نظریه اطلاعات کوانتمی ۱ ترم پاییز ۱۳۹۱-۱۳۹۲

مدرسین: ابوالفتح بیگی و امین‌زاده گوهری نویسنده: مجید محزون

جلسه ۱۱

در دو جلسه قبل اصول مکانیک کوانتمی را بررسی کردیم:

1- **فضای حالات:**

متناظر با هر سیستم فیزیکی یک فضای هیلبرت (فضای با ضرب داخلی) وجود دارد. حالات سیستم بردارهایی به طول یک هستند. همچنین دیدیم که اگر یک بردار واحد در یک فاز ضرب شود حالت سیستم عوض نمی‌شود، بنابراین تناظر بین حالات و بردارهای به طول یک، یک به یک نمی‌باشد.

2- **اندازه‌گیری:**

اندازه‌گیری متناظر با تعدادی عملگر خطی $\{M_1, ..., M_k\}$ روی همان فضای هیلبرت می‌باشد که در شرط کامل بودن [۱] یعنی $\sum_{i=1}^{k} M_i^\dagger M_i = I$ صدق می‌کنند. اگر حالت سیستم $|\psi\rangle$ باشد و یک اندازه‌گیری انجام دهیم، متناظر با این اندازه‌گیری یک توزیع احتمال خواهیم داشت. احتمال این که حاصل اندازه‌گیری i باشد برابر است با:

$$P(i) = \langle\psi|M_i^\dagger M_i|\psi\rangle.$$

همچنین اگر حاصل اندازه‌گیری i باشد، سیستم به حالت زیر سقوط [۲] می‌کند:

$$\frac{M_i|\psi\rangle}{\|M_i|\psi\rangle\|}.$$

3- **تحول زمانی:**

تحول زمانی متناظر با عملگرهای یکانی است. اگر حالت سیستم $|\psi\rangle$ باشد، پس از تحول زمانی حالت آن $U|\psi\rangle$ خواهد بود (که این معادل با معادله شرودینگر است). چون عملگرهای یکانی عملگرهایی هستند که طول را حفظ می‌کنند، $U|\psi\rangle$ دارای طول یک و در نتیجه یک حالت مجاز خواهد بود.

4- **سیستم‌های ترکیبی :**

اگر دو سیستم A و B داشته باشیم و فضای هیلبرت متناظر با آن‌ها به ترتیب $\mathcal{H}_A$ و $\mathcal{H}_B$ باشد، فضای هیلبرت سیستم ترکیبی AB برابراست با $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. اگر سیستم A در حالت $|\psi_1\rangle$ و سیستم B در حالت $|\psi_2\rangle$ باشد، سیستم ترکیبی AB در حالت $|\psi_1\rangle \otimes |\psi_2\rangle$ خواهد بود. چنین حالاتی را جدایی پذیر [۳] می‌نامیم. توجه کنید که

---

[۱] Completeness
[۲] Collapse
[۳] Seperable, Product State

هر بردار دلخواه در فضای هیلبرت سیستم ترکیبی AB را همیشه نمی‌توان به صورت ضرب تانسوری دو بردار در فضای هیلبرت سیستم‌های A و B نوشت. چنین حالاتی را درهم‌تنیده[۴] می‌نامیم. به عنوان مثال:

$$\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B+|1\rangle_A|1\rangle_B)\neq|\psi_1\rangle_A\otimes|\psi_2\rangle_B.$$

هر حالت دلخواه در سیستم AB یا جدایی‌پذیر است و یا در هم تنیده.

مثال ۱ فرض کنید آلیس می‌خواهد یک پیام بین 1 تا k را برای باب ارسال کند. به آلیس اجازه داده شده که یک سیستم کوانتمی را برای باب ارسال کند. آلیس برای این کار پیام $i, 1\leq i\leq k$ را در حالت کوانتمی $|\psi_i\rangle$ کد میکند و سیستم کوانتمی را برای باب ارسال می‌کند. باب پس از دریافت سیستم کوانتمی یک اندازه‌گیری روی آن انجام می‌دهد تا با استفاده از نتیجه آن حدس بزند که آلیس چه پیامی برایش ارسال کرده است. بدست آوردن اندازه‌گیری بهینه مساله مهمی است اما فعلا یک حالت خاص را در نظر میگیریم: فرض کنید $|\psi_i\rangle, 1\leq i\leq k$ها دو به دو بر هم عمود باشند. بنابراین می توان $\{|\psi_1\rangle,...,|\psi_k\rangle\}$ را به یک پایه متعامد یکه برای کل فضا، $\{|\psi_1\rangle,...,|\psi_l\rangle\}$، گسترش داد. حال اندازه‌گیری در این پایه را در نظر بگیرید. عملگرهای اندازه‌گیری عبارتند از:

$$M_j=|\psi_j\rangle\langle\psi_j|.$$

در این صورت اگر حالت سیستم i باشد احتمال این‌که حاصل اندازه‌گیری j باشد (احتمال کدگشایی j به شرط اینکه پیام i باشد) عبارتست از:

$$\langle\psi_i|M_j^\dagger M_j|\psi_i\rangle=|\langle\psi_i|\psi_j\rangle|^2=\delta_{ij}$$

که در آن

$$\delta_{ij}=\begin{cases}0, & i\neq j\\ 1, & i=j\end{cases}$$

مشاهده می‌کنیم که در گیرنده با احتمال یک کدگشایی بدون خطا صورت می‌گیرد. نتیجه این بحث به طور خلاصه این است که اگر بردارهایی که پیام را در آن ها کد می‌کنیم دو به دو بر هم عمود باشند، می‌توانیم با احتمال یک کدگشایی بدون خطا انجام دهیم.

علیرغم ظاهر ساده چهار اصل مکانیک کوانتمی، نتایج عجیبی از آنها قابل استخراج است. در زیر به دو پروتکل جالب کوانتمی بنام‌های کدگذاری فوق چگال و فرابرد می‌پردازیم. اما قبل از بیان این پروتکل ها نیاز به نمادگذاری زیر داریم:

تعریف ۲ چهار بردار زیر در فضای تانسوری دو کیوبیت را در نظر بگیرید:

$$|\Phi^+\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle),\quad |\Psi^+\rangle=\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle),$$

$$|\Phi^-\rangle=\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle),\quad |\Psi^-\rangle=\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle).$$

[۴] Entangled

این چهار بردار دو به دو بر هم عمودند و یک پایه متعامد یکه برای فضای دو کیوبیت تشکیل می‌دهند. به این پایه، پایه بل [۵] گفته میشود.

دو بردار Φ^+ و Ψ^- به هم عمودند زیرا

$$\begin{aligned}
\langle\Phi^+|\Psi^-\rangle &= \frac{1}{2}(\langle 00| + \langle 11|)(|01\rangle - |10\rangle) \\
&= \frac{1}{2}\big(\langle 00|01\rangle - \langle 00|10\rangle + \langle 11|01\rangle - \langle 11|10\rangle\big) \\
&= \frac{1}{2}\big(\langle 0|0\rangle\cdot\langle 0|1\rangle - \langle 0|1\rangle\cdot\langle 0|0\rangle + \langle 1|0\rangle\cdot\langle 1|1\rangle - \langle 1|1\rangle\cdot\langle 1|0\rangle\big) \\
&= \frac{1}{2}\big(1\cdot 0 - 0\cdot 1 + 0\cdot 1 - 1\cdot 0\big) \\
&= 0.
\end{aligned}$$

ادامه بررسی اینکه پایه بل یک پایه متعامد یکه برای فضای دو کیوبیت تشکیل می‌دهد را به عنوان تمرین به خواننده واگذار می‌کنیم.

۱ کدگذاری فوق چگال

کدگذاری فوق چگال [۶] جز اولین پروتکل‌های کوانتمی بوده است. فرض کنید آلیس می‌خواهد دو بیت اطلاعات کلاسیک را برای باب بفرستد اما بین آلیس و باب فقط یک کانال برای انتقال اطلاعات کوانتمی (ارسال کیوبیت) وجود دارد. کدگذاری فوق چگال نشان می‌دهد که ارسال دو بیت از آلیس به باب با فرستادن فقط یک کیوبیت امکان پذیر است. یعنی با فرستادن یک کیوبیت از سمت آلیس به باب می‌توان دو بیت اطلاعات کلاسیک را انتقال داد ولی با این شرط که بین آلیس و باب درهم تنیدگی به اشتراک گذاشته شده باشد. فرض کنید دو کیوبیت A و B در حالت درهم‌تنیده $|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}$ قرار داشته باشند و کیوبیت اول در اختیار آلیس و کیوبیت دوم در اختیار باب قرار داشته باشد. (در واقع آلیس و باب دو کیوبیت A و B را در این حالت خاص با هم تقسیم [۷] می‌کنند به این معنی که این دو کیوبیت همزمان با هم در آزمایشگاه تولید شده‌اند، سپس آلیس یک کیوبیت را برداشته و با خود می‌برد، و باب یک کیوبیت دیگر را برداشته و با خودش می‌برد).

به بیان دیگر اگر حالت $|\Phi^+\rangle_{AB}$ که آلیس و باب از قبل تقسیم کرده بودند را یک واحد درهم‌تنیدگی یا ای-بیت [۸] بنامیم:

انتقال ۲ بیت کلاسیک $\Longrightarrow$ انتقال ۱ کیوبیت + ۱ ای-بیت

شرح پروتکل:

[۵] Bell basis
[۶] Superdense Coding (1992)
[۷] Share
[۸] Entanglement bit, ebit

فرض کنید دو کیوبیت A و B در حالت $|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}$ بین آلیس و باب تقسیم شده باشند و کیوبیت اول در اختیار آلیس و کیوبیت دوم در اختیار باب قرار داشته باشد. آلیس می‌خواهد پیام $m \in \{1,2,3,4\}$ را برای باب بفرستد. نمادگذاری زیر را در نظر بگیرید:

$$U_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I, \quad U_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad U_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad U_4 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

توجه کنید که این چهار عملگر یکانی هستند و در نتیجه متناظر با یک تحول زمانی، پس آلیس می‌تواند هر یک از آن‌ها را بر کیوبیت خود (A) اثر دهد. اگر پیام آلیس m باشد، آلیس U_m را روی کیوبیت خودش (A) اعمال می‌کند. اینکه آلیس یک تحول زمانی U_m روی کیوبیت خودش اعمال می‌کند معادل این است که تحول زمانی ($U_m^A \otimes I^B$) روی کل سیستم اعمال می‌شود، و در نتیجه حالت کل سیستم به $(U_m^A \otimes I^B)|\Phi^+\rangle_{AB}$ تغییر می‌کند. آلیس سپس کیوبیت A را برای باب می‌فرستد. حال باب دو کیوبیت در حالت $(U_m^A \otimes I^B)|\Phi^+\rangle_{AB}$ در اختیار دارد. بسته به اینکه مقدار m چه باشد مشاهده کنید که حاصل ($U_m^A \otimes I^B$) برابر با یکی از حالت‌های زیر (یکی از بردارهای پایه بل) می‌شود:

$$(U_1 \otimes I)|\Phi^+\rangle = |\Phi^+\rangle, \quad (U_2 \otimes I)|\Phi^+\rangle = |\Phi^-\rangle,$$

$$(U_3 \otimes I)|\Phi^+\rangle = |\Psi^+\rangle, \quad (U_4 \otimes I)|\Phi^+\rangle = |\Psi^-\rangle.$$

مثلا جهت اثبات درستی رابطه اول داریم:

$$\begin{aligned}(U_1 \otimes I)|\Phi^+\rangle =& (I \otimes I)|\Phi^+\rangle \\ =& |\Phi^+\rangle\end{aligned}$$

جهت اثبات درستی رابطه دوم داریم:

$$\begin{aligned}(U_2 \otimes I)|\Phi^+\rangle &= \frac{1}{\sqrt{2}}(U_2 \otimes I)(|00\rangle + |11\rangle) \\ &= \frac{1}{\sqrt{2}}(U_2 \otimes I)|00\rangle + \frac{1}{\sqrt{2}}(U_2 \otimes I)|11\rangle \\ &= \frac{1}{\sqrt{2}}(U_2|0\rangle \otimes I|0\rangle) + \frac{1}{\sqrt{2}}(U_2|1\rangle \otimes I|1\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle) + \frac{1}{\sqrt{2}}(-|1\rangle \otimes |1\rangle) \\ &= \frac{1}{\sqrt{2}}(|00\rangle) + \frac{1}{\sqrt{2}}(-|11\rangle) \\ &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ &= |\Phi^-\rangle\end{aligned}$$

اثبات بقیه حالت‌ها مشابه بوده و به خواننده واگذار می‌شود.

باب در پایه متناظر با این چهار حالت (در پایه بل) روی دو کیوبیت اندازه‌گیری انجام می‌دهد. از آن‌جا که چهار حالت $(U_m^A \otimes I^B)|\Phi^+\rangle_{AB}$ برای مقادیر مختلف m بر هم عمودند طبق بحثی که در مثال ۱ داشتیم، باب می‌تواند بدون خطا تشخیص دهد که این دو کیوبیت در چه حالتی هستند و از آنجا می‌فهمد که آلیس کدام U_m را اثر داده است. پس باب از روی حاصل اندازه‌گیری‌اش می‌تواند m را بیابد.

ملاحظاتی در باب واجب الوجود و ممکن الوجود:

جهت فهم بهتر الگوریتم کدگذاری فوق چگال خوب است ببینیم که چه بخش هایی از الگوریتم واجب الوجود، و چه بخش هایی ممکن الوجود هستند. مثلا آیا انتخاب U_1، U_2، U_3 و U_4 باید حتما به همین شکلی که تعریف شده باشد یا انتخاب های دیگری هم ممکن است. آیا حالت تقسیم شده بین آلیس و باب باید حتما $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}$ باشد، یا حالات دیگری نیز ممکن است.

سؤال اول امتحان دوم جبر خطی را بیاد آورید:

> *فرض کنید $\{|v_0\rangle, |v_1\rangle, \ldots, |v_{n-1}\rangle\}$ یک پایه‌ی متعامد یکه برای $\mathcal{V}$ باشد و تعریف کنید*
>
> $$|\Psi\rangle = |v_0\rangle|v_0\rangle + |v_1\rangle|v_1\rangle + \cdots + |v_{n-1}\rangle|v_{n-1}\rangle.$$
>
> *نشان دهید برای هر $|\phi\rangle \in \mathcal{V} \otimes \mathcal{W}$ عملگر $T : \mathcal{V} \to \mathcal{W}$ وجود دارد به طوری که $|\phi\rangle = (I \otimes T)|\Psi\rangle$.همچنین نشان دهید که در این صورت $\||\phi\rangle\|^2 = \mathrm{tr}(T^\dagger T)$.*

پس اگر با حالت $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}$ شروع کنیم (که همان بردار $|00\rangle + |11\rangle$ صورت مساله با یک ضریب اضافه $\frac{1}{\sqrt{2}}$ است)، با اعمال یک عملگر T مناسب روی کیوبیت اول می‌توانیم حالت کل سیستم را به هر حالت دلخواه $|\phi\rangle$ تبدیل کنیم. اما باید تضمین کنیم که T یکانی باشد. اگر به راه حل دوم ارائه شده برای این سؤال نگاه کنیم می‌بینیم که T یکانی است (پایه متعامد یکه را به پایه متعامد یکه می‌برد) اگر و فقط اگر بردار $|\phi\rangle$ به شکل

$$|\phi\rangle = \frac{1}{\sqrt{2}}|0\rangle \otimes |w_0\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |w_1\rangle$$

برای یک پایه متعامد یکه $|w_0\rangle$ و $|w_1\rangle$ باشد. پس بصورت خلاصه، با اعمال عملگر یکانی مناسب روی کیوبیت A میتوان حالت سیستم را به شکل بالا برای هر پایه متعامد یکه دلخواه $|w_0\rangle$ و $|w_1\rangle$ برد. در کدگذاری فوق چگال که در بالا آمده است ما با استفاده از عملگر U_m حالت سیستم را به انتخاب های خاصی از $|w_0\rangle$ و $|w_1\rangle$ تغییر می‌دهیم:

$$m = 1 \rightarrow |w_0\rangle = |0\rangle, \quad |w_1\rangle = |1\rangle$$

$$m = 2 \rightarrow |w_0\rangle = |0\rangle, \quad |w_1\rangle = -|1\rangle$$

$$m = 3 \rightarrow |w_0\rangle = |1\rangle, \quad |w_1\rangle = |0\rangle$$

$$m = 4 \rightarrow |w_0\rangle = -|1\rangle, |w_1\rangle = |0\rangle$$

نکته مهمی که در مورد این انتخاب ها وجود دارد این است که منجر به یک پایه متعامد یکه (پایه بل) در فضای تانسوری می‌شوند. این تعامد باعث می‌شود که بتوانیم در این پایه اندازه گیری بدون خطا انجام دهیم. اما مشخصا می‌توان انتخاب‌های متفاوتی از $|w_0\rangle$ و $|w_1\rangle$ ها در حالات مختلف یافت که باز هم به بردارهای متعامد یکه منجر شوند. پس پایه بل یک ممکن الوجود است و نه یک واجب الوجود.

تمرین ۳ به نظر شما اینکه حالت تقسیم شده بین آلیس و باب $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}$ باشد ضروری است یا حالات دیگری هم ممکن است. اگر این امکان وجود دارد دقیقا با چه انتخاب‌هایی از تقسیم در هم‌تنیدگی می‌توان پروتکل را پس از اصلاحات اجرا کرد و به همان نتیجه نهایی ارسال دو بیت توسط یک کیوبیت رسید.

تمرین ۴ فرض کنید E یک عملگر مثبت دلخواه باشد که روی کیوبیت آلیس اثر می‌کند. نشان دهید اگر $|\psi\rangle$ هر یک از چهار بردار پایه بل باشد، مقدار $\langle\psi|E \otimes I|\psi\rangle$ یکسان است (مقدار این عبارت برای هر انتخاب از بردارهای پایه بل یکسان است). سپس فرض کنید در پروتکل کدگذاری فوق چگال فرد سوم شنودگری کیوبیت آلیس را در مسیر رسیدن به باب دریافت و در اختیار می‌گیرد. آیا شنودگر می تواند اطلاعاتی در مورد این‌که آلیس می‌خواهد کدام یک از چهار پیام $m = 1, 2, 3, 4$ را بفرستد، به دست بیاورد؟ اگر می‌تواند چگونه و اگر نمی‌تواند چرا؟

روشی برای ساختن دو کیوبیت در یک حالت درهم‌تنیده. فرض کنید دو کیوبیت A و B در اختیار داریم که هر دو در حالت $|0\rangle$ قرار دارند، یعنی حالت سیستم ترکیبی $|0\rangle|0\rangle$ است. اگر عملگر یکانی

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

را بر روی کیوبیت A اعمال کنیم، حالت سیستم ترکیبی

$$(H_A \otimes I_B)|0\rangle|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$

خواهد شد. حال عملگر

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

را روی کل سیستم (دو کیوبیت) اعمال می‌کنیم. اگر حالت کیوبیت اول $|0\rangle$ باشد، عملگر CNOT کاری انجام نمی‌دهد و اگر حالت کیوبیت اول $|1\rangle$ باشد، حالت کیوبیت دوم را تغییر می‌دهد. بنابراین در پایان حالت سیستم ترکیبی عبارتست از:

$$(CNOT)(H_A \otimes I_B)|0\rangle|0\rangle = (CNOT)\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

نکته. در اواخر درس خواهیم دید که اگر بین آلیس و باب درهم‌تنیدگی وجود نداشته باشد، با فرستادن یک کیوبیت حداکثر می‌توان یک بیت اطلاعات کلاسیک ارسال کرد.

۲ فرابرد یا طی العرض کوانتمی

پروتکل فرابرد یا طی العرض کوانتمی [۹] دقیقاً برعکس کدگذاری فوق چگال است و تنها یک سال پس از کدگذاری فوق چگال کشف شده است. فرض کنید دو کیوبیت A و B در حالت $|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}$ بین آلیس و باب تقسیم شده باشند و کیوبیت اول در اختیار آلیس و کیوبیت دوم در اختیار باب باشد. آلیس یک کیوبیت دیگر بنام C در اختیار دارد که از حالت آن مطلع نیست. یعنی کیوبیت C در حالت دلخواه $|v\rangle_C = \alpha|0\rangle_C + \beta|1\rangle_C$ قرار دارد اما آلیس از مقادیر α و β خبر ندارد و این مقادیر را نیز با اندازه گیری نمیتواند کشف کند زیرا نتایج اندازه گیری احتمالی خواهد بود و بعلاوه حالت کیوبیت C را تغییر میدهد. بنابراین در کل سه کیوبیت داریم که کیوبیت‌های C و A در اختیار آلیس و کیوبیت B در اختیار باب است.

هدف آلیس فرستادن کیوبیت C برای باب است اما بین آلیس و باب فقط یک کانال برای انتقال اطلاعات کلاسیک (مانند تلفن معمولی) وجود دارد. فرابرد نشان می‌دهد که این کار با فرستادن دو بیت کلاسیک امکان‌پذیر است! عنوان این پروتکل (فرابرد یا طی العرض) از آنجا آمده است که پس از انجام این الگوریتم کیوبیت C از سمت آلیس غیب می‌شود و یک نسخه یکسان از آن در سمت باب بوجود می‌آید، بدون اینکه کانال کوانتمی میان آلیس و باب وجود داشته باشد (فقط یک خط تلفن برای انتقال اطلاعات کلاسیک میان این دو وجود دارد).

