیست چون این عبارت به $|\psi\rangle$ نیز بستگی دارد.
[۳] $\hbar$ ثابت پلانک است.

حال اگر قرار دهیم

$$U = e^{-\frac{it}{\hbar}H}, \tag{۳}$$

آنگاه $|\psi(t)\rangle = U|\psi(0)\rangle$. پس برای نشان دادن سازگاری معادله‌ی شرودینگر با اصلی که بیان کردیم کافی است نشان دهیم که U یکانی است، یعنی $U^\dagger U = I = UU^\dagger$. بسط تیلور تابع e^x را در نظر بگیرید: $e^x = \sum_n a_n x^n$ که در آن a_n اعدادی حقیقی هستند.

$$U = \sum_n a_n \left(-\frac{it}{\hbar}H\right)^n$$

و در نتیجه

$$\begin{aligned}
U^\dagger &= \left[\sum_n a_n \left(-\frac{it}{\hbar}H\right)^n\right]^\dagger \\
&= \sum_n a_n \left[\left(-\frac{it}{\hbar}H\right)^n\right]^\dagger \\
&= \sum_n a_n \left[\left(-\frac{it}{\hbar}H\right)^\dagger\right]^n \\
&= \sum_n a_n \left(\frac{it}{\hbar}H^\dagger\right)^n \\
&= \sum_n a_n \left(\frac{it}{\hbar}H\right)^n \\
&= e^{\frac{it}{\hbar}H}.
\end{aligned}$$

اما می‌دانیم که دو عملگر نرمال در یک پایه‌ی متعامد یکه قطری می‌شوند اگر و تنها اگر جابجا شوند. دو عملگر $\frac{it}{\hbar}H$ و $-\frac{it}{\hbar}H$ با هم جابجا می‌شوند در نتیجه

$$U^\dagger U = e^{\frac{it}{\hbar}H}.e^{-\frac{it}{\hbar}H} = e^{(\frac{it}{\hbar}H - \frac{it}{\hbar}H)} = e^0 = I$$

به همین ترتیب $UU^\dagger = I$، و در نتیجه U یکانی است. در حالت کلی‌تر، وقتی که همیلتونی H مستقل از زمان نیست نیز می‌توان نشان داد که $|\psi(0)\rangle$ و $|\psi(t)\rangle$ با یک عملگر یکانی به هم تبدیل می‌شوند.

برعکس، برای هر U یکانی، همیلتونی H وجود دارد به طوری که (۳) برقرار باشد، درواقع کافی است قرار دهیم

$$H = \frac{\hbar}{it}\log U. \tag{۴}$$

بنابراین، اصل دوم که تحول زمانی سیستم‌های کوانتمی را با عملگرهای یکانی بیان می‌کند، در واقع فرمول‌بندی دیگری از معادله‌ی شرودینگر است.

تمرین ۱۰. نشان دهید همیلتونی که از معادله‌ی (۴) بدست می‌آید همان تحول زمانی در معادله‌ی شرودینگر را نتیجه می‌دهد.

در ادامه وقتی صحبت از تحول زمانی می‌کنیم منظورمان عملگر یکانی است، که همان طور که در بالا مشاهده کردیم، در عمل این عملگر یکانی از یک همیلتونی استخراج می‌شود.

همیلتونی در واقع برهم‌کنش بین اجزای یک سیستم را نشان می‌دهد. پس در عمل برای طراحی یک تحول زمانی باید از روی ماتریس یکانی مورد نظر عملگر همیلتونی را محاسبه کنیم و بعد برهم‌کنش متناظر را روی سیستم اعمال نماییم.

۴ اصل چهارم: سیستم‌های ترکیبی

تا به حال در مورد فضای حالت یک سیستم، اندازه‌گیری یک سیستم و تحول زمانی یک سیستم صحبت کردیم. حال می‌خواهیم ببینیم وقتی چند سیستم کنار هم قرار داشته باشند این موارد چگونه تغییر می‌کند.

اصل (سیستم‌های ترکیبی). فضای هیلبرت متناظر با یک سیستم فیزیکی که متشکل از n سیستم کوچکتر (زیرسیستم)[۴] است از ضرب تانسوری فضاهای کوچک‌تر بدست می آید. به عبارت دیگر اگر فضای هیلبرت متناظر با سیستم i-ام، $\mathcal{H}_i$ باشد، فضای هیلبرت متناظر با کل n سیستم برابر است با

$$\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n.$$

اگر سیستم i-ام در حالت $|\psi_i\rangle \in \mathcal{H}_i$ باشد، کل سیستم در حالت $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$ است.

برای مثال دو کیوبیت A و B را در نظر بگیرید و فرض کنید $\mathcal{H}_A$ و $\mathcal{H}_B$ فضای هیلبرت معادل هر کدام از این کوبیت‌ها با پایه‌های $\{|0\rangle_A, |1\rangle_A\}$ و $\{|0\rangle_B, |1\rangle_B\}$ باشند. طبق اصل چهارم فضای هیلبرت متناظر با سیستم ترکیبی این دو کیوبیت برابر است با:

$$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B.$$

که با پایه‌ی متعامد یکه‌ی

$$\{|0\rangle_A \otimes |0\rangle_B, |0\rangle_A \otimes |1\rangle_B, |1\rangle_A \otimes |0\rangle_B, |1\rangle_A \otimes |1\rangle_B\} = \{|00\rangle_{AB}, |01\rangle_{AB}, |10\rangle_{AB}, |11\rangle_{AB}\}$$

مشخص می‌شود. دقت کنید که در این نمادگذاری ترتیب مهم است و اول عضو فضای A را می‌نویسیم .

هر $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ به صورت ترکیب خطی از چهار عضو مجموعه‌ی بالا است. اگر $|\psi\rangle_{AB}$ را بتوان به صورت $|\psi\rangle_{AB} = |v\rangle_A \otimes |w\rangle_B$ نمایش داد به این حالت، حالت ضربی[۵] یا جدایی‌پذیر[۶] گفته می شود. اگر چنین نمایشی برای $|\psi\rangle_{AB}$ وجود نداشته باشد به آن حالت درهم تنیده[۷] می گویند.

به عنوان مثال

$$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = \frac{1}{\sqrt{2}}|0\rangle_A \otimes (|0\rangle_B + |1\rangle_B)$$

[۴] Subsystem
[۵] product state
[۶] separable state
[۷] entangled state

حالت ضربی و

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

حالت درهم تنیده است.

در واقع حالت ضربی حالتی است که عدد اشمیت[۸] آن 1 باشد. توجه کنید که طبق قضیه‌ی تجزیه‌ی اشمیت[۹] هر عضو دلخواه $|\psi\rangle_{AB} \in \mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ را می توان به صورت

$$|\psi\rangle_{AB} = \sum_{i=0}^{d-1} \lambda_i |v_i\rangle_A |w_i\rangle_B$$

نمایش داد که λ_i ها نامنفی باشند و $\{|v_i\rangle\}$ و $\{|w_i\rangle\}$ ها پایه متعامد یکه برای به ترتیب $\mathcal{H}_A$ و $\mathcal{H}_B$ باشند. تعداد λ_i های ناصفر یک کمیت خوش تعریف است و به آن عدد اشمیت حالت $|\psi\rangle_{AB}$ گویند. در این صورت یک حالت ضربی است اگر و فقط اگر عدد اشمیت آن یک باشد.

۱.۴ اندازه‌گیری روی بخشی از یک سیستم ترکیبی

فرض کنید بخواهیم یک اندازه‌گیری روی بخش A از یک سیستم دو بخشی AB انجام دهیم. اندازه‌گیری روی A با عملگرهای

$$M_i : \mathcal{H}_A \to \mathcal{H}_A$$

با شرط $\sum_i M_i^\dagger M_i = I_{\mathcal{H}_A}$ مشخص می‌شود. در این صورت عملگرهای اندازه گیری متناظر روی سیستم ترکیبی AB

$$N_i^{AB} = M_i^A \otimes I^B$$

هستند. توجه کنید که شرط تمامیت برای N_i ها برقرار است:

$$\begin{aligned}
\sum_i N_i^\dagger N_i &= \sum_i (M_i \otimes I)^\dagger (M_i \otimes I) = \sum_i (M_i^\dagger \otimes I)(M_i \otimes I) \\
&= \sum_i (M_i^\dagger M_i \otimes I) = (\sum_i M_i^\dagger M_i) \otimes I \\
&= I^A \otimes I^B = I^{AB}.
\end{aligned}$$

در صورتی که حالت سیستم $|\psi\rangle_{AB}$ باشد احتمال اینکه حاصل اندازه‌گیری i باشد برابر است با

$$p(i) = \langle\psi|N_i^\dagger N_i|\psi\rangle = \langle\psi|M_i^\dagger M_i \otimes I|\psi\rangle$$

و بعد از اندازه گیری حالت سیستم به

$$\frac{1}{\|N_i|\psi\rangle\|} N_i|\psi\rangle = \frac{1}{\|M_i \otimes I|\psi\rangle\|} M_i \otimes I|\psi\rangle$$

[۸] Schmidt number
[۹] Schmidt decomposition

تغییر می کند.

اگر حالت سیستم ضربی باشد یعنی $|\psi\rangle_{AB} = |v\rangle_A \otimes |w\rangle_B$ داریم

$$\begin{aligned}
p(i) &= \langle v|_A \langle w|_B (M_i^\dagger M_i) \otimes I_B |v\rangle_A |w\rangle_B \\
&= \langle v|M_i^\dagger M_i|v\rangle \langle w|I|w\rangle \\
&= \langle v|M_i^\dagger M_i|v\rangle,
\end{aligned}$$

و حالت سیستم به

$$\frac{1}{\|M_i|v\rangle\|}(M_i|v\rangle) \otimes |w\rangle$$

تغییر می کند. نتیجه این که در حالت ضربی، وقتی اندازه‌گیری بر روی یک بخش از سیستم انجام می‌شود، نه توزیع احتمال حاصل و نه تغییر حالت هیچ کدام به بخش‌های دیگر ارتباطی ندارد.

برعکس، اگر حالت سیستم ترکیبی درهم تنیده باشد، مثلا

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

و اندازه‌گیری $\{M_0 = |0\rangle\langle 0|, M_1 = |1\rangle\langle 1|\}$ را روی سیستم اول اعمال کنیم، داریم:

$$\begin{aligned}
p(0) &= \frac{1}{2}(\langle 00| + \langle 11|)\,(|0\rangle\langle 0| \otimes I)\,(|00\rangle + |11\rangle) \\
&= \frac{1}{2}\left[\langle 00|(|0\rangle\langle 0| \otimes I)|00\rangle + \langle 00|(|0\rangle\langle 0| \otimes I)|11\rangle + \langle 11|(|0\rangle\langle 0| \otimes I)|00\rangle + \langle 11|(|0\rangle\langle 0| \otimes I)|11\rangle\right] \\
&= \frac{1}{2}\langle 00|(|0\rangle\langle 0| \otimes I)|00\rangle = \frac{1}{2}.
\end{aligned}$$

و اگر حاصل اندازه‌گیری 0 باشد تغییر سیستم

$$M_0^A \otimes I|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}|0\rangle|0\rangle \sim |0\rangle|0\rangle$$

خواهد بود. توجه کنید که در این حالت سیستم B نیز تغییر می کند.

اگر در سیستم ترکیبی AB سیستم A تحت تحول زمانی U_A باشد، عملگر تحول زمانی متناظر روی سیستم ترکیبی

$$U_A \otimes I_B$$

است.

در مثال زیر نحوه‌ی تولید زوج‌های درهم‌تنیده را مشاهده می‌کنیم.

مثال ۱۱. فرض کنید دو کیوبیت A و B در حالت‌های $|0\rangle_A$ و $|0\rangle_B$ قرار داده شده باشند. طبق اصل چهارم حالت سیستم ترکیبی $|\psi_1\rangle_{AB} = |0\rangle_A|0\rangle_B$ است. تحول زمانی هادامارد را که به صورت تعریف شده روی سیستم اول اعمال می‌کنیم:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

می‌توانید بررسی کنید که این ماتریس واقعا یکانی است و لذا تحول زمانی متناظر با آن مجاز است. طبق مطالبی که پیشتر بحث شد، تحول زمانی روی کل سیستم به صورت

$$U_{AB} = H_A \otimes I_B,$$

خواهد بود. اگر حالت سیستم بعد از اعمال این تحول زمانی $|\psi_2\rangle_{AB}$ باشد داریم

$$|\psi_2\rangle_{AB} = U_{AB}|\psi_1\rangle_{AB} = (H_A|0\rangle_A) \otimes |0\rangle_B = \frac{1}{\sqrt{2}}(|0\rangle_A + |1\rangle_A) \otimes |0\rangle_B,$$

همان طور که انتظار داشتیم حالت سیستم دوم تغییر نکرده است. حال تحول یکانی V_{AB} را روی فضای دو کیوبیت $\mathbb{C}^2 \otimes \mathbb{C}^2$ به صورت زیر در نظر بگیرید:

$$V_{AB} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

دقت کنید پایه‌ای که برای فضای حاصلضربی در نظر می‌گیریم، به ترتیب زیر است

$$|0\rangle|0\rangle \qquad |0\rangle|1\rangle \qquad |1\rangle|0\rangle \qquad |1\rangle|1\rangle,$$

و ستون‌های ماتریس V_{AB} تصویر این پایه هستند. بنابراین

$$\begin{aligned}
V_{AB}(|0\rangle_A|0\rangle_B) &= |0\rangle_A|0\rangle_B, \\
V_{AB}(|0\rangle_A|1\rangle_B) &= |0\rangle_A|1\rangle_B, \\
V_{AB}(|1\rangle_A|0\rangle_B) &= |1\rangle_A|1\rangle_B, \\
V_{AB}(|1\rangle_A|1\rangle_B) &= |1\rangle_A|0\rangle_B.
\end{aligned}$$

می‌توان عبارت فوق را به این صورت ساده نمود:

$$V_{AB}|x\rangle_A|y\rangle_B = |x\rangle_A|y \oplus x\rangle_B \qquad x, y \in \{0,1\}, \tag{۵}$$

که در آن $\oplus$ جمع در مبنای دو است.

با اعمال تحول زمانی V_{AB} روی $|\psi_2\rangle_{AB}$ داریم:

$$\begin{aligned}
V_{AB}|\psi_2\rangle_{AB} &= \frac{1}{\sqrt{2}} V_{AB}\left((|0\rangle_A + |1\rangle_A) \otimes |0\rangle_B\right) \\
&= \frac{1}{\sqrt{2}} V_{AB}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|0\rangle_B\right) \\
&= \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right),
\end{aligned}$$

که یک حالت درهم تنیده است و نمی‌توان آن را به صورت $|\phi_1\rangle|\phi_2\rangle$ نوشت.

در این مثال دیدیم که دو کیوبیت ابتدا از هم جدا و مستقل بودند. بعد از اعمال تحول زمانی اول ($|\psi_2\rangle$) هنوز جدایی‌پذیر است. اما بعد از اعمال V_{AB} دو سیستم دیگر جدا نبوده و درهم‌تنیده هستند. در واقع این موضوع از عبارت (۵) فهمیده می‌شود، چراکه عبارت $y \oplus x$ نشان می‌دهد که سیستم اول روی حالت سیستم دوم تاثیر می‌گذارد و آن را کنترل می‌کند. درواقع اگر $x = 0$ باشد y تغییری نمی‌کند اما اگر $x = 1$ باشد، y برعکس (NOT) می‌شود. به V_{AB} در اصطلاح Controlled Not و یا CNOT گفته می‌شود.

تمرین ۱۲. بررسی کنید که ماتریس هادامارد تعریف شده در مثال بالا یکانی است و $H^2 = I$. به علاوه مقادیر ویژه و بردارهای ویژه‌ی آن را نیز بیابید.

