

مدل مداری برای محاسبات کوانتومی

وحید کریمی پور- دانشکده فیزیک - دانشگاه صنعتی شریف

۲۷ آبان ۱۴۰۴

۱ مقدمه

گیت کوانتومی یک عملگر یکانی است که روی بردارهای دلخواه عمل می کند. اگر یک حافظه n کیوبیتی داشته باشیم فضای هیلبرت حالت های آن عبارت است از $\mathcal{H} = \mathcal{C}^{2^n}$ که در آن $\mathcal{C}^2$ یک فضای دوبعدی مختلط است. بعد این فضا برابر است با 2^n و یک گیت دلخواه یعنی یک عملگر یکانی که روی این فضای هیلبرت عمل کند. چنین عملگری با یک ماتریس مربعی $2^n \times 2^n$ نشان داده می شود که دارای تعداد 2^{2n} پارامتر است، زیرا ماتریس های یکانی $N \times N$ دارای N^2 پارامتر آزاد هستند. به عنوان مثال فضای گیت های تک کیوبیتی یک فضای 4 پارامتری و فضای گیت های دو کیوبیتی یک فضای 16 پارامتری و فضای گیت های 10 کیوبیتی یک فضای 1048576 پارامتری است. دقت کنید که این فضاها همه پیوسته هستند و بی نهایت نقطه دارند که هر نقطه آنها نشان دهنده یک عملگر یکانی است و تعداد پارامترهایی که شمردیم تنها تعداد پارامتر ها لازم برای برجسب زدن روی نقاط این فضاها را مشخص می کند. به این ترتیب فضای سه بعدی متعارف دکارتی در مقابل همه این فضاها کوچک است زیرا هر نقطه اش تنها با سه پارامتر مشخص می شود. به این ترتیب با اولین دشواری خود در نظریه و هم چنین ساخت کامپیوترهای کوانتومی مواجه می شویم. آیا می توان با یک مجموعه متناهی از گیت ها، آنچنانکه در کامپیوترهای کلاسیک انجام می شود، تمام گیت های ممکن را پیاده سازی کرد؟ اگر بتوان یک مجموعه متناهی مثل $G := \{G_1, G_2, \dots, G_K\}$ پیدا کرد که به کمک آنها بتوان تمام گیت های یکانی را پیاده سازی کرد، می گوییم مجموعه G یک مجموعه ی گیت های یونیورسال یا عام را تشکیل می دهد. در همین ابتدا باید دو نکته مهم را توضیح دهیم.

نکته اول: مسلم است که با یک مجموعه متناهی هرگز نمی توان یک مجموعه پیوسته از گیت ها را پیاده سازی کرد مگر اینکه خود را قانع به پیاده سازی تقریبی از گیت ها کنیم. بنابراین فرض کنید که حد دقتی که در نظر داریم برابر با ϵ باشد. در این صورت هرگاه بجای عملگر U ، با استفاده از گیت های عام خود عملگر $\tilde{U}$ را چنان بسازیم که شرط

$$E(U, \tilde{U}) := \max_{|\psi\rangle} \|(U - \tilde{U})|\psi\rangle\| < \epsilon \quad (1)$$

برقرار شود، می گوییم که گیت U را با دقت خوب (یعنی با دقت قابل قبول ϵ) پیاده سازی کرده ایم.

نکته دوم: در پیاده سازی گیت ها مهم است که چه تعداد گیت یونیورسال برای ساختن یک گیت دلخواه استفاده می کنیم و این تعداد چه نسبتی با n یعنی تعداد کیوبیت ها و هم چنین دقتی که می خواهیم به کار ببریم یعنی ϵ دارد. اگر مجبور شویم که برای بالابردن دقت خود و یا تعداد کیوبیت ها تعداد گیت های یونیورسالی را که به کار می بریم به طور نمایی افزایش دهیم، بازهم پروژه ساخت کامپیوترهای کوانتومی با شکست مواجه خواهد شد. خوشبختانه چنین نیست و این موضوع نیز از دلایلی است که ما را به ساختن کامپیوترهای کوانتومی امیدوار می کند.