شرح پروتکل:

دیدیم که $\{|\Phi_1\rangle, |\Phi_-\rangle, |\Psi_+\rangle, |\Psi_-\rangle\}$ یک پایه متعامد یکه برای فضای دو کیوبیت تشکیل می‌دهد. از طرفی $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ نیز یک پایه متعامد یکه برای این فضا تشکیل می‌دهد و می توان آن را بر حسب پایه دیگر به صورت زیر نوشت:

$$|00\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle + |\Phi^-\rangle), \quad |01\rangle = \frac{1}{\sqrt{2}}(|\Psi^+\rangle + |\Psi^-\rangle),$$
$$|11\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle - |\Phi^-\rangle), \quad |10\rangle = \frac{1}{\sqrt{2}}(|\Psi^+\rangle - |\Psi^-\rangle).$$

سیستم ترکیبی هر سه کیوبیت در حالت $|v\rangle_C \otimes |\Phi^+\rangle_{AB}$ است که اگرسیستم CA را در پایه بل بنویسیم، داریم:

$$\begin{aligned}
|v_C\rangle \otimes |\Phi^+\rangle_{AB} &= \frac{1}{\sqrt{2}}(\alpha|000\rangle_{CAB} + \alpha|011\rangle_{CAB} + \beta|100\rangle_{CAB} + \beta|111\rangle_{CAB}) \\
&= \frac{1}{\sqrt{2}}\Big[\alpha|00\rangle_{CA}|0\rangle_B + \alpha|01\rangle_{CA}|1\rangle_B + \beta|10\rangle_{CA}|0\rangle_B + \beta|11\rangle_{CA}|1\rangle_B\Big] \\
&= \frac{1}{2}\Big[\alpha\left(|\Phi^+\rangle + |\Phi^-\rangle\right)_{CA}|0\rangle_B + \alpha(|\Psi^+\rangle + |\Psi^-\rangle)_{CA}|1\rangle_B \\
&\quad + \beta(|\Psi^+\rangle - |\Psi^-\rangle)_{CA}|0\rangle_B + \beta(|\Phi^+\rangle - |\Phi^-\rangle)_{CA}|1\rangle_B\Big] \\
&= \frac{1}{2}\Big[|\Phi^+\rangle_{CA}(\alpha|0\rangle + \beta|1\rangle)_B + |\Phi^-\rangle_{CA}(\alpha|0\rangle - \beta|1\rangle)_B \\
&\quad + |\Psi^+\rangle_{CA}(\alpha|1\rangle + \beta|0\rangle)_B + |\Psi^-\rangle_{CA}(\alpha|1\rangle - \beta|0\rangle)_B\Big].
\end{aligned}$$

[۹] Teleportation (1993)

به عبارت دیگر:

$$|v\rangle_C\otimes|\Phi^+\rangle_{AB}=\frac{1}{2}\Big[|\Phi^+\rangle_{CA}\otimes U_1|v\rangle_B+|\Phi^-\rangle_{CA}\otimes U_2|v\rangle_B+|\Psi^+\rangle_{CA}\otimes U_3|v\rangle_B+|\Psi^-\rangle_{CA}\otimes U_4|v\rangle_B\Big].$$

پروتکل این طور شروع می‌شود که آلیس دو کیوبیتی که در اختیار دارد، یعنی سیستم CA را در پایه بل اندازه‌گیری می‌کند. حاصل اندازه‌گیری یکی از اعداد $m\in\{1,2,3,4\}$ می‌باشد. در این صورت عملگرهای اندازه‌گیری آلیس عبارتند از:

$$M_1=|\Phi^+\rangle\langle\Phi^+|,\quad M_2=|\Phi^-\rangle\langle\Phi^-|,$$
$$M_3=|\Psi^+\rangle\langle\Psi^+|,\quad M_4=|\Psi^-\rangle\langle\Psi^-|.$$

برای مثال اگر حاصل اندازه‌گیری آلیس 1 باشد، با توجه به محاسبات فوق، سیستم به حالت زیر سقوط می کند (ضریب ۲ برای نرمالیزه کردن به کار رفته است.):

$$2\left(M_1^{CA}\otimes I^B\right)|v\rangle_C\otimes|\Phi^+\rangle_{AB}=2\left(\frac{1}{2}|\Phi^+\rangle\langle\Phi^+|^{CA}\otimes I^B\right)|v\rangle_C\otimes|\Phi^+\rangle_{AB}=|\Phi^+\rangle_{CA}|v\rangle_B.$$

یعنی کیوبیت باب به حالت $|v\rangle$ تغییر پیدا می‌کند. در واقع بسته به حاصل اندازه‌گیری آلیس، کیوبیت باب به یکی از حالت‌های زیر سقوط می کند:

$$M_1\Longrightarrow U_1|v\rangle,\quad M_2\Longrightarrow U_2|v\rangle,$$
$$M_3\Longrightarrow U_3|v\rangle,\quad M_4\Longrightarrow U_4|v\rangle.$$

به عنوان تمرین درستی عبارات فوق را تحقیق کنید.

حال فرض کنید که آلیس بعد از انجام اندازه‌گیری، حاصل را با تلفن به باب گزارش دهد. در این صورت اگر حاصل اندازه گیری m باشد، باب با اعمال U_m روی کیوبیت خود $|v\rangle=\alpha|0\rangle+\beta|1\rangle$ را به دست می‌آورد. نکته مهمی که در این‌جا وجود دارد این است که ماتریس‌های U_m یکانی هستند و در نتیجه متناظر با یک تحول زمانی. لذا طبق اصول مکانیک کوانتمی اعمال آنها برای باب امکان‌پذیر است.

ملاحظات:

توجه کنید که در این پروتکل، اندازه‌گیری آلیس چهار حالت دارد، پس آلیس 2 بیت اطلاعات کلاسیک برای باب می‌فرستد. در واقع:

انتقال ۱ کیوبیت $\Longleftarrow$ انتقال ۲ بیت + ۱ ای-بیت

دو پروتکل فرابرد و کدگذاری فوق چگال دوگان یکدیگر هستند، یعنی اگر درهم تنیدگی وجود داشته باشد، ارسال یک کیوبیت معادل ارسال دو بیت است و بالعکس. برای مثال فرض کنید بخواهیم ظرفیت یک کانال را وقتی بینهایت درهم تنیدگی تقسیم شده وجود داشته باشد، محاسبه کنیم. در این صورت ظرفیت کلاسیک آن دو برابر ظرفیت کوانتمی آن است.

نکته. پروتکل کدگذاری فوق چگال بهینه است، یعنی با ارسال یک کیوبیت نمی‌توان بیش از دو بیت اطلاعات کلاسیک ارسال کرد (حتی اگر بینهایت درهم تنیدگی تقسیم ebit وجود داشته باشد). یک روش برای مشاهده این موضوع این است که اگر بتوان با ارسال یک کیوبیت بیش از دو بیت اطلاعات کلاسیک انتقال داد، با ترکیب کردن فرابرد و کدگذاری فوق چگال نشان داده می‌شود که برای ارسال یک کیوبیت می‌توان کمتر از یک کیوبیت ارسال کرد که این تناقض است. پس کدگذاری فوق چگال واقعا چگال است و هیچ فضایی را اسراف نمی‌کند!

تمرین ۵ تمرین ۳ در مورد پروتکل فرابرد تکرار کنید.

۳ پارادوکس اینشتین-پودولسکی-روزن و آزمایش بل

اتفاق عجیبی که در پروتکل فرابرد می‌افتد این است که آلیس یک اندازه‌گیری روی کیوبیت خود انجام می‌دهد و کیوبیت باب در همان لحظه و بصورت آنی سقوط می‌کند. اولین بار اینشتین و همکارانش، پودولسکی و روزن متوجه عجیب بودن پدیده سقوط در فرضیات مکانیک کوانتمی شدند و در سال ۱۹۳۵ مقاله‌ای[۱۰] منتشر و ادعا کردند که فرمول‌بندی مکانیک کوانتمی ناقص است و تئوری دیگری به جای آن ارایه دادند. شهود آن‌ها این بود که دنیایی که ما در آن زندگی می‌کنیم موضعی[۱۱] است و بنابراین نباید تأثیر کاری که در یک لحظه در جایی انجام می‌شود بلافاصله و در همان لحظه در جایی دیگر ظاهر شود. اما اینشتین و همکارانش باید برخی پدیده‌های تجربی کوانتومی را توضیح می‌دادند: مثلا اگر دو کیوبیت در حالت در هم تندیده $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}$ داشته باشیم و نتیجه مشاهده اولی 0 یا 1 باشد (که این دو با هرکدام با احتمال $\frac{1}{2}$ رخ میدهد)، نتیجه اندازه گیری کیوبیت دومی نیز همان خواهد بود. یعنی یک پیوند میان این دو کیوبیت که ظاهرا از هم خیلی دور هستند برقرار است. اینشتین و همکارانش در پاسخ به چالش مفهوم متغیرهای پنهان [۱۲] را ارائه دادند. متغیرهای پنهان متغیرهایی هستند که به صورت مستقیم قابل مشاهده نیستند اما وجود آنها بصورت غیرمستقیم توسط مشاهدات و یک الگوی ریاضی استنباط می‌شوند. طبق نظر اینشتین و همکارانش دنیایی که ما در آن زندگی می‌کنیم موضعی بوده اما میان سیستم‌های کوانتمی که در فاصله از هم قرار دارند متغیرهایی به اشتراک گذاشته شده که ما از مقدار آنها مطلع نیستیم، و تنها از طریق مشاهده می‌توانیم به مقادیر آنها پی ببریم. بنابراین تصادفی بودن اندازه‌گیری که در هنگام مشاهدات می‌بینیم در واقع نتیجه ظهور متغیرهای پنهان است. مثلا اگر دو کیوبیت در حالت در هم تندیده $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}$ داشته باشیم مثل این است که این دو کیوبیت زمانی که نزدیک هم بوده‌اند، یک بیت تصادفی را به اشتراک گذاشته‌اند (متغیر پنهان). زمانی که ما یکی از این کیوبیت‌ها را اندازه گیری می‌کنیم نتیجه همین بیت تصادفی به اشتراک گذاشته شده برای ما مشخص می‌شود. قطعا چون همین بیت در نزد کیوبیت دوم نیز نهفته است، اگراندازه‌گیری‌ای روی کیوبیت دوم انجام دهیم، باید به نتیجه یکسانی برسیم. پس در نظر اینشتین و همکارانش لزومی ندارد که صحبتی از مفهومی به نام در هم تنیدگی بکنیم. با بیت‌های تصادفی به اشتراک گذاشته شده می‌توان همه چیز را توجیه کرد.

[۱۰] A. Einstein, B. Podolsky, and N. Rosen, Can quantum-mechanical description of physical reality be considered complete.

[۱۱] Local

[۱۲] hidden variable

سال‌ها پس از انتشار مقاله اینشتین-پودولسکی-روزن، بل[۱۳] آزمایشی طراحی کرد تا درستی ادعای اینشتین را اثبات کند، اما این آزمایش نهایتا نتیجه معکوس داد و ثابت کرد که مدل متغیرهای پنهان اینشتین و همکارانش درست نیست. هر چند این آزمایش درستی فرضیات مکانیک کوانتمی را "اثبات" نمی‌کند، اما نشان می‌دهد که طبیعت موضعی نیست.

برای توضیح ایده‌ی بل از بازی CHSH استفاده می‌کنیم. این بازی دقیقا آن چیزی نیست که بل مطرح کرد، اما ایده اصلی آن را بیان می‌کند. این بازی بین دو نفر، آلیس و باب انجام می‌شود. فرد سومی به نام داور دو بیت $s \in \{0,1\}$ و $t \in \{0,1\}$ را به صورت کاملا تصادفی انتخاب می‌کند. s را برای آلیس و t را برای باب می‌فرستد و سپس از آلیس و باب می‌خواهد که هر کدام در پاسخ بیتی به او بازگردانند. حال آلیس و باب بدون داشتن ارتباط، هرکدام باید یک بیت به فرد سوم بدهند. این بیت‌های خروجی را $a \in \{0,1\}$ و $b \in \{0,1\}$ می‌نامیم. آلیس و باب برنده بازی خواهند بود اگر

$$a + b \overset{2}{\equiv} s \cdot t.$$

بازی CHSH در دنیای کلاسیک:

فرض کنید که آلیس و باب همواره خروجی‌های $a = b = 0$ را بدهند. توجه کنید که $s \cdot t$ با احتمال $\frac{3}{4}$ برابر 0 است. لذا با این استراتژی آن‌ها با احتمال $\frac{3}{4}$ برنده خواهند بود. بنابراین احتمال برد آن‌ها حداقل برابر $\frac{3}{4}$ است. به عنوان تمرین ثابت کنید که بهترین استراتژی برای آلیس و باب همین بوده و احتمال برد همان $\frac{3}{4}$ است.

حال اگر فرض کنیم که قبل از شروع بازی بیت های تصادفی به اشتراک گذاشته شده بین آلیس و باب وجود داشته باشند، آیا این بیت‌ها کمکی به افزایش احتمال برد آن‌ها می کند؟ جواب منفی است (همان‌طور که بیت های تصادفی به اشتراک گذاشته شده در مخابرات نقطه به نقطه کمکی نمی‌کند). برای اثبات فرض کنید بیت‌های تصادفی به اشتراک گذاشته شده به برد آن‌ها کمک کند. متغیر تصادفی متناظر با بیت های تصادفی به اشتراک گذاشته شده را با R نمایش می‌دهیم. آلیس و باب به ازای هر $R = r$ یک استراتژی دارند. در این صورت احتمال برد برابر است با:

$$\sum_r Pr(R = r) Pr(\text{برد} | R = r).$$

اگر این احتمال از $\frac{3}{4}$ بیشتر باشد آن‌گاه حداقل یکی از مقادیر $Pr(\text{برد}|R = r)$ (احتمال برد به شرط استراتژی r) بزرگ‌تر از $\frac{3}{4}$ است و آلیس و باب می‌توانند فرض کنند که بیت های تصادفی به اشتراک گذاشته شده وجود ندارد و با استرتژی متناظر با $R = r$ بازی کنند. بنابراین چون بدون بیت‌های تصادفی به اشتراک گذاشته شده به احتمال برد بیشتر از $\frac{3}{4}$ دست نمی‌یابیم، در صورت وجود آن نیز به احتمال برد بالاتر از $\frac{3}{4}$ دست نخواهیم یافت. در واقع انتخاب خروجی‌های $a = b = 0$ استراتژی بهینه است.

بازی CHSH در دنیای کوانتمی:

دیدیم که در دنیای کلاسیک احتمال برد برابر $\frac{3}{4}$ می‌باشد. در ادامه استراتژی کوانتمی را مطرح می‌کنیم و ثابت می‌کنیم که احتمال برد در دنیای کوانتمی بیشتر است. این استراتژی نتیجه می‌دهد بر خلاف تصور اینشتین و همکارانش مدل متغیرهای پنهان نمی‌تواند مکانیک کوانتمی را توضیح دهد زیرا دیدیم که متغیرهای پنهان نمی‌توانند احتمال برد در

[۱۳] J.S. Bell, On the Einstein-Poldolsky-Rosen paradox

دنیای کلاسیک با تغییر دهند و لی در دنیای کوانتمی استراتژی برد بهتری وجود دارد. بنابراین فیزیک کوانتمی چیزی فراتر از متغیر پنهان دارد.

فرض کنید آلیس و باب قبل از شروع بازی دو کیوبیت A و B که در حالت $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$ آماده‌سازی شده‌اند را با هم تقسیم کنند. پایه متعامد یکه P_θ را به صورت زیر در نظر بگیرید:

$$P_\theta = \{|v_0(\theta)\rangle, |v_1(\theta)\rangle\},$$

که در آن

$$|v_0(\theta)\rangle = \cos(\theta)|0\rangle + \sin(\theta)|1\rangle, \quad |v_1(\theta)\rangle = -\sin(\theta)|0\rangle + \cos(\theta)|1\rangle.$$

همچنین قرار دهید:

$$\alpha_0 = 0, \quad \alpha_1 = \frac{\pi}{4} \qquad \beta_0 = \frac{\pi}{8}, \quad \beta_1 = \frac{-\pi}{8}$$

استراتژی این است که آلیس کیوبیت A را در پایه P_{α_s} اندازه می‌گیرد و a را برابر حاصل این اندازه‌گیری قرار می‌دهد. باب هم کیوبیت B را در پایه‌ی P_{β_t} اندازه می‌گیرد و بیت b را برابر حاصل این اندازه‌گیری قرار می‌دهد. بنابراین عملگرهای اندازه‌گیری آلیس یا باب متناظر با ورودی‌های s و t عبارتند از:

$$M_0(\theta) = |v_0(\theta)\rangle\langle v_0(\theta)|, \quad M_1(\theta) = |v_1(\theta)\rangle\langle v_1(\theta)|.$$

در این صورت عملگرهای اندازه‌گیری روی کل سیستم متناظر با ورودی‌های s و t عبارتند از:

$$M_0(\alpha_s) \otimes M_0(\beta_t), \quad M_0(\alpha_s) \otimes M_1(\beta_t),$$

$$M_1(\alpha_s) \otimes M_0(\beta_t), \quad M_1(\alpha_s) \otimes M_1(\beta_t).$$

احتمال اینکه خروجی‌های آلیس و باب a و b باشند به شرط این که ورودی ها s و t باشند برابر است با:

$$\begin{aligned} P(a, b|s, t) &= \langle\Phi^+|M_a(\alpha_s) \otimes M_b(\beta_t)|\Phi^+\rangle \\ &= \frac{1}{2}\mathrm{tr}(M_a(\alpha_s)^\dagger M_b(\beta_t)) \\ &= \frac{1}{2}|\langle v_a(\alpha_s)|v_b(\beta_t)\rangle|^2, \end{aligned}$$

در اینجا از رابطه

$$\langle\Phi^+|M_a(\alpha_s) \otimes M_b(\beta_t)|\Phi^+\rangle = \frac{1}{2}\mathrm{tr}(M_a(\alpha_s)^T M_b(\beta_t))$$

استفاده کردیم که تحقیق درستی آن به عنوان تمرین به خواننده واگذار می‌شود.

اگر $a=b$ باشد، $P(a,b|s,t)$ برابر است با $\frac{1}{2}\cos^2(\alpha_s-\beta_t)$ و اگر $a\neq b$ باشد، برابراست با $\frac{1}{2}\sin^2(\alpha_s-\beta_t)$.
بنابراین احتمال برد با این استراتژی برابر است با:

$$\begin{aligned}
Pr(a+b=s.t) &= \sum_{s,t} Pr(s,t)Pr(a+b=s.t|s,t) \\
&= \sum_{s,t} \sum_{a,b:\ a+b\overset{2}{\equiv}s\cdot t} \frac{1}{4}P(a,b|s,t) \\
&= \sum_{s,t} \sum_{a,b:\ a+b\overset{2}{\equiv}s\cdot t} \frac{1}{8}|\langle v_a(\alpha_s)|v_b(\beta_t)\rangle|^2 \\
&= \cos^2(\frac{\pi}{8}) = \frac{1}{2}+\frac{1}{2\sqrt{2}} \approx 0.8535 > \frac{3}{4}.
\end{aligned}$$

پس با استراتژی کوانتمی فوق آلیس و باب می‌توانند با احتمال $\cos^2(\pi/8)$ برنده شوند. در واقع ثابت می‌شود که این استراتژی بهینه است و احتمال برد در دنیای کوانتمی نمی‌تواند بالاتر از این باشد.

نکته . این آزمایش درستی مکانیک کوانتمی را اثبات نمی‌کند بلکه نادرستی مکانیک کلاسیک را اثبات می‌کند.

تمرین ۶ آلیس، باب و چارلی را سه بازیکن جدا از هم در نظر بگیرید. آلیس بیت ورودی x، باب بیت ورودی y و چارلی بیت ورودی z را دریافت می‌کنند. ورودی‌ها در شرط $x\oplus y\oplus z=0$ صدق می‌کنند. هدف بازیکنان این است که به ترتیب خروجی‌های a، b و c را تولید کنند به طوری که $a\oplus b\oplus c=OR(x,y,z)$. به عبارت دیگر اگر $x=y=z=0$ باشد، مجموع خروجی‌ها در پیمانه 2 باید برابر صفر باشد و در غیر این صورت مجموع خروجی‌ها در پیمانه 2 باید برابر یک باشد.

(آ) نشان دهید که هر استراتژی غیرتصادفی کلاسیک حداقل در یکی از 4 ورودی ممکن منجر به باخت می‌شود.

(ب) نشان دهید که هر استراتژی تصادفی کلاسیک، تحت توزیع یکنواخت روی چهار ورودی مجاز، دارای احتمال برد حداکثر $\frac{3}{4}$ می‌باشد.

(ج) فرض کنید بازیکنان سه کیوبیت در حالت درهم‌تنیده

$$\frac{1}{2}(|000\rangle-|011\rangle-|101\rangle-|110\rangle)$$

را با هم تقسیم می‌کنند. فرض کنید هر بازیکن به صورت زیر عمل می‌کند: اگر بیت ورودی‌اش 1 باشد، عملگر H (که در بالا معرفی شد) را بر کیوبیت خود اعمال می‌کند و در غیر این صورت کاری انجام نمی‌دهد. حالت سه کیوبیتی حاصل را بر حسب بیت‌های ورودی x,y,z توصیف کنید.

(د) با استفاده از قسمت (ج)، یک استراتژی کوانتمی ارائه دهید که برای هر ورودی ممکن بازی فوق را با احتمال یک ببرد.