آ حل گزیده‌ای از تمرین‌ها

تمرین ۵ اگر ماکسیمم هنگامی که $k+1$ عملگر داشته باشیم را با Γ_{k+1} و هنگامی که k متغیر داریم را برابر Γ_k در نظر داریم، چون همیشه می‌توان E_{k+1} را صفر قرار داد

$$\Gamma_k \leq \Gamma_{k+1}.$$

حال فرض کنید ماکسیمم Γ_{k+1} به ازای عملگرهای $E_1, \dots, E_k, E_{k+1}$ اتفاق می‌افتد. تعریف کنید $E'_k = E_k + E_{k+1}$ در این صورت داریم چون $E_{k+1} \geq 0$

$$\sum_{i=1}^{k-1} \langle\psi_i|E_i|\psi_i\rangle + \langle\psi_k|E'_k|\psi_k\rangle = \sum_{i=1}^{k} \langle\psi_i|E_i|\psi_i\rangle + \langle\psi_k|E_{k+1}|\psi_k\rangle \geq \sum_{i=1}^{k} \langle\psi_i|E_i|\psi_i\rangle.$$

بنابراین $\Gamma_k \geq \Gamma_{k+1}$, و در نتیجه $\Gamma_k = \Gamma_{k+1}$.

تمرین ۶ باید مساله بهینه‌سازی زیر را حل کنیم:

$$p_{max} = \max_{E_1, E_2 : \text{POVM}} \frac{1}{2} \left[\langle\psi_2|E_1|\psi_2\rangle + \langle\psi_2|E_2|\psi_2\rangle\right].$$

اما چون $E_1 + E_2 = I$، $E_2 = I - E_1$ و چون $E_2 \geq 0$ داریم $0 \leq E_1 \leq I$ و در نتیجه مساله تبدیل می‌شود به

$$\begin{aligned} p_{max} &= \max_{0 \leq E \leq I} \frac{1}{2} \left(\langle\psi_1|E|\psi_1\rangle + \langle\psi_2|(I-E)|\psi_2\rangle\right) \\ &= \max_{0 \leq E \leq I} \frac{1}{2} \left(\langle\psi_1|E|\psi_1\rangle - \langle\psi_2|E|\psi_2\rangle + 1\right), \end{aligned}$$

چون E هرمیتی است داریم:

$$E = \begin{bmatrix} a & b+ci \\ b-ci & d \end{bmatrix}$$

که در آن $a, b, c, d \in \mathbb{R}$. طبق تمرین ۳۳ جلسه ششم $E \geq 0$ معادل این است که $a \geq 0$ و $\det E \geq 0$ یا

$$\begin{aligned} a &\geq 0 \\ ad &\geq b^2 + c^2, \end{aligned}$$

و $I - E \geq 0$ معادل است با اینکه

$$a \leq 1$$
$$(1-a)(1-d) \geq b^2 + c^2.$$

با جاگذاری $\langle\psi_1|$ و $\langle\psi_2|$ و ساده سازی داریم:

$$\langle\psi_1|E|\psi_1\rangle - \langle\psi_2|E|\psi_2\rangle = a - 2b - d.$$

پس باید مساله‌ی بهینه‌سازی زیر را حل کنیم:

$$\max a - 2b - d$$
$$\text{s.t.} \begin{cases} 0 \leq a \leq 1 \\ b^2 + c^2 \leq ad \\ b^2 + c^2 \leq (1-a)(1-d) \end{cases}$$

اما چون c در تابع ظاهر نشده است و در سمت چپ نامساوی‌ها ظاهر شده است، می‌توان مشاهده کرد که مساله‌ی بالا معادل است با

$$\max a - 2b - d$$
$$\text{s.t.} \begin{cases} 0 \leq a \leq 1 \\ b^2 \leq ad \\ b^2 \leq (1-a)(1-d) \end{cases} \tag{۶}$$

با ساده کردن دو عبارت $b^2 \leq ad$ و $b^2 \leq (1-a)(1-d)$ داریم

$$\frac{b^2}{a} \leq d \leq 1 - \frac{b^2}{1-a}.$$

بنابراین باید داشته باشیم

$$\frac{b^2}{a} \leq 1 - \frac{b^2}{1-a},$$

و یا $-\sqrt{a(1-a)} \leq b \leq \sqrt{a(1-a)}$. چون d با علامت مثبت در تابع ظاهر شده باید مقدار مینیمم خود یعنی b^2/a را اتخاذ کند پس (۶) تبدیل می‌شود به

$$\max_{\substack{0 \leq a \leq 1 \\ |b| \leq \sqrt{a(1-a)}}} a - 2b - \frac{b^2}{a}.$$