۲ چند مثال ساده

در بخش آینده نشان خواهیم داد که چگونه به طور سیستماتیک می توان از یک مجموعه گیت های ابتدایی هر گیت دلخواه n کیوبیتی را ساخت. استدلالی که در بخش بعدی خواهد آمد یک استدلال کلی و وجودی است به این معنا که نشان می دهیم این کار علی الاصول امکان پذیر است. اما همواره لازم نیست که برای ساختن مدار از این روش استدلال بهره بجوییم چرا که در خیلی از موارد می توانیم با استفاده از شهود فیزیکی، تجربه عملی و یا روش های دیگر به سادگی مدار مورد نظر خود را بسازیم.

■ تمرین: یک مدار کوانتومی بسازید که حالت های $(|00\dots 0\rangle + |11\dots 1\rangle)$ را بسازد.

■ تمرین: یک مدار کوانتومی بسازید که از حالت ورودی $|00\rangle$

حالت

$$\cos \theta |00\rangle + \sin \theta |11\rangle$$

را بسازد. اگر ورودی مدار را به $i, j = 0, 1$ تغییر دهید چه حالت هایی ساخته خواهد شد.

■ تمرین: حالت زیر را در نظر بگیرید:

$$|W_n\rangle = \frac{1}{\sqrt{n}} (|100\cdots 0\rangle + |010\cdots 0\rangle + \cdots |000\cdots 1\rangle). \quad (۲)$$

رابطه بالا را می توان به شکل زیر نوشت:

$$|W_n\rangle = \frac{1}{\sqrt{n}} |1\rangle \otimes |000\cdots 0\rangle + \sqrt{\frac{n-1}{n}} |0\rangle \otimes |W_{n-1}\rangle. \quad (۳)$$

با استفاده از این رابطه تکرار مداری بسازید که بتواند حالت $|W_3\rangle$ را تولید کند. سپس مداری بسازید که بتواند حالت $|W_4\rangle$ را تولید کند.

■ تمرین: حالت زیر را در نظر بگیرید:

$$|\psi\rangle = \cos\theta \cos\phi |00\rangle + \cos\theta \sin\phi |01\rangle + \sin\theta |11\rangle. \quad (۴)$$

یک مدار کوانتومی بسازید که حالت بالا را از ورودی $|00\rangle$ تولید کند.

۳ یک مجموعه عملگرهای یونیورسال یا عام

در این بخش می خواهیم نشان دهیم که اگر بتوانیم عملگرهای دلخواه تک کیوبیتی و $CNOT$ را بسازیم آنگاه می توانیم هر عملگر چند کیوبیتی متعلق به $U(N)$ را بسازیم. دقت کنید که برای n کیوبیت بعد فضای هیلبرت برابر با $N = 2^n$ است در نتیجه عملگرهای n بیتی متعلق به $U(N) = U(2^n)$ هستند. در این نحوه ساخت فرض کرده ایم که هر عملگر تک کیوبیتی را می توانیم بسازیم. این البته فرض دور از ذهنی نیست، زیرا مثلاً اگر کیوبیت را اسپین یک هسته در نظر بگیریم می توانیم با تاباندن امواج با فرکانس رادیویی به طرز مناسب و عمل میدان مغناطیسی آنها روی اسپین هر نوع دورانی را روی اسپین انجام دهیم. اگر تنها یک مجموعه گسسته از عملگرهای تک کیوبیتی در اختیار داشته باشیم، آنگاه می توانیم با هر دقت دلخواهی عملگرهای تک کیوبیتی را بسازیم. استدلال ما از اینجا شروع می شود که نشان می دهیم هر عملگر یکانی n بیتی را می توانیم به حاصلضربی از عملگرهای ساده تر تجزیه کنیم. نخست احتیاج به یک تعریف داریم.

تعریف: فرض کنید که $\tilde{U}$ یک عملگر یکانی متعلق به $U(n)$ باشد که فقط یک زیر ماتریس 2×2 آن غیر بدیهی باشد، به این معنا که این عملگر فقط روی یک زیر فضای دوبعدی به صورت عملگر U عمل می کند و روی هر بردار دیگری خارج از این زیر فضا مثل عملگر واحد عمل می کند. در این صورت این عملگر یک عملگر دو ترازوی ^۱ خوانده می شود.

مثال: فرض کنید که $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. در این صورت ماتریس های زیر همگی عملگرهای دو ترازوی متعلق به $U(4)$ هستند:

$$\tilde{U}_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{pmatrix}. \quad (5)$$

$$\tilde{U}_2 = \begin{pmatrix} a & 0 & 0 & b \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ c & 0 & 0 & d \end{pmatrix}. \quad (6)$$

$$\tilde{U}_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & a & 0 & b \\ 0 & 0 & 1 & 0 \\ 0 & c & 0 & d \end{pmatrix}. \quad (7)$$

قضیه: هر عملگر یکانی $U \in U(n)$ را می توان به صورت حاصل ضرب عملگرهای یکانی دو ترازوی نوشت.

اثبات: ایده کلی اثبات این است که یک ماتریس یکانی دلخواه را همواره می توان با ضرب کردن ماتریس های یکانی و دو ترازوی مناسب از سمت چپ به شکل ماتریس واحد درآورد. این کار درواقع چیزی نیست جز فرایند تقلیل گاوس - جردان، با این تفاوت که این بار با ضرب

ماتریس های یکانی انجام می شود. اگر این ماتریس ها را $U_1, U_2, U_3, \dots$ بنامیم آنگاه معنای سخن بالا آن است که

$$U_K U_{K-1} \cdots U_2 U_1 U = I, \quad (۸)$$

که نتیجه اش این است که

$$U = U_1^{-1} U_2^{-1} \cdots U_K^{-1}. \quad (۹)$$

این ایده را با یک مثال ساده توضیح می دهیم. ماتریس یکانی U را به شکل زیر در نظر می گیریم:

$$U = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & k \end{pmatrix}. \quad (۱۰)$$

ماتریس U_1 می بایست طوری انتخاب شود که عنصر d را در این ماتریس صفر کند. بنابراین قرار می دهیم

$$U_1 = \begin{pmatrix} x & y & 0 \\ z & w & 0 \\ 0 & 0 & 1 \end{pmatrix}. \quad (۱۱)$$

که در آن $za + dw = 0$ و یا $z = -\kappa d$ و $w = \kappa a$. برای آنکه U_1 یکانی شود، x و y را به نحو مناسب انتخاب می کنیم و قرار می دهیم:

$$U_1 = \begin{pmatrix} \kappa a^* & \kappa d^* & 0 \\ -\kappa d & \kappa a & 0 \\ 0 & 0 & 1 \end{pmatrix}. \quad (۱۲)$$

که در آن $\kappa := \frac{1}{\sqrt{|a|^2 + |d|^2}}$. حال مطمئن هستیم که $U_1 U$ شکل زیر را دارد:

$$U_1 U = \begin{pmatrix} a' & b' & c' \\ 0 & e' & f' \\ g' & h' & k' \end{pmatrix}. \quad (۱۳)$$

به همین نحو می توان ماتریسی مثل U_2 یافت که شرط زیر حاصل شود. (به طور نمادین همه درایه های جدید را با علامت ' نشان می دهیم.)

$$U_2 U_1 U = \begin{pmatrix} a' & b' & c' \\ 0 & e' & f' \\ 0 & h' & k' \end{pmatrix}. \quad (۱۴)$$

یکانی بودن U الزام می کند که $a' = 1$ یک فاز خالص باشد و در نتیجه $b' = c' = 0$. این فاز خالص را می توان با ضرب یک ماتریس که تنها درایه 11 آن غیر صفر است از بین برد. بنابراین

$$U_3 U_2 U_1 U = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e' & f' \\ 0 & h' & k' \end{pmatrix}. \quad (۱۵)$$

اما ماتریس طرف راست چیزی نیست جز یک ماتریس یکانی دو ترازوی و در نتیجه با ضرب طرفین این رابطه در $U_1^{-1} U_2^{-1} U_3^{-1}$ ، U به صورت حاصلضربی از ماتریس های یکانی دو ترازوی در می آید. برای ماتریس های بزرگ تر این کار را می توان در صورت لزوم ادامه داد. در مرحله بعدی نشان می دهیم که هر عملگر دو ترازوی را می توان از عملگرهای کنترلی ساخت. ساده ترین عملگر کنترلی عملگر $CNOT$ است که به صورت زیر عمل می کند:

$$CNOT|x, y\rangle = |x, x \oplus y\rangle. \quad (۱۶)$$

بنابراین هرگاه مقدار x برابر با صفر باشد، عملگر $CNOT$ روی کیوبیت دوم مثل عملگر واحد عمل می کند و هرگاه مقدار $x = 1$ باشد روی کیوبیت دوم مثل X عمل می کند. به همین دلیل کیوبیت اول را بیت کنترل و بیت دوم را بیت هدف می نامیم. عملگرهای کنترلی دلخواه به صورت زیر تعریف می شوند.

تعریف: فرض کنید که U یک عملگر یکانی تک کیوبیتی باشد، در این صورت عملگر کنترلی $\Lambda^1(U)$ به شکل زیر تعریف می شود:

$$\Lambda^1(U)|x, y\rangle = |x\rangle \otimes U^x|y\rangle \quad (۱۷)$$

به عبارت دیگر عملگر U روی کیوبیت دوم تنها وقتی اثر می کند که مقدار x برابر با 1 باشد، در غیر این صورت روی کیوبیت دوم عملگر واحد عمل می کند. به این معناست که مقدار بیت x عملی را که قرار است روی کیوبیت دوم انجام شود تعیین می کند و $\Lambda^1(U)$ یک عملگر

کنترلی خوانده می شود.

مثال ۱: هرگاه $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ یک عملگر یکانی یک بیتی باشد، ماتریس های $\Lambda^1(U)$ و $\Lambda^2(U)$ چنین شکلی دارند:

$$\Lambda^1(U) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{pmatrix}. \quad (۱۸)$$

$$\Lambda^2(U) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & a & b \\ 0 & 0 & 0 & 0 & 0 & 0 & c & d \end{pmatrix}. \quad (۱۹)$$

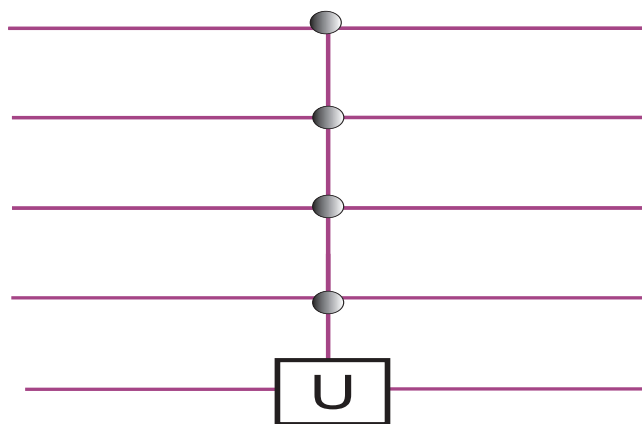
به همین ترتیب می توانیم عملگرهایی را تعریف کنیم که عمل آنها روی بیت $n + 1$ ام توسط n بیت اول تعیین شود:

$$\Lambda^n(U)|x_1, x_2, \dots, x_n, y\rangle = |x_1, x_2, \dots, x_n\rangle \otimes U^{x_1 x_2 \dots x_n} |y\rangle. \quad (۲۰)$$

شکل ۳ یک عملگر $\Lambda^4(U)$ را نشان می دهد.

مثال ۲: عملگر $CNOT = \Lambda^1(\sigma_x)$ یکی از مهم ترین عملگرهای کنترلی است. این عملگر به شکل زیر عمل می کند

$$\Lambda^1(\sigma_x)|x, y\rangle = |x, x \oplus y\rangle, \quad (۲۱)$$



شکل ۱: یک عملگر کنترلی $\Lambda^4(U)$.

و شکل ماتریسی آن عبارت است از:

$$CNOT = \Lambda^1(\sigma_x) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \quad (22)$$

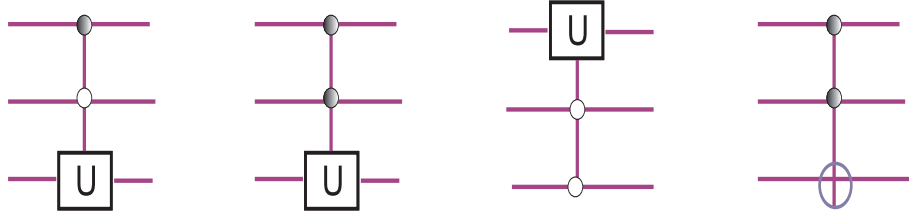
هم چنین داریم

$$\Lambda^2(\sigma_x)|x, y, z\rangle = |x, y, xy \oplus z\rangle. \quad (23)$$

یک نکته مهم: همه‌ی عملگرهای $\Lambda^n(\sigma_x)$ را بدلیل کاربرد وسیع آنها عملگر $CNOT$ می‌نامیم. این عملگرها و دیگر عملگرهای کنترلی به شکل استاندارد به گونه‌ای تعریف شده‌اند که بیت آخر آنها بیت هدف و $n - 1$ بیت اول آنها بیت‌های کنترل باشند. هم چنین این عملگرها تنها وقتی عمل می‌کنند که بیت‌های اول همگی برابر با صفر باشند. روشن است که انواع متفاوتی از عملگرهای کنترلی می‌توان تصور کرد که بیت‌های کنترلی آنها با هم متفاوت باشند. هم چنین الزامی ندارد که این عملگرها حتماً وقتی که بیت‌های کنترل برابر با صفر هستند، عمل کنند. برای اینکه تفاوت این عملگرها را در مدارها نشان دهیم روی بیت‌های کنترل یک دایره قرار می‌دهیم. دایره توپر به معنای این است که آن بیت می‌بایست مساوی ۱ باشد تا عملگر کار کند و دایره توخالی به معنای این است که آن بیت می‌بایست مساوی ۰ باشد تا عملگر کار کند. شکل زیر چند نوع از عملگرهای کنترلی را نشان می‌دهد. در شکل زیر عملگرهای نشان داده شده از چپ به راست به ترتیب زیر عمل می‌کند.

کنند:

$$|x, y, z\rangle \longrightarrow |x, y, U^{xy}z\rangle, \quad |x, y, z\rangle \longrightarrow |x, y, U^{xy}z\rangle, \quad |x, y, z\rangle \longrightarrow U^{\bar{y}\bar{z}}|x\rangle|y, z\rangle, \quad |x, y, z\rangle \longrightarrow |x, y, xy \oplus z\rangle.$$



شکل ۲: عملگرهای کنترلی که بیت کنترل آنها و نحوه عمل کردن آنها با هم متفاوت است.

قضیه: هر عملگر دو تراز $\tilde{U}$ روی n کیوبیت را می توان از عملگرهای کنترلی $CNOT$ و عملگر $\Lambda^{n-1}(U)$ ساخت.

اثبات روش ساخت را نشان می دهیم که با استفاده از آن خواننده می تواند ایده اصلی اثبات را دریابد. فرض کنید که عملگر $\tilde{U}$ روی زیرفضایی که با بردارهای $|g_0\rangle, |g_m\rangle$ جاروب می شود به طور غیر بدیهی عمل می کند. یک کد گری می نویسیم که رشته ی g_0 را به رشته g_m ربط دهد. بردارهای متناظر با این رشته را به صورت زیر نمایش می دهیم:

$$|g_0\rangle, |g_2\rangle |g_3\rangle \cdots |g_m\rangle. \quad (24)$$

به عنوان مثال اگر $|g_0\rangle = |00\rangle$ و $|g_2\rangle = |11\rangle$ می نویسیم

$$|g_0\rangle = |00\rangle, \quad |g_1\rangle = |01\rangle, \quad |g_2\rangle = |11\rangle, \quad (25)$$

یا اگر $|g_0\rangle = |000\rangle$ و $|g_3\rangle = |111\rangle$ می نویسیم

$$|g_0\rangle = |000\rangle, \quad |g_1\rangle = |001\rangle, \quad |g_2\rangle = |011\rangle, \quad |g_3\rangle = |111\rangle. \quad (26)$$

حال رشته ای از عملگرهای تعمیم یافته ی $CNOT$ در نظر می گیریم که حالت $|g_0\rangle$ را به $|g_1\rangle$ ، حالت $|g_1\rangle$ را به $|g_2\rangle$ و بالاخره حالت $|g_{m-1}\rangle$ را به حالت $|g_m\rangle$ تبدیل کنند. این عملگرها را به ترتیب با $C_0, C_1, \dots, C_{m-1}$ نشان می دهیم. اثر این رشته عملگر روی حالت $|g_0\rangle$ حالت $|g_{m-1}\rangle$ را تولید می کنند. سپس یک عملگر کنترلی $\Lambda^{n-1}(U)$ اعمال می کنیم که بیت های کنترلی اش همه بیت های مشترک بین $|g_{m-1}\rangle$

و $|g_m\rangle$ باشد. پس از آن عملگرهای C_0, C_1 تا C_{m-1} را به ترتیب معکوس اعمال می کنیم. به عبارت دیگر عملگر زیر را می سازیم

$$\tilde{U} := C_0 \cdots C_{m-2} C_{m-1} \Lambda^{n-1}(U) C_{m-1} C_{m-2} \cdots C_0 \quad (27)$$

این عملگر تنها روی زیر فضای ساخته شده از $|g_0\rangle$ و $|g_m\rangle$ به طور غیر بدیهی عمل می کند.

مثال ۳ فرض کنید که

$$\tilde{U} := \begin{pmatrix} a & 0 & 0 & b \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ c & 0 & 0 & d \end{pmatrix} \quad (28)$$

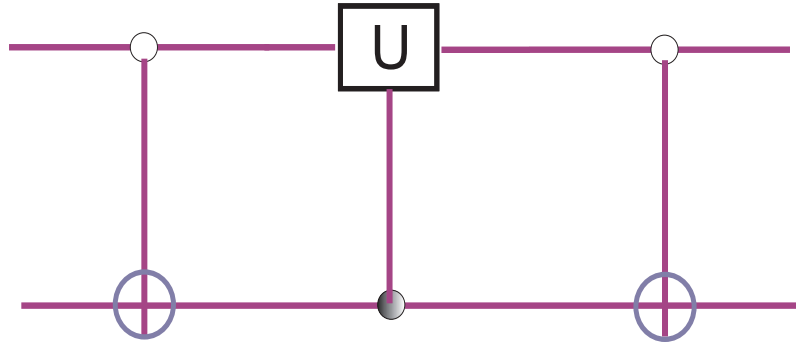
این عملگر روی زیر فضای $|g_0\rangle = |00\rangle$ و $|g_2\rangle := |11\rangle$ به صورت غیر بدیهی عمل می کند. در مثال ۱ یک کد گری برای این دو حالت نوشته شده است. عملگر C_0 می بایست حالت $|g_0\rangle = |00\rangle$ را به حالت $|g_1\rangle = |01\rangle$ تبدیل کند. بنابراین C_0 یک عملگر $CNOT$ است که بیت اول اش کنترلی و بیت دوم اش هدف است و وقتی عمل می کند که بیت کنترلی اش برابر با صفر باشد. عملگر $\Lambda^1(U)$ نیز بیت دوم اش کنترلی است و وقتی عمل می کند که این بیت برابر با ۱ باشد. بنابراین داریم

$$\tilde{U} = C_0 \Lambda^1(U) C_0. \quad (29)$$

مداری که این عملگر را پیاده سازی می کند در شکل ۳ نشان داده شده است. با دنبال کردن این مدار از چپ به راست خواننده می تواند تحقیق کند که این عملگر تنها حالت های $|00\rangle$ و $|11\rangle$ را به هم تبدیل می کند: درواقع داریم

$$\begin{aligned} |00\rangle &\longrightarrow |01\rangle \longrightarrow a|01\rangle + c|11\rangle \longrightarrow a|00\rangle + c|11\rangle \\ |01\rangle &\longrightarrow |00\rangle \longrightarrow |00\rangle \longrightarrow |01\rangle \\ |10\rangle &\longrightarrow |10\rangle \longrightarrow |10\rangle \longrightarrow |10\rangle \\ |11\rangle &\longrightarrow |11\rangle \longrightarrow b|01\rangle + d|11\rangle \longrightarrow b|00\rangle + d|11\rangle. \end{aligned} \quad (30)$$

تا کنون نشان داده ایم که تمام عملگرهای n کیوبیتی را می توانیم از ترکیب عملگرهای کنترلی n بیتی ساخت. درتجزیه ای که از عملگرهای دلخواه در پیