مدرسین: ابوالفتح بیگی و امین‌زاده گوهری
نویسنده: مرتضی نوشاد

جلسه ۲۸

۱ تقطیر و ترقیق درهم تنیدگی

فرض کنید که m نسخه مستقل یک حالت محض دلخواه $|\psi\rangle_{AB}^{\otimes m}$ بین آذر و بابک به اشتراک گذاشته شده است. آذر و بابک با استفاده از یک سری تبدیلات می‌خواهند این m نسخه را به حالت‌های درهم تنیده بیشینه (حالت‌های بل) تبدیل کنند. اصطلاحا به این عملیات تقطیر درهم تنیدگی[۱] می‌گویند. به بیان دقیق‌تر، آذر و بابک باید بوسیله انجام عملگرهای محلی و مخابرات کلاسیک LOCC [۲] حالت $|\psi\rangle_{AB}^{\otimes m}$ را (بصورت تقریبی) تبدیل به n کپی از حالت‌های بل کنند (بطوری که وفاداری بین حالات تولید شده و حالات بل مطلوب زیاد باشد، و یا معادلا فاصله اثر میان آنها کم باشد). به مقدار $\frac{n}{m}$ نرخ تقطیر می‌گویند. هدف یافتن مقدار بیشینه نرخ تقطیر است زمانی که m به سمت بینهایت برود. در اینجا هیچ گونه محدودیتی روی میزان مخابرات کلاسیک وجود ندارد.

اما حالت برعکس تقطیر نیز قابل تعریف است. فرض کنیم که یک تعداد کپی از حالت‌های بل را داشته باشیم و می خواهیم آنها را با عملیات LOCC تبدیل به حالت دلخواه $|\psi\rangle_{AB}^{\otimes}$ کنیم. به این عمل ترقیق درهم تنیدگی[۳] یا درهم تنیدگی تشکیل [۴] $|\psi\rangle$ گفته می‌شود. بصورت دقیق‌تر فرض کنیم که n کپی از حالت بل در اختیار داشته باشیم و از ما خواسته شده که با عملیات LOCC به مقدار هر چه بیشتر کپی‌هایی از $|\psi\rangle$ تولید کنیم. حال اگر مقدار کپی‌های تولید شده از این حالت را نیز m در نظر بگیریم، نسبت $\frac{n}{m}$ هنگامی که n به سمت بینهایت میل کند را نرخ درهم تنیدگی تشکیل می‌گوییم.

فرض کنید که تجزیه اشمیت $|\psi\rangle$ به صورت زیر باشد:

$$|\psi\rangle = \sum_x \sqrt{p(x)}|x_A\rangle|x_B\rangle$$

که در آن ضرایب اشمیت را بصورت $\sqrt{p(x)}$ نشان داده‌ایم؛ $|x_A\rangle$ یک پایه متعامد یکه برای فضای هیلبرت سیستم A و $|x_B\rangle$ یک پایه متعامد یکه برای فضای هیلبرت سیستم B است که لزوما ارتباط خاصی با هم ندارند. اگر اثر جزئی نسبت به سیستم B را محاسبه کنیم خواهیم داشت:

$$\rho_\psi^A = \mathrm{tr}_B(|\psi\rangle\langle\psi|) = \sum_x p(x)|x_A\rangle\langle x_A|$$

[۱] Entanglement Distillation
[۲] Local Operations and Classical Communication
[۳] Entanglement Dilution
[۴] Entanglement of Formation

نشان خواهیم داد که تقطیر بر هم نهی در صورتی امکان دارد که نرخ تقطیر حداکثر

$$\frac{n}{m} < H(\{p(x)\}) = H(\rho_\psi^A),$$

و ترقیق برهم نهی زمانی ممکن است وقتی که نرخ ترقیق حداقل

$$\frac{n}{m} > H(\{p(x)\}) = H(\rho_\psi^A),$$

باشند. این دو نتیجه به این معنی هستند که $H(\rho_\psi^A)$ بیانگر میزان درهم‌تنیدگی بر حسب کیوبیت حالت $|\psi\rangle_{AB}$ است. با استفاده از این دو نتیجه می‌توان قضیه زیر را ثابت کرد:

قضیه ۱ برای نرخ داده شده R و $\epsilon > 0$ به دلخواه کوچک، m به اندازه کافی بزرگ وجود دارد بطوریکه m نسخه از حالت دوبخشی $|\psi\rangle$ را بتوان با عملیات *LOCC* به $m(R-\epsilon)$ نسخه از یک حالت محض دیگری مثل $|\phi\rangle$ تبدیل کرد اگر و فقط اگر

$$R \geq \frac{H(\rho_\phi^A)}{H(\rho_\psi^A)}.$$

که درآن ρ_ϕ^A از اثر جزئی‌گیری حالت $|\phi\rangle$ بدست می‌آید؛ ρ_ψ^A بصورت مشابه تعریف می‌شود.

نکته ۲ توجه کنید که قضیه بالا در مورد تبدیل حالات محض به حالات محض است. در صورتی که حالات غیر محض باشند، مساله حل نشده است. بصورت خاص نشان داده شده که برای یک حالت غیر محض ممکن است که نرخ درهم‌تنیدگی تشکیل مثبت باشد، اما نرخ در هم‌تنیدگی تقطیر صفر باشد!

۱.۱ تبدیل تنها یک نسخه از حالت محض به حالت محض دیگر

حال فرض کنید که بجای اینکه نسخه‌های زیادی از یک حالت محض را داشته باشیم، تنها یک نسخه داشته باشیم. در این صورت شرط لازم و کافی برای تبدیل یک حالت به حالت دیگر در قضیه زیر آمده است:

قضیه ۳ یک حالت دوبخشی $|\psi\rangle$ می‌تواند تحت عملیات *LOCC* به حالت محض دیگری مثل $|\phi\rangle$ تبدیل شود اگر و فقط اگر دنباله مقادیر ویژه‌ی ρ_ϕ بر دنباله مقادیر ویژه ρ_ψ غلبه کند: $\lambda_{\rho_\psi} \preceq \lambda_{\rho_\phi}$.

می‌گوییم که یک دنباله بر یک دنباله دیگر غلبه[۵] می‌کند اگر پس از مرتب کردن دو دنباله بصورت نزولی، برای هر k جمع k جمله‌ی اول دنباله اول بزرگتر مساوی جمع k جمله‌ی اول دنباله دوم باشد، و بعلاوه جمع تمامی اعضای دو دنباله با هم مساوی باشند.

مثال ۴ حالت محض $|0^A0^B\rangle$ همواره و بدون دسترسی به هیچ منبعی با عملیات *LOCC* قابل ساختن است زیرا کافی است که آذر و بابک هر دو حالت $|0\rangle$ را تولید کنند. این موضوع با قضیه بالا سازگار است زیرا دنباله مقادیر ویژه‌ی متناظر با این حالت برابر $(1, 0, 0, \cdots, 0)$ است که بر هر دنباله مقادیر ویژه‌ی دیگری غلبه می‌کند.

[۵] Majorize

مثال ۵ اگر آذر و بابک یک حالت بل را به اشتراک گذاشته باشند، هر حالت دلخواه محض روی یک کیوبیت سمت آذر و یک کیوبیت سمت بابک را می‌توانند بسازند زیرا دنباله مقادیر ویژه‌ی متناظر با حالت بل برابر $(\frac{1}{2}, \frac{1}{2})$ است که هر دنباله دوتایی دیگری به فرم $(a, 1-a)$ بر آن غلبه می‌کند.

۲ ترقیق درهم تنیدگی

ابتدا می‌خواهیم یک پروتکل ساده برای ترقیق درهم تنیدگی ارائه دهیم. برای m کپی از $|\psi\rangle$ می‌توان نوشت:

$$|\psi\rangle^{\otimes m} = \sum_{x_1, x_2, \cdots, x_m} \sqrt{p(x_1)p(x_2)\cdots p(x_m)} |x_{1A}, x_{2A}, \cdots, x_{mA}\rangle |x_{1B}, x_{2B}, \cdots, x_{mB}\rangle.$$

حالت جدید $|\phi_m\rangle$ را به صورت زیر تعریف می‌کنیم:

$$|\phi_m\rangle = \sum_{\epsilon-typical\ (x_1, \cdots, x_m)} \sqrt{p(x_1)p(x_2)\cdots p(x_m)} |x_{1A}, x_{2A}, \cdots, x_{mA}\rangle |x_{1B}, x_{2B}, \cdots, x_{mB}\rangle.$$

برای این که برداری با طول واحد داشته باشیم تعریف می‌کنیم $|\phi'_m\rangle \equiv \frac{|\phi_m\rangle}{\sqrt{\langle\phi_m|\phi_m\rangle}}$. اما با توجه به قضایای زیرفضاهای نوعی خواهیم داشت: $\||\psi\rangle^{\otimes m} - |\phi'_m\rangle\|_{\text{tr}} \to 0$ اگر m به سمت بینهایت میل کند. همچنین تعداد جملات در این مجموع حداکثر برابر $2^{m(H(\{p(x)\})+\epsilon)} = 2^{m(H(\rho_\psi^A)+\epsilon)}$ است.

حال فرض کنیم که آذر و بابک $n = m(H(\rho_\psi^A) + \epsilon)$ حالت بل را به اشتراک گذاشته باشند. برای تولید (تقریبی) $|\psi\rangle^{\otimes m}$ پروتکل به این صورت می‌باشد که آذر بصورت محلی هر دو قسمت $|\phi'_m\rangle$ را آماده کرده و سپس با استفاده از حالت‌های بل که با بابک به اشتراک دارد قسمت دوم $|\phi'_m\rangle$ را به بابک فرابرد[۶] می‌کند. بدین ترتیب آذر و بابک می‌توانند n حالت بل خود را به حالت $|\phi'_m\rangle$ ترقیق کنند. در این فرایند ترقیق نسبت $\frac{n}{m}$ به $H(\rho_\psi) + \epsilon$ میل می‌کند. با کوچک گرفتن ϵ می‌توان نتیجه گرفت که $H(\rho_\psi)$ یک کران بالا برای درهم‌تنیدگی تشکیل برای حالت $|\psi\rangle$ می‌باشد.

۳ تقطیر درهم‌تنیدگی

فرض کنیم که آذر و بابک m کپی از $|\psi\rangle$ را به اشتراک داشته باشند. ادعا می‌کنیم که آذر با انجام یک اندازه‌گیری محلی تصویری به زیر فضای ϵ-نوعی از ρ_ψ^A می‌تواند حالت مشترک $|\psi\rangle^{\otimes m}$ را به حالت $|\phi'_m\rangle$ تبدیل کند.

تمرین ۶ ادعای بالا را ثابت کنید.

بزرگترین ضریب اشمیتی که در تجزیه $|\phi_m\rangle$ ظاهر می شود حداکثر برابر $2^{-m(H(\rho_\psi)-\epsilon)}$ است (با توجه به نوعی بودن). همچنین بزرگترین مقدار ویژه حالت نرمال شده $|\phi'_m\rangle$ برابر $\frac{1}{1-\delta}2^{-m(H(\rho_\psi)-\epsilon)}$ خواهد بود. حال فرض کنیم که n طوری انتخاب شود که در نامساوی زیر صدق کند:

$$\frac{1}{1-\delta}2^{-m(H(\rho_\psi)-\epsilon)} \leq 2^{-n}.$$

[۶] Teleport

در این صورت بردار مقادیر ویژه‌ی $\rho_{\phi'_m}$ به ازای تک تک عناصر کمتر از 2^{-n} خواهد بود.

برداری به شکل $(2^{-n}, 2^{-n}, \cdots, 2^{-n}, 0, 0, \cdots, 0)$ در نظر بگیرید که تعداد صفرهای اضافه شده در انتها برای این است که طول این بردار برابر تعداد مقادیر ویژه $\rho_{\phi'_m}$ بشود. این بردار متناظر با مقادیر ویژه n نسخه از حالت‌های بل می‌باشد. ادعا می‌کنیم که دنباله مقادیر ویژه $\rho_{\phi'_m}$ بر دنباله مقادیر ویژه $(2^{-n}, 2^{-n}, \cdots, 2^{-n}, 0, 0, \cdots, 0)$ غلبه می‌کند. در اینجا صفرهای آخر برای این اضافه شده‌اند که طول این بردار با تعداد مقادیر ویژه $\rho_{\phi'_m}$ برابر شود و در نتیجه دو دنباله قابل مقایسه باشند. دلیل این غلبه کردن این است که جمع k مقادیر ویژه بزرگ، حداکثر $\frac{k}{2^n}$ است زیرا هرکدام از آنها حداکثر $\frac{1}{2^n}$ است. طبق قضیه ۳ حالت $|\phi'_m\rangle$ می تواند تحت عملیات LOCC به n نسخه از حالت‌های بل تبدیل شود. بنابراین می‌توان نتیجه گرفت که درهم‌تنیدگی قابل تقطیر حداقل برابر $H(\rho_\psi)$ است.

نکته ۷ در جلسات قبل دیدیم که هر دنباله‌ای بر دنباله توزیع یکنواخت غلبه می‌کند. در نگاه اول ممکن است به نظر برسد که دنباله مقادیر ویژه $\rho_{\phi'_m}$ باید بر دنباله $(2^{-n}, 2^{-n}, \cdots, 2^{-n}, 0, 0, \cdots, 0)$ غلبه کند چون این دنباله نزدیک توزیع یکنواخت است. اما از آنجایی که دنباله $(2^{-n}, 2^{-n}, \cdots, 2^{-n}, 0, 0, \cdots, 0)$ حاوی تعدادی صفر است، از یکنواخت بودن خارج شده و تناقضی وجود ندارد.

۴ عملگرهای محلی و مخابرات کلاسیک

هدف این بخش فهمیدن بهتر تغییر حالاتی است که از طریق عملگرهای محلی و مخابرات کلاسیک LOCC حاصل می‌شود. ابتدا با یک قضیه شروع می‌کنیم. این قضیه بیان می‌دارد که اندازه‌گیری در سمت بابک معادل یک اندازه‌گیری در سمت آذر و یک تحول یکانی در سمت بابک است. نتیجه استفاده متوالی از این قضیه این است که تمامی اندازه‌گیری‌هایی که در سمت بابک انجام می‌شود را می‌توان به سمت آذر منتقل کرد و معادل آنها یک تحول یکانی در سمت بابک قرار داد.

قضیه ۸ فرض کنید که یک حالت محض $|\psi^{AB}\rangle$ میان آذر و بابک به اشتراک گذاشته شده باشد. یک اندازه‌گیری دلخواه $\{M_j\}$ سمت بابک را در نظر بگیرید. حاصل اندازه‌گیری با احتمال

$$p_j = \|(I \otimes M_i)|\psi^{AB}\rangle\|^2$$

برابر j بوده و در صورت مشاهده j حالت مشترک سیستم به حالت محض

$$|\psi_j\rangle = \frac{1}{\sqrt{p_j}}(I \otimes M_i)|\psi^{AB}\rangle$$

سقوط می‌کند. در این صورت اندازه‌گیری N_j در سمت آذر و عملگر یکانی W_j روی سیستم بابک وجود دارند به طوری که اگر ابتدا آذر با استفاده از N_j سیستمش را اندازه‌گیری کند، احتمال مشاهده j همان p_j بوده، و در صورتی که پس از اندازه‌گیری آذر، بابک عملگر W_j را روی سیستمش اعمال کند، حالت مشترک سیستم به همان حالت محض $|\psi_j\rangle$ تغییر کند. به عبارت دیگر اندازه‌گیری در سمت بابک معادل اندازه‌گیری در سمت آذر به همراه یک تحول زمانی در سمت بابک است.

اثبات: توجه کنید که با نشاندن فضاهای $\mathcal{H}_A$ و $\mathcal{H}_B$ در فضاهای با بعد بزرگتر بدون کاسته شدن از کلیت مسأله می‌توانیم فرض کنیم که $\dim \mathcal{H}_A = \dim \mathcal{H}_B$. به همین ترتیب بدون کاسته شدن از کلیت مسأله می‌توان فرض کرد که عملگرهای M_j فضای $\mathcal{H}_B$ را به خودش می‌برند. حال فرض کنید که $|\psi^{AB}\rangle$ دارای تجزیه اشمیت $|\psi\rangle = \sum_l \lambda_l |l_A\rangle|l_B\rangle$ باشد که در آن $\{|l_A\rangle : l = 0, \dots, d-1\}$ پایه‌ای متعامد یکه برای فضای $\mathcal{H}_A$ و $\{|l_B\rangle : l = 0, \dots, d-1\}$ پایه‌ای متعامد یکه برای فضای $\mathcal{H}_B$ هستند. تعریف کنید

$$|\Phi\rangle_{AB} = \sum_l |l_A\rangle|l_B\rangle,$$

و Λ ماتریسی قطری (در پایه‌ی مشخص شده) بگیرید که درایه‌ی l-ام روی قطر آن λ_l باشد. در اینصورت[۷]

$$|\psi\rangle = \Lambda \otimes I|\Phi\rangle = I \otimes \Lambda|\Phi\rangle.$$

در ادامه از رابطه‌ی $X \otimes I|\Phi\rangle = I \otimes X^T|\Phi\rangle$ استفاده می‌کنیم که برای هر ماتریس X برقرار است و اثبات آن به خواننده واگذار می‌شود. داریم:

$$I \otimes M_j|\psi\rangle = (I \otimes M_j)(\Lambda \otimes I)|\Phi\rangle = (\Lambda \otimes I)(I \otimes M_j)|\Phi\rangle = (\Lambda \otimes I)(M_j^T \otimes I)|\Phi\rangle = \Lambda M_j^T \otimes I|\Phi\rangle.$$

با استفاده از قضیه‌ی تجزیه‌ی مقادیر تکین براحتی قابل اثبات است[۸] که برای هر عملگر X عملگرهای یکانی U, V وجود دارند به طوری که $X = UX^TV$. بنابراین عملگرهای یکانی U_j, V_j وجود دارند که $\Lambda M_j^T = U_j M_j \Lambda V_j$. در نتیجه

$$I \otimes M_j|\psi\rangle = U_j M_j \Lambda V_j \otimes I|\Phi\rangle = U_j M_j \otimes V_j^T \Lambda|\Phi\rangle = U_j M_j \otimes V_j^T|\psi\rangle.$$

حال قرار دهید $N_j = U_j M_j$ و $W_j = V_j^T$. واضح است که $\{N_j\}$ یک اندازه‌گیری در سمت آذر تعریف می‌کند و اثبات تمام است. □

قضیه ۹ فرض کنید آذر و بابک با انجام عملگرهای محلی (کوانتمی) و مخابرات کلاسیک $LOCC$ حالت محضی را که به اشتراک گذاشته‌اند به حالت محض دیگری تبدیل کنند. در این صورت این تبدیل را می‌توان با شرط این که آذر فقط یک پیغام کلاسیک به بابک می‌فرستد انجام داد. به عبارت دیگر عملیات $LOCC$ که حالت محضی را به حالت محضی تبدیل می‌کنند به صورت زیر نیز قابل شبیه‌سازی است: آذر یک اندازه گیری انجام داده و حاصل را برای بابک می‌فرستد؛ بابک با توجه به حاصل اندازه‌گیری آذر یک تحول یکانی روی سیستمش اعمال می‌کند.

اثبات: مانند اثبات قضیه‌ی قبل بدون کاسته شدن از کلیت مسأله می‌توان فرض کرد که بعد فضای هیلبرت سیستم آذر برابر با بعد فضای هیلبرت سیستم بابک است. همچنین توجه کنید که ممکن است در میانه‌ی پروتکل آذر یا بابک از (مثلا) کیوبیت‌های کمکی که در حالت $|0\rangle$ آماده سازی شده‌اند استفاده کنند ولی به راحتی قابل بررسی که این مانند

---

[۷] سؤال اول امتحان دوم بخش جبر خطی را بیاد آورید

[۸] فرض کنید که $X = U\Sigma V$ تجزیه مقادیر تکین X باشد. در این صورت $X^T = V^T \Sigma U^T$ خواهد بود و تجزیه مقادیر تکینی برای X^T مشخص میکند زیر ترانهانده هر ماتریس یکانی، یکانی است. پس $X = U\Sigma V = U(V^T)^{-1}\Sigma(U^T)^{-1}V$. پس $X = U_1 X^T V_1$ که در آن $U_1 = U(V^T)^{-1}, V_1 = (U^T)^{-1}V$.

بزرگ کردن فضای هیلبرت سیستم آذر و اعمال یک ایزومتری است ($|v\rangle \mapsto |v\rangle|0\rangle$). همچنین ممکن است مثلا بابک در میانه‌ی پروتکل یک کیوبیت را از سیستم خود خارج کند. به وضوح می‌توان این خارج کردن را به انتهای پروتکل تأخیر داد. از طرف دیگر چون فرض کرده‌ایم در انتها آذر و بابک به حالتی محض رسیده‌اند این خارج کردن کیوبیت حتما به صورت ($|w\rangle|v\rangle \mapsto |w\rangle$) خواهد بود. با در نظر گرفتن این نکات نتیجه می‌گیریم که (با بزرگتر در نظر گرفتن فضاهای سیستم‌های آذر و بابک) می‌توان فرض کرد که عملگرهای آذر و بابک در هر مرحله از پروتکل فقط شامل اندازه‌گیری و فرستادن حاصل اندازه‌گیری برای دیگری و اعمال عملگرهای یکانی است. حال با استفاده از قضیه‌ی قبل هر اندازه‌گیری بابک معادل یک اندازه‌گیری آذر و یک عملگر یکانی در سمت بابک است. پس می‌توان فرض کرد که آذر همه‌ی اندازه‌گیری‌ها را (چه اندازه‌گیری‌های خود و چه اندازه‌گیری‌های مربوط به بابک) پشت سر هم انجام داده، حاصل همه‌ی آنها را به یک باره برای بابک بفرستد و سپس بابک عملگرهای یکانی مربوطه را یکی پس از دیگری اعمال می‌کند. نکته در این است که طبق قضیه‌ی قبل بابک نیازی به انجام اندازه‌گیری ندارد و فقط عملگرهای یکانی اعمال می‌کند، لذا پیغامی ندارد که برای آذر بفرستد. □