برای a ثابت، مشتق تابع $2b + b^2/a$ در $b = -a$ صفر می‌شود که وقتی قابل قبول است که $a \leq \sqrt{a(1-a)}$ و یا معادلا $a \leq 1/2$. به ازای این مقدار، مقدار تابع می‌شود $2a$ که در ماکسیمم آن به شرط $a \leq 1/2$ در $a = 1/2$ و برابر 1 است. حال نقاط مرزی را بررسی می‌کنیم. اگر b را برابر نقطه‌ی انتهایی بازه بگذاریم حداکثر به مقدار

$$a + 2\sqrt{a(1-a)} - (1-a)$$

می‌رسیم که در $a=\frac{1}{4}(2+\sqrt{2})$ ماکسیمم می‌شود و مقدار آن $\sqrt{2}$ است که می‌بینیم از ماکسیمم نقاط با مشتق صفر بیشتر است بنابراین با جاگذاری در مساله‌ی اصلی داریم

$$p_{max}=\frac{1+\sqrt{2}}{2},$$

که به ازای

$$E=\left[\begin{array}{cc}\frac{1}{4}(2+\sqrt{2}) & \frac{-1}{2\sqrt{2}}\\ \frac{-1}{2\sqrt{2}} & \frac{1}{4}(2-\sqrt{2})\end{array}\right],$$

بدست می‌آید.

تمرین ۷ ابتدا فرض کنید احتمال خطا صفر شده است، بنابراین عملگرهای POVM $E_1,\dots E_k$ پیدا شده اند که

$$\frac{1}{k}\sum\langle\psi_i|E_i|\psi_i\rangle=1. \qquad (۷)$$

اما $\langle\psi_i|E_i|\psi_i\rangle$ احتمال این است که نتیجه‌ی آزمایش i باشد در صورتی که حالت سیستم $|\psi_i\rangle$ باشد، بنابراین $\langle\psi_i|E_i|\psi_i\rangle\leq 1$. این موضوع در کنار معادله‌ی (۷) نتیجه می‌دهد که

$$\langle\psi_i|E_i|\psi_i\rangle=1 \qquad 1\leq i\leq k.$$

حال توجه کنید که

$$1=\langle\psi_i||\psi_i\rangle=\langle\psi_i|I|\psi_i\rangle=\langle\psi_i|\left(\sum E_j\right)|\psi_i\rangle=1+\sum_{j\neq i}\langle\psi_i|E_j|\psi_i\rangle, \qquad (۸)$$

اما $\langle\psi_i|E_j|\psi_i\rangle\geq 0$ بنابراین معادله‌ی بالا نتیجه می‌دهد

$$\langle\psi_i|E_j|\psi_i\rangle=0 \qquad i\neq j,$$

و در نتیجه طبق $E_j\geq 0$ داریم:

$$E_j|\psi_i\rangle=0 \quad i\neq j.$$

حال برای $i\neq j$ داریم

$$\langle\psi_i|\psi_j\rangle=\langle\psi_i|I|\psi_j\rangle=\sum_k\langle\psi_i|E_k|\psi_j\rangle=0$$

چراکه در عبارت بالا یا $k\neq j$ که در آن صورت $E_k|\psi_j\rangle=0$ و یا $k\neq i$ که در آن صورت $\langle\psi_j|E_k=(E_k|\psi_j\rangle)^\dagger=0$.
بنابراین اگر بتوان با احتمال یک کدگشایی کرد باید $|\psi_i\rangle$ها بر هم عمود باشند.

اگر فرض کنیم $|\psi_i\rangle$ها بر هم عمود باشند نیز کافی است عملگرهای تصویری روی آنها را در نظر بگیرید، یعنی

$$E_i=|\psi_i\rangle\langle\psi_i| \qquad 1\leq i\leq k$$

$$E_{k+1}=I-\sum_{i=1}^{k}E_i$$

در این صورت

$$\frac{1}{k}\sum_{i=1}^{k}\langle\psi_i|E_i|\psi_i\rangle = \frac{1}{k}\sum\langle\psi_i||\psi_i\rangle\langle\psi_i||\psi_i\rangle = 1,$$

و احتمال کدگشایی درست یک است.