مدرس: سلمان ابوالفتح بیگی
نویسنده: سلمان ابوالفتح بیگی

جلسه ۱۳

جلسه‌ی گذشته دیدیم که یک کد کوانتمی در کلی‌ترین شکل خود متناظر با یک زیرفضای $W \subseteq \mathcal{H}$ است که در آن $\mathcal{H}$ فضای هیلبرت n کیوبیت است (که در این حالت طول کد n خواهد بود). کدگذاری با یک عملگر خطی حافظ ضرب داخلی (isometry) $V : \mathcal{K} \to W \subseteq \mathcal{H}$ مشخص می‌شود که در آن $\mathcal{K}$ فضای هیلبرت k کیوبیت است (که در این حالت کد کوانتمی k کیوبیت را کد می‌کند). P را عملگر تصویر عمود روی زیر فضای W گرفتیم.

خطایی که روی فضای کد اثر می‌کند را در حالت کلی یک نگاشت کوانتمی کاملا مثبت و حافظ اثر به صورت $\mathcal{E} : \mathbf{L}(\mathcal{H}) \to \mathbf{L}(\mathcal{H})$ گرفتیم.

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger$$

که $\sum_i E_i^\dagger E_i = I$. در این صورت کد P خطای $\mathcal{E}$ را تصحیح می‌کند اگر وجود داشته باشد نگاشت کوانتمی $\mathcal{R} : \mathbf{L}(\mathcal{H}) \to \mathbf{L}(\mathcal{H})$ به طوری که برای هر ماتریس چگالی ρ داشته باشیم $\mathcal{R} \circ \mathcal{E}(P\rho P) = P\rho P$.

قضیه‌ی زیر مهم‌ترین نتیجه‌ی جلسه‌ی گذشته بود.

قضیه: کد P تحت خطای $\mathcal{E}$ قابل تصحیح است اگر و فقط اگر برای هر i, j وجود داشته باشد $\alpha_{ij} \in \mathbb{C}$ به طوری که

$$PE_i^\dagger E_j P = \alpha_{ij} P. \qquad (۱)$$

۱ گسسته سازی خطا

فرض کنید کد P خطای $\mathcal{E}$ را تصحیح کند و $\mathcal{F}(\rho) = \sum_k F_k \rho F_k^\dagger$ را نگاشت کوانتمی دیگری بگیرید به طوری که وجود داشته باشد $c_{ki} \in \mathbb{C}$ که

$$F_k = \sum_i c_{ki} E_i. \qquad (۲)$$

در این صورت داریم

$$PF_k^\dagger F_\ell P = \sum_{i,j} c_{ki}^* c_{\ell j} PE_i^\dagger E_j P = \left(\sum_{i,j} c_{ki}^* c_{\ell j} \alpha_{ij} \right) P.$$

بنابراین طبق قضیه‌ی بالا کد P خطای $\mathcal{F}$ را نیز تصحیح می‌کند.

قضیه: فرض کنید کد P خطای $\mathcal{E}$ را تصحیح کند و وجود داشته باشد $\mathcal{R}$ به طوری که برای هر ρ داشته باشیم $\mathcal{R}\circ\mathcal{E}(P\rho P) = P\rho P$. همچنین فرض کنید $\mathcal{F}$ خطای دیگری باشد و (۲) برقرار باشد. در این صورت داریم $\mathcal{R}\circ\mathcal{F}(P\rho P) = P\rho P$.

در بالا استدلال کردیم که خطای $\mathcal{F}$ قابل تصحیح است اگر خطای $\mathcal{E}$ قابل تصحیح باشد. نکته‌ی نابدیهی دیگری که در این قضیه وجود دارد این است که «همان» عملیات کدبرداری‌ای که خطای $\mathcal{E}$ تصحیح می‌کند، خطای $\mathcal{F}$ را نیز تصحیح می‌کند.

$$\mathcal{R}\circ\mathcal{E}(P\rho P) = P\rho P \quad \Rightarrow \quad \mathcal{R}\circ\mathcal{F}(P\rho P) = P\rho P.$$

برای اثبات این قضیه به کتاب مراجعه کنید.

جلسه‌ی پیش گفتیم یکی از استدلال‌های انکار کنندگان وجود کد کوانتمی پیوسته بودن فضای خطاها بود. قضیه‌ی فوق فضای خطاهای کوانتمی را گسسته می‌کند. فرض کنید بخواهیم کدی طراحی کنیم که هر گونه خطا روی «یک» کیوبیت را تصحیح کند. برای این کار کافی است نشان دهیم که این کد مجموعه‌ی خطاهای $\{E_i\} = \{I, X, Y, Z\}$ را تصحیح می‌کند که X, Y, Z ماتریس‌های پاولی هستند.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

نکته در این است که ماتریس‌های پاولی یک پایه برای فضای ماتریس‌های 2×2 تشکیل می‌دهند و لذا با تصحیح این خطاها هر خطای دیگری نیز تصحیح می‌شود. این ایده را با بررسی دقیق‌تر کد 9-کیوبیتی شور بررسی می‌کنیم.

۲ کد 9-کیوبیتی شور

کد شور 1 کیوبیت را که در حالت $\alpha|0\rangle + \beta|1\rangle$ قرار دارد در 9 کیوبیت به صورت $\alpha|v_0\rangle + \beta|v_1\rangle$ کد می‌کند که در آن

$$|v_0\rangle = \frac{1}{2\sqrt{2}}\left((|000\rangle + |111\rangle)\otimes(|000\rangle + |111\rangle)\otimes(|000\rangle + |111\rangle)\right),$$
$$|v_1\rangle = \frac{1}{2\sqrt{2}}\left((|000\rangle - |111\rangle)\otimes(|000\rangle - |111\rangle)\otimes(|000\rangle - |111\rangle)\right).$$

در نتیجه طبق تعریف P یعنی زیرفضای کد برابر است با

$$P = |v_0\rangle\langle v_0| + |v_1\rangle\langle v_1|.$$

می‌خواهیم نشان دهیم این کد هر خطایی که روی یک کیوبیت به وجود بیاید را تصحیح می‌کند. برای این کار خطای زیر را در نظر می‌گیریم

$$\mathcal{E}(\rho) = \frac{1}{28}\left(\rho + \sum_{i=1}^{9} X_i\rho X_i + Y_i\rho Y_i + Z_i\rho Z_i\right).$$

در اینجا منظور از (برای مثال) X_i عملگر پاولی X است که روی کیوبیت i-ام اثر می‌کند (و روی باقی کیوبیت‌ها به صورت همانی اثر می‌کند). توجه کنید که هر عملگر E که روی کیوبیت i-ام اثر کند را می‌توان به صورت ترکیب خطی I, X_i, Y_i, Z_i نوشت. پس طبق قضیه‌ی قبل اگر خطای فوق قابل تصحیح باشد هر خطای دیگر نیز قابل تصحیح است و می‌توان نتیجه گرفت که کد P هر خطایی که روی یک کیوبیت واقع شود را تصحیح می‌کند.

حال می‌خواهیم ثابت کنیم که برای هر $E, E' \in \{I, X_1, \dots, X_9, Y_1, \dots, Y_9, Z_1, \dots, Z_9\}$ وجود دارد $\alpha \in \mathbb{C}$ که $PE^\dagger E'P = \alpha P$.

تعریف کنید

$$g_1 = Z_1Z_2, \quad g_2 = Z_2Z_3, \quad g_3 = Z_4Z_5$$
$$g_4 = Z_5Z_6, \quad g_5 = Z_7Z_8, \quad g_6 = Z_8Z_9$$
$$g_7 = X_1X_2X_3X_4X_5X_6, \quad g_8 = X_4X_5X_6X_7X_8X_9$$

داریم $g_i^\dagger = g_i$، $g_i^2 = I$ و $g_ig_j = g_jg_i$. همچنین داریم $g_i|v_a\rangle = |v_a\rangle$ برای $a = 0, 1$. به عبارت دیگر تحدید g_i-ها روی زیرفضای کد عملگر همانی است:

$$g_iP = P.$$

قرار دهید

$$Q = \prod_{i=1}^{8} \frac{I + g_i}{2}.$$

از آنجا که $g_i^2 = I$، مقادیر ویژه‌ی g_i برابر با ± 1 هستند و $\frac{I+g_i}{2}$ برابر عملگر تصویر روی زیرفضای ویژه‌ی g_i با مقدار ویژه‌ی $+1$ است. از طرف دیگر g_i-ها دو به دو جابجا می‌شوند. بنابراین Q برابر با عملگر تصویر روی زیر فضای ویژه‌ی «مشترک» همه‌ی g_i-ها با مقدار ویژه‌ی $+1$ است. در واقع از $g_iP = P$ نتیجه می‌شود $QP = P$. یعنی P را می‌توان به عنوان زیر فضایی از Q در نظر گرفت.

ادعا می‌کنیم $Q = P$. برای اثبات این تساوی از آنجا که $QP = P$ کافی است نشان دهیم $\text{rank}Q = \text{rank}P = 2$. چون Q یک عملگر تصویر است داریم $\text{rank}Q = \text{tr}Q$.

$$\begin{aligned}\text{tr}Q &= \text{tr}\prod_{i=1}^{8}\frac{I+g_i}{2}\\ &= \frac{1}{2^8}\sum_{T\subseteq\{1,\dots 8\}} \text{tr}\left(\prod_{i\in T} g_i\right)\\ &= \frac{1}{2^8}\text{tr}I = \frac{2^9}{2^8} = 2.\end{aligned}$$

در اینجا از این نکته استفاده کردیم که اثر هر عملگر پاولی برابر 2^9 است اگر همانی باشد و در غیر این صورت برابر 0 است. پس

$$P = Q = \prod_{i=1}^{8} \frac{I+g_i}{2}.$$

حال فرض کنید $E, E' \in \{I, X_1, \ldots, X_9, Y_1, \ldots, Y_9, Z_1, \ldots, Z_9\}$. در نتیجه $F = E^\dagger E'$ یک ماتریس پاولی است که روی حداکثر 2 کیوبیت اثر می‌کند. به راحتی قابل بررسی است که به ازای هر عملگر پاولی $F \neq I$ که روی یک یا دو کیوبیت اثر کند وجود دارد i به طوری که $Fg_i = -g_i F$. به عبارت دیگر هر عملگر پاولی نابدیهی (غیر همانی) که با همه‌ی g_i-ها جابجا شود، حداقل روی 3 کیوبیت اثر می‌کند. (توجه کنید که برای هر دو ماتریس پاولی g, h داریم $gh = hg$ یا $gh = -hg$.) بنابراین:

$$PFP = P\left(\frac{I+g_i}{2}\right)F\left(\frac{I+g_i}{2}\right)P = PF\left(\frac{I-g_i}{2}\right)\cdot\left(\frac{I+g_i}{2}\right)P = 0.$$

ادعا ثابت شد.

۳ کدهای کوانتمی جمعی

کد شور و استدلال‌های فوق حالت خاصی از فرمول‌بندی کدهای جمعی کوانتمی هستند. با چند نمادگذاری شروع می‌کنیم. G را مجموعه‌ی ماتریس‌های پاولی بگیرید که روی n کیوبیت اثر می‌کنند.

$$G = \{c\sigma_1 \otimes \cdots \otimes \sigma_n : \quad c \in \{\pm 1, \pm i\}, \sigma_j \in \{I, X, Y, Z\}\}.$$

منظور از X_1Z_2 عملگر پاولی است که $c = 1$، $\sigma_1 = X, \sigma_2 = Z$ و $\sigma_j = I$ برای هر $j \neq 1, 2$. G یک گروه است که که به آن گروه پاولی می‌گویند. به راحتی قابل بررسی است که برای هر دو ماتریس پاولی داریم $gh = gh$ یا $hg = -gh$. همچنین اگر $g^\dagger = g$ آن گاه $g^2 = I$. در واقع مقادیر ویژه‌ی $g \in G$ یا ± 1 است و یا $\pm i$.

در روش کدهای جمعی ابتدا یک زیرگروه $S \subseteq G$ مشخص می‌کنیم و P را (عملگر تصویر روی) زیرفضای ویژه‌ی مشترک اعضای S با مقدار ویژه‌ی $+1$ می‌گیریم. سوالی که در اینجا پیش می‌آید این است که چه موقع P ناصفر است؟

قضیه: P ناصفر است اگر و فقط اگر S آبلی باشد و $-I \notin S$.

اثبات: ($\Leftarrow$) چون همه‌ی مقادیر ویژه‌ی $-I$، -1 هستند، اگر $-I \in S$ آنگاه طبق تعریف $P = 0$. همچنین اگر $g, h \in S$ به طوری که $gh = -hg$ و $|\psi\rangle$ یک بردار ویژه‌ی مشترک آنها با مقدار ویژه‌ی $+1$ باشد داریم:

$$|\psi\rangle = g|\psi\rangle = gh|\psi\rangle = -hg|\psi\rangle = -|\psi\rangle$$

پس $|\psi\rangle = 0$.

($\Rightarrow$) فرض کنید S آبلی باشد و $-I \notin S$. اگر $g \in S$ هرمیتی نباشد آنگاه $g^2 = -I \in S$ که تناقض است. نتیجه می‌گیریم که همه‌ی اعضای $g \in S$ هرمیتی هستند و در نتیجه $g^2 = I$.

$S \supseteq \{g_1, \dots, g_k\}$ را یک مجموعه‌ی مولد مینیمال زیرگروه S بگیرید. با تکرار محاسباتی که در مورد کد شور انجام دادیم نتیجه می‌شود که

$$P = \prod_{i=1}^{k} \frac{I + g_i}{2}.$$

همچنین توجه کنید که طبق فرض $\{g_1, \dots, g_k\}$ یک مجموعه‌ی مولد مینیمال است. پس $\prod_{i\in T} g_i$ فقط وقتی همانی است که $T = \emptyset$. در نتیجه بعد فضای کد برابر است با

$$\mathrm{tr}P = \frac{1}{2^k} \sum_{T\subseteq\{1,\dots,k\}} \mathrm{tr}\left(\prod_{i\in T} g_i\right) = 2^{n-k} \neq 0.$$

طبق این قضیه نه تنها می‌توانیم تشخیص دهیم که چه موقع فضای کد نابدیهی است، بلکه بعد فضای کد را نیز می‌توانیم محاسبه کنیم. در واقع کد P (یعنی فضای ویژه‌ی مشترک اعضای S با مقدار ویژه‌ی $+1$) تعداد $n - k$ کیوبیت را کد می‌کند اگر S آبلی باشد، $-I \notin S$ و مجموعه‌ی مولد مینیمال S، k عضوی باشد. قدم بعدی این است که مشخص کنیم P چه خطاهایی را تصحیح می‌کند. طبق قضیه‌ی گسسته‌سازی خطاها و این که ماتریس‌هایی پاولی پایه‌ای برای فضای خطاها تشکیل می‌دهند، به طور معادل می‌توانیم به سوال زیر پاسخ دهیم. P چه خطاهای پاولی‌ای را تصحیح می‌کند.

برای جواب دادن به سوال فوق به یک تعریف نیاز داریم:

$$N(S) = \{h \in G : \quad \forall g \in S,\ \ hg = gh\} = \{h \in G : \quad \forall i, 1 \leq i \leq k,\ \ hg_i = g_i h\}.$$

در واقع از آنجا که $-I \notin S$ می‌توان نشان داد که $N(S)$ همان «نرمال‌ساز» S در G است. چون S آبلی است داریم $S \subseteq N(S)$.

قضیه: فرض کنید $M \subseteq G$ مجموعه‌ای از خطاهای پاولی باشد. در این صورت P خطاهای M را تصحیح می‌کند اگر به ازای هر $E, E' \in M$ داشته باشیم $E^\dagger E' \notin N(S) \setminus S$.

اثبات: باید نشان دهیم $\alpha \in \mathbb{C}$ وجود دارد به طوری که $PE^\dagger E' P = \alpha P$.

$F = E^\dagger E'$ یک ماتریس پاولی است. اگر $F \notin N(S) \setminus S$ دو حالت داریم: یا $F \in S$ و یا $F \notin N(S)$. اگر $F \in S$ آنگاه طبق تعریف داریم $PFP = P$. اگر $F \notin N(S)$ طبق تعریف وجود دارد i به طوری که $g_i F = -F g_i$. داریم

$$PFP = P\left(\frac{I + g_i}{2}\right) F \left(\frac{I + g_i}{2}\right) P = PF\left(\frac{I - g_i}{2}\right) \cdot \left(\frac{I + g_i}{2}\right) P = 0.$$

در واقع اگر خطا در S باشد، آنگاه اثر آن روی فضای کد همانی است. آگر خطا در $N(S)$ نباشد که اثر آن زیرفضای کد را به یک زیرفضای عمود بر آن می‌برد و لذا قابل تشخیص و تصحیح است.