تمرین ۱۰ ثابت کنید که دو حالت محض ψ_{AB} و ϕ_{AB} توسط عملگرهای یکانی محلی (و بدون مخابره کلاسیک) قابل تبدیل به یکدیگرند اگر و فقط اگر ضرایب تجزیه اشمیت آنها یکسان باشد.

۵ اثبات قضیه ۳

حال می‌توانیم به اثبات قضیه‌ی ۳ بپردازیم. ولی قبل از آن به قضیه‌ی دیگری نیاز داریم:

قضیه ۱۱ فرض کنیم که F و K دو عملگر هرمیتی باشند. در این صورت دنباله مقادیر ویژه K بر دنباله مقادیر ویژه F غلبه میکند (یا با نمادگذاری معادل $F \prec K$) اگر و فقط اگر یک توزیع احتمال p_j و ماتریس های یکانی U_j وجود داشته باشند به طوری که

$$F = \sum_j p_j U_j K U_j^\dagger.$$

اثبات قضیه بالا چندان پیچیده نیست و به صفحه ۵۷۵ کتاب ارجاع داده می‌شود.[۹]

حال قضیه ۳ را اثبات می‌کنیم:

اثبات: فرض کنیم که حالت $|\psi\rangle$ بتواند به وسیله LOCC به یک حالت محض دیگری مثل $|\phi\rangle$ تبدیل شود. طبق قضیه ۹ می‌توان فرض که این تبدیل حالت به صورت زیر است: آذر یک اندازه‌گیری انجام می‌دهد، حاصل اندازه‌گیری را برای بابک می‌فرستد و بابک با توجه با این حاصل اندازه‌گیری یک عملگر یکانی روی سیستم خود اعمال می‌کند. عملگرهای اندازه‌گیری آذر را $\{M_j\}$ بگیرید و فرض کنید که اگر حاصل اندازه‌گیری او j بود بابک عملگر یکانی U_j را روی سیستم خود اعمال می‌کند.

[۹] ذکر این نکته مفید است که این قضیه شبیه قضیه ای است که در مورد غلبه کردن بردارها داشتیم. یک بردار a بر بردار b غلبه میکرد ($b \prec a$) اگر b در پوش محدب a و بردارهایی که از جایگشت دادن درایه های a بدست می آید قرار میگرفت. اینجا بجای جایگشت دادن، دوران دادن با یک ماتریس یکانی را داریم.

ماتریس چگالی کاهیده روی سیستم آذر را با ρ_ψ^A نمایش دهید. در این صورت پس از اندازه‌گیری او سیستم A با احتمال p_j به حالت $\frac{1}{p_j} M_j \rho_\psi M_j^\dagger$ سقوط می‌کند. حال توجه کنید که عملگر یکانی‌ای که بابک اعمال می‌کند سیستم آذر را تغییر حالت نمی‌دهد. از طرف دیگر می‌دانیم که در انتها حالت مشترک آذر و بابک $|\phi\rangle$ است. پس باید داشته باشیم:

$$\rho_\phi = \frac{1}{p_j} M_j \rho_\psi M_j \dagger \quad \Rightarrow \quad M_j \rho_\psi M_j \dagger = p_i \rho_\phi.$$

تعریف کنید $X_j = M_j \sqrt{\rho_\psi}$ در این صورت:

$$X_j X_j^\dagger = p_i \rho_\phi.$$

هدف ما حل این معادله و یافتن X_j بر حسب $p_i \rho_\phi$ است. برای این کار از تجزیه‌ی قطبی X_j استفاده می‌کنیم. عملگر مثبت نیمه معین T_j و عملگر یکانی V_j وجود دارند به طوری که $X_j = T_j V_j$. در نتیجه با استفاده از رابطه فوق داریم

$$T_j^2 = p_j \rho_\phi = (\sqrt{p_j \rho_\phi})^2.$$

از آنجا که T_j و $\sqrt{p_j \rho_\phi}$ هر دو مثبت نیمه معین هستند و توان دوم آنها برابر است داریم $T_j = \sqrt{p_j \rho_\phi}$. نتیجه این که

$$M_j \sqrt{\rho_\psi} = X_j = \sqrt{p_j \rho_\phi} V_j.$$

متاسفانه از این معادله نمی‌توان مستقیما ρ_ψ را یافت چون ممکن است M_j وارون‌پذیر نباشد. اما می‌دانیم که شرط تمامیت $\sum_j M_j^\dagger M_j = I$ برقرار است. پس تلاش می‌کنیم که این جمله را بسازیم. با ضرب کردن $M_j \sqrt{\rho_\psi}$ با الحاقی آن نتیجه می‌گیریم:

$$\sqrt{\rho_\psi} M_j^\dagger M_j \sqrt{\rho_\psi} = p_j V_j^\dagger \rho_\phi V_j.$$

با جمع زدن روی j و با در نظر گرفتن شرط تمامیت $\sum_j M_j^\dagger M_j = I$ داریم

$$\rho_\psi = \sum_j p_j V_j^\dagger \rho_\phi V_j.$$

پس با توجه به قضیه ۱۱ نتیجه می‌گیریم که $\lambda_\psi \prec \lambda_\phi$.

اما اثبات عکس قضیه مشابه است. ابتدا با تحدید فضای هیلبرت سیستم آذر بدون کاسته شدن از کلیت می‌توان فرض کرد ρ_ψ وارون پذیر است. فرض کنید $\lambda_\psi \prec \lambda_\phi$ و یا معادلا $\rho_\psi \prec \rho_\phi$. پس با استفاده از قضیه ۱۱ می‌دانیم که احتمال‌های p_j و عملگرهای یکانی U_j وجود دارد به طوری که

$$\rho_\psi = \sum_j p_j U_j \rho_\phi U_j^\dagger.$$

با توجه به وارون‌پذیر بودن ρ_ψ عملگر M_j وجود دارد که

$$M_j \sqrt{\rho_\psi} = \sqrt{p_j \rho_\phi} U_j^\dagger. \qquad (۱)$$

حال شرط تمامیت را بررسی می‌کنیم:

$$\sum_j M_j^\dagger M_j = \rho_\psi^{-1/2}(\sum_j p_j U_j \rho_\phi U_j^\dagger)\rho_\psi^{-1/2} = \rho_\psi^{-1/2}\rho_\psi\rho_\psi^{-1/2} = I.$$

بنابراین $\{M_j\}$ تشکیل یک اندازه‌گیری می‌دهد. فرض کنیم که آذر این اندازه‌گیری را روی سیستم خود انجام داده و حاصل این اندازه‌گیری j شود. در این صورت حالت مشترک آذر و بابک به $M_j \otimes I|\psi\rangle$ و حالت سیستم آذر به

$$M_j\rho_\psi M_j^\dagger = p_j\rho_\phi$$

سقوط می‌کنند و این با احتمال

$$\|M_j \otimes I|\psi\rangle\|^2 = \mathrm{tr}(M_j\rho_\psi M_j^\dagger) = p_j,$$

اتفاق می‌افتد. در واقع پس از اندازه‌گیری آذر کل سیستم به حالت $\frac{1}{\sqrt{p_j}}M_j \otimes I|\psi\rangle$ سقوط می‌کند و این حالت یک محض‌سازی از حالت سیستم آذر (پس از اندازه‌گیری) یعنی ρ_ϕ است. از طرف دیگر $|\phi\rangle$ خود نیز یک محض‌سازی از ρ_ϕ است. نتیجه این که عملگر یکانی V_j وجود دارد که

$$|\phi\rangle = \frac{1}{\sqrt{p_j}}M_j \otimes V_j|\psi\rangle,$$

و بابک پس از اطلاع از حاصل اندازه‌گیری آذر با اعمال V_j می‌تواند کل سیستم را به حالت $|\phi\rangle$ ببرد. $\square$