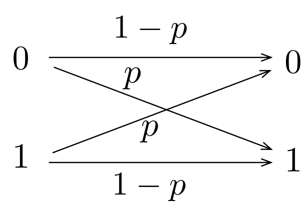
محاسبات کوانتمی (۲۲۶۷۱) ترم بهار ۱۳۹۱-۱۳۹۰
مدرس: سلمان ابوالفتح بیگی نویسنده: سلمان ابوالفتح بیگی

جلسه ۱۲

ذخیره، پردازش و انتقال اطلاعات در دنیای واقعی همواره در حضور خطا[۱] انجام می‌شود. مثلا اطلاعات کلاسیکی که به صورت دنباله‌ای از $0, 1$ نمایش داده شده‌اند، در حین محاسبه ممکن است با خطا مواجه شده و یکی از بیت‌های آن تغییر کند. اگر احتمال تغییر هر بیت را p در نظر بگیریم، خطا با «کانال» زیر نمایش داده می‌شود:



در نتیجه اگر اطلاعات ذخیره شده 011 باشد، با احتمال $p(1-p)^2$ به 010 تبدیل و با احتمال $(1-p)^3$ هیچ تغییری نمی‌کند. حال فرض کنید که برای ذخیره‌ی اطلاعات از «کد تکرار[۲]» استفاده کرده و بیت 0 را با 000 و بیت 1 را با 111 ذخیره کنیم

$$0 \to 000$$
$$1 \to 111$$

به هر یک از 000 و 111 یک کلمه کد[۳] گویند. در این مثال اطلاعات 011 به صورت 000111111 ذخیره می‌شود. حال فرض کنید که مثلا روی بیت اول خطا ایجاد شده و به 100111111 تبدیل شود. در این صورت با نگاه کردن به سه بیت اول متوجه می‌شویم که آنها یکسان نیستند و لذا روی حداقل یکی از آنها خطا به وجود آمده. همچنین با فرض اینکه خطا فقط روی یک بیت ایجاد شده، نتیجه می‌گیریم که بیت اول تغییر کرده و می‌توانیم آن را تصحیح کنیم.

در این مثال سه مرحله را در نظر گرفتیم. ابتدا «کد گذاری» که مشخص کردیم هر بیت 0 یا 1 چگونه ذخیره می‌شود. قدم دوم مدل کردن نوع خطایی (کانالی) است که روی اطلاعات ذخیره شده ایجاد می‌شود. در انتها مرحله‌ی «کد برداری[۴]» است که روشی است برای تصحیح خطا.

[۱] Noise
[۲] Repetition code
[۳] Codeword
[۴] Decoding

در بالا مثالی از نحوه‌ی کدگذاری و کانال را معرفی کردیم. در این مثال الگوریتم ما برای کدبرداری به این صورت خواهد بود که سه بیت متناظر با هر بیت از اطلاعات را درنظر می‌گیریم. از این سه بیت حداقل دو بیت یکسان هستند، و بیت سوم را (در صورت تفاوت) تصحیح کرده و برابر با آن دو بیت قرار می‌دهیم. مثلا با مشاهده‌ی 010 آن را به 000 تغییر می‌دهیم.

در این مثال احتمال خطا روی هر بیت از اطلاعات، قبل از کد گذاری p بود. بعد از کد گذاری، الگوریتم کد برداری ما دچار اشتباه می‌شود اگر 2 یا 3 خطا ایجاد شود. پس احتمال اشتباه در کدبرداری برابر است با $3p(1-p)^2 + p^3$ که اکیدا کوچکتر از p است (اگر $p < 1/2$). در حالت کلی‌تر اگر هر بیت را با $n = 2m+1$ بیت یکسان کد کنیم و کدبرداری مشابهی را در نظر بگیریم احتمال خطا برابر خواهد بود با

$$\sum_{\ell \geq m+1} \binom{n}{\ell} p^{\ell}(1-p)^{n-\ell}$$

که به 0 میل می‌کند وقتی n، یعنی طول کد به سمت بینهایت برود.

بهینه بودن یک کد با سه پارامتر مشخص می‌شود. یکی k تعداد بیت‌هایی است که کد می‌شود. در مثال بالا $k = 1$ بود چون فقط یک بیت را کد می‌کنیم. دوم n طول کد است و برابر با طول هر یک از کلمه کدها. در آخر d فاصله‌ی کد[۵] است. در کد تکرار $d = n$ زیرا تعداد بیت‌های متفاوت دو کلمه کد $0\ldots00$ و $1\ldots11$ برابر n است. یک کد کلاسیک با $[n, k, d]$ نشان داده می‌شود.

۱ کدهای کوانتمی

بعد از الگوریتم تجزیه‌ی شور عده‌ای اعتقاد داشتند که این الگوریتم هیچ‌گاه قابل پیاده سازی نیست. آنها استدلال می‌کردند که کد کوانتمی وجود ندارد پس خطاهایی که در دنیای واقعی در حین پیاده سازی الگوریتم ایجاد می‌شوند را نمی‌توان تصحیح کرد. استدلال آنها برای انکار وجود کد کوانتمی سه محور اصلی داشت. نخست اینکه طبق قضیه‌ی no cloning اطلاعات کوانتمی را نمی‌توان کپی کرد. برای مثال در کد کلاسیک تکرار هر بیت را n بار کپی می‌کنیم، ولی کپی کردن کیوبیت‌ها امکان پذیر نیست. دوم اینکه خطاهای کوانتمی پیوسته هستند. در دنیای کلاسیک خطاهایی که روی یک (یا چند بیت) ایجاد می‌شود مجموعه‌ای گسسته و متناهی تشکیل می‌دهند ولی در دنیای کوانتمی، دینامیک‌های کوانتمی (که مجموعه‌ای پیوسته و نامتناهی تشکیل می‌دهند) را می‌توان به عنوان یک خطا در نظر گرفت. سوم اینکه برای تصحیح خطا (کد برداری) یک سیستم کوانتمی ابتدا باید اندازه‌گیری انجام داد، ولی این اندازه‌گیری باعث تغییر حالت[۶] سیستم می‌شود و اطلاعات را از بین می‌برد. با وجود این استدلال‌ها اولین کد کوانتمی در سال ۱۹۹۵ کشف شد.

بررسی کدهای کوانتمی را با مثال‌هایی ساده شروع می‌کنیم.

خطای کوانتمی در واقع یک دینامیک کوانتمی است، پس با یک نگاشت کاملا مثبت و حافظ اثر مشخص می‌شود. X را ماتریس پاولی بگیرید

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

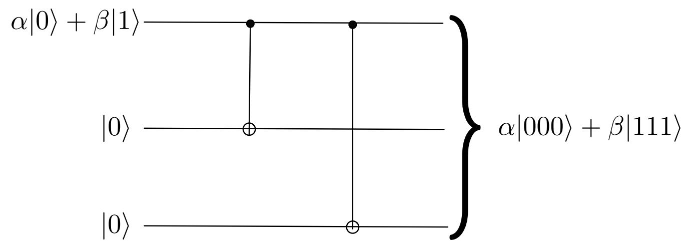
[۵] Code distance
[۶] Collapse

و خطا را برابر $\mathcal{E}(\rho) = (1-p)\rho + pX\rho X$ قرار دهید. این نگاشت را می‌توان به این صورت تعبیر کرد که روی ورودی ρ با احتمال p خطای X رخ می‌دهد و با احتمال $(1-p)$ هیچ خطایی ایجاد نمی‌شود. توجه کنید که $X|0\rangle = |1\rangle$ و $X|1\rangle = |0\rangle$ پس این خطا معادل کوانتمی خطای کلاسیکی است که در بالا در نظر گرفتیم.

حال با مشخص کردن خطا قدم بعد مشخص کردن نحوه‌ی کدگذاری و کدبرداری است. برای کدگذاری معادل کوانتمی کد تکرار را در نظر می‌گیریم:

$$\begin{aligned} |0\rangle &\to |000\rangle, \\ |1\rangle &\to |111\rangle. \end{aligned} \tag{۱}$$

با این کدگذاری فضای دو بعدی یک کیوبیت، به زیر فضایی دو بعدی از فضای هشت بعدی متناظر با سه کیوبیت نگاشته می‌شود. در واقع حالت $\alpha|0\rangle + \beta|1\rangle$ به حالت $\alpha|000\rangle + \beta|111\rangle$ کد می‌شود. مدار زیر نحوه‌ی کدگذاری را مشخص می‌کند.



حال باید کدبرداری را معرفی کنیم. در کدبرداری ابتدا باید «اندازه‌گیری» انجام دهیم. این اندازه‌گیری مشخص می‌کند که آیا روی اطلاعات ما خطا رخ داده یا نه. بعد اگر خطا رخ داده بود باید آن را تصحیح کرد. به این اندازه‌گیری اصطلاحا syndrome measurement گویند. در این مثال خاص اندازه‌گیری متناظر همانند همان اندازه‌گیری کد کلاسیک تکرار است:

$$\begin{aligned} P_0 &= |000\rangle\langle 000| + |111\rangle\langle 111|, \\ P_1 &= |100\rangle\langle 100| + |011\rangle\langle 011|, \\ P_2 &= |010\rangle\langle 010| + |101\rangle\langle 101|, \\ P_3 &= |001\rangle\langle 001| + |110\rangle\langle 110|. \end{aligned}$$

توجه کنید که $P_0 + P_1 + P_2 + P_3 = I$. اگر حاصل اندازه‌گیری P_0 باشد فرض می‌کنیم که هیچ خطایی رخ نداده و اگر حاصل اندازه‌گیری P_i باشد $(1 \le i \le 3)$ فرض می‌کنیم که خطای X روی کیوبیت i-ام رخ داده که با اعمال عملگر X روی آن کیوبیت خطا را تصحیح می‌کنیم. نگاشت کوانتمی متناظر با این کدبرداری برابر است با

$$\mathcal{R}(\sigma) = P_0\sigma P_0 + X_1P_1\sigma P_1X_1 + X_2P_2\sigma P_2X_2 + X_3P_3\sigma P_3X_3,$$

که در آن منظور از X_i عملگر X است که روی کیوبیت i-ام اثر می‌کند (برای مثال $X_2 = I \otimes X \otimes I$).

به راحتی می‌توان دید که این کد کوانتمی همانند کد کلاسیک تکرار عمل می‌کند. به این معنا که قبل از کدگذاری احتمال خطا p بود و بعد از آن برابر $3p(1-p)^2+p^3$ می‌شود.

این کد کوانتمی خاص قابلیت تصحیح خطای X روی یک کیوبیت را دارد. ولی خطای Z

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

را نیز می‌توان به عنوان یک خطا کوانتمی در نظر گرفت. مثلاً فرض کنید که روی کیوبیت اول خطای Z رخ دهد. اگر حالت سیستم بعد از کدگذاری $\alpha|000\rangle + \beta|111\rangle$ باشد پس از ایجاد خطا حالت $\alpha|000\rangle - \beta|111\rangle$ خواهد شد. این حالت متناظر با کد شده‌ی حالت $\alpha|0\rangle - \beta|1\rangle$ نیز هست. حال با مشاهده‌ی (اندازه‌گیری) این حالت ما نمی‌توانیم تشخیص دهیم که حالت سیستم قبل از کدگذاری $\alpha|0\rangle + \beta|1\rangle$ بوده که روی آن خطا ایجاد شده و یا $\alpha|0\rangle - \beta|1\rangle$ بوده و خطایی رخ نداده. پس این کد خطای Z را تصحیح نمی‌کند.

گرچه کد بالا خطای Z را تصحیح نمی‌کند اگر کانال متناظر با خطا برابر $\mathcal{E}(\rho) = (1-p)\rho + pZ\rho Z$ بود می‌توانستیم از کد

$$\alpha|0\rangle + \beta|1\rangle \to \alpha|+++\rangle + \beta|---\rangle \tag{۲}$$

استفاده کنیم که در آن $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. به راحتی می‌توان کدبرداری متناظر را نیز تعریف و بررسی کرد که این کد خطای Z که روی یک کیوبیت رخ داده را تصحیح می‌کند.

۲ کد شور

سؤالی که در اینجا پیش می آید این است که آیا کدی وجود دارد که هم خطای X را تصحیح کند و هم خطای Z را. کد شور[۷] کدی است 9 کیوبیتی که «هر» خطایی (شامل خطای X و Z) که روی یک کیوبیت رخ دهد را تصحیح می‌کند. نحوه‌ی کدگذاری کد شور به صورت زیر است:

$$\begin{aligned} |0\rangle &\to \frac{1}{2\sqrt{2}}\left((|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)\right), \\ |1\rangle &\to \frac{1}{2\sqrt{2}}\left((|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)\right). \end{aligned}$$

توجه کنید که این کد به این صورت بدست می‌آید که ابتدا یک کیوبیت را با کد (۲) کد می‌کنیم و یک حالت سه-کیوبیتی بدست می‌آوریم. سپس هر یک از سه کیوبیت را با کد (۱) کد می‌کنیم. از آنجا که هر یک از کدهای (۱) و (۲) می‌تواند به ترتیب خطای X یا Z را تصحیح کند، می‌توان نتیجه کرد که کد شور خطای X و Z هر دو را تصحیح می‌کند. نکته‌ی نابدیهی این است که این کد نه تنها این دو خطا، بلکه هر خطای دیگری که روی یک کیوبیت رخ دهد را نیز تصحیح می‌کند. این ادعا را در جلسات آینده ثابت می‌کنیم.

[۷] Shor's code

۳ قضیه‌ی کنیل-لافلامه

فرض کنید بخواهیم k کیوبیت را در n کیوبیت کد کنیم. فضای هیلبرت متناظر با k کیوبیت یک فضای برداری 2^k بعدی است با پایه‌ی متعامد یکه‌ی $\{|x\rangle \, : \, x \in \{0,1\}^k\}$. برای کدگذاری باید متناظر با هر یک از حالات $|x\rangle$ یک حالت n-کیوبیتی $|\psi_x\rangle$ نسبت دهیم. از آنجا که حالات $|x\rangle$ متعامد یکه هستند، انتظار داریم $|\psi_x\rangle$ها نیز متعامد یکه باشند. اگر W را زیر فضای برداری پوشیده شده با بردارهای $|\psi_x\rangle$ بگیریم، W را زیر فضای کد گویند و

$$P = \sum_{x\in\{0,1\}^k} |\psi_x\rangle\langle\psi_x|$$

عملگر تصویر عمود روی این زیرفضاست و داریم $\dim W = \mathrm{tr} P = 2^k$.

خطای کوانتمی در حالت کلی متناظر با یک نگاشت کاملاً مثبت و حافظ اثر است:

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

که در آن $\sum_i E_i^\dagger E_i = I$.

همچنین عمل کدبردای و تصحیح خطا نیز در حالت کلی متناظر با یک نگاشت کوانتمی است:

$$\mathcal{R}(\rho) = \sum_\ell R_\ell \rho R_\ell^\dagger$$

که $\sum_\ell R_\ell^\dagger R_\ell = I$.

تعریف: کد P خطای $\mathcal{E}$ را تصحیح می‌کند اگر $\mathcal{R}$ وجود داشته باشد به طوری که برای هر $|\psi\rangle \in W$

$$\mathcal{R}\circ\mathcal{E}(|\psi\rangle\langle\psi|) = |\psi\rangle\langle\psi|.$$

به طور معادل خطای $\mathcal{E}$ توسط $\mathcal{R}$ قابل تصحیح است اگر برای هر ρ داشته باشیم: $\mathcal{R}\circ\mathcal{E}(P\rho P) = P\rho P$.

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

$$PE_i^\dagger E_j P = \alpha_{ij} P. \qquad (۳)$$

در مثال کد (۱)، W برابر زیرفضای تولید شده توسط $\{|000\rangle, |111\rangle\}$ است و $P = |000\rangle\langle 000| + |111\rangle\langle 111|$. همچنین $\mathcal{E}(\rho) = q_1 X_1 \rho X_1 + q_2 X_2 \rho X_2 + q_3 X_3 \rho X_3$ که در آن $q_i > 0$ و $\sum_i q_i = 1$. یعنی با احتمال q_i خطای X روی کیوبیت i-ام رخ می‌دهد. پس $E_i \sim X_i$ و داریم $PX_i^\dagger X_j P = \delta_{ij} P$. درنتیجه شرط قضیه برقرار

است و خطای $\mathcal{E}$ قابل تصحیح است.

اثبات: $(\Leftarrow)$ اگر $\mathcal{R}$ وجود داشته باشد به طوری که برای هر $|\psi\rangle \in W$ داشته باشیم $\mathcal{R} \circ \mathcal{E}(|\psi\rangle\langle\psi|) = |\psi\rangle\langle\psi|$ داریم

$$\begin{aligned} |\psi\rangle\langle\psi| &= \sum_\ell R_\ell \left(\sum_i E_i |\psi\rangle\langle\psi| E_i^\dagger \right) R_\ell^\dagger \\ &= \sum_{i,\ell} R_\ell E_i |\psi\rangle\langle\psi| E_i^\dagger R_\ell^\dagger. \end{aligned}$$

در نتیجه برای هر i, ℓ داریم $R_\ell E_i |\psi\rangle$ ضریبی از $|\psi\rangle$ است. (سمت چپ یک عملگر با رتبه‌ی یک است، پس سمت راست نیز باید رتبه‌ی یک داشته باشد.) در واقع از آنجا که این رابطه برای هر $|\psi\rangle \in W$ برقرار است و $P|\psi\rangle = |\psi\rangle$ می‌توان نتیجه گرفت که برای هر i, ℓ وجود دارد $c_{i\ell}$ به طوری که $R_\ell E_i P = c_{i\ell} P$. حال داریم

$$\begin{aligned} P E_i^\dagger E_j P &= \sum_\ell P E_i^\dagger R_\ell^\dagger R_\ell E_j P \\ &= \sum_\ell (R_\ell E_i P)^\dagger (R_\ell E_j P) \\ &= \sum_\ell (c_{i\ell} P)^\dagger (c_{j\ell} P) \\ &= \left(\sum_\ell c_{i\ell}^* c_{j\ell} \right) P, \end{aligned}$$

که در اینجا از رابطه‌ی $\sum_\ell R_\ell^\dagger R_\ell = I$ استفاده کردیم.

$(\Rightarrow)$ فرض کنید α_{ij} وجود داشته باشد به طوری که $P E_i^\dagger E_j P = \alpha_{ij} P$ و α را ماتریسی بگیرید که درایه‌ی (i, j) آن برابر α_{ij} باشد. به راحتی می‌توان بررسی کرد که α هرمیتی و مثبت نیمه معین است. در نتیجه ماتریس یکانی $u = (u_{ik})$ وجود دارد به طوری که $d = u^\dagger \alpha u$ قطری باشد با درایه‌های $d_{ii} \geq 0$ روی قطر. توجه کنید که

$$P = P^2 = \sum_i P E_i^\dagger E_i P = \sum_i \alpha_{ii} P.$$

بنابراین $\mathrm{tr}\alpha = 1$. تعریف کنید

$$F_k = \sum_i u_{ik} E_i.$$

با توجه به یکانی بودن u می‌توان بررسی کرد که $\sum_k F_k \rho F_k^\dagger = \sum_i E_i \rho E_i^\dagger = \mathcal{E}(\rho)$. همچنین داریم

$$P F_k^\dagger F_\ell P = \sum_{i,j} u_{ik}^* u_{j\ell} P E_i^\dagger E_j P = \sum_{i,j} u_{ik}^* u_{j\ell} \alpha_{ij} P = d_{k\ell} P = \delta_{k,l} d_{kk} P.$$

در نتیجه $(F_kP)^\dagger(F_kP) = d_{kk}P$ و با در نظر گرفتن singular value decomposition عملگر F_kP نتیجه می‌گیریم که عملگر یکانی U_k وجود دارد به طوری که

$$F_kP = \sqrt{d_{kk}}U_kP.$$

قرار دهید $P_k := U_kPU_k^\dagger = \frac{1}{\sqrt{d_{kk}}}F_kPU_k^\dagger$. داریم

$$P_kP_\ell = P_k^\dagger P_\ell = \frac{1}{\sqrt{d_{kk}d_{\ell\ell}}}U_kPF_k^\dagger F_\ell PU_\ell^\dagger = \delta_{k,\ell}\frac{d_{kk}}{\sqrt{d_{kk}d_{\ell\ell}}}U_kPU_\ell^\dagger = \delta_{k,\ell}P_k.$$

پس P_kها عملگرهای تصویر دو به دو عمود بر هم هستند. لذا P_kها به همراه $P_0 = I - \sum_k P_k$ یک اندازه‌گیری تصویری تشکیل می‌دهند. در کدبرداری می‌خواهیم این اندازه‌گیری را به عنوان syndrome measurement در نظر بگیریم. در واقع ابتدا این اندازه‌گیری را انجام می‌دهیم، اگر حاصل اندازه‌گیری P_k شد برای تصحیح خطا عملگر $U_k^\dagger$ را اعمال می‌کنیم (در اینجا قرار می‌دهیم $U_0 = I$). در نتیجه نگاشت کوانتمی متناظر برابر است با

$$\mathcal{R}(\rho) = \sum_k U_k^\dagger P_k\rho P_kU_k.$$

واضح است که $\mathcal{R}$ یک نگاشت کاملاً مثبت و حافظ اثر است.

$$\begin{aligned}
\mathcal{R}\circ\mathcal{E}(P\rho P) &= \sum_k U_k^\dagger P_k\mathcal{E}(P\rho P)P_kU_k\\
&= \sum_{k,\ell} U_k^\dagger P_kF_\ell P\rho PF_\ell^\dagger P_kU_k\\
&= \sum_{k,\ell} d_{\ell\ell}U_k^\dagger P_kP_\ell U_\ell\rho U_\ell^\dagger P_\ell P_kU_k\\
&= \sum_k d_{kk}U_k^\dagger P_kU_k\rho U_k^\dagger P_kU_k\\
&= \sum_k d_{kk}P\rho P\\
&= \mathrm{tr}(\alpha)P\rho P\\
&= P\rho P.
\end{aligned}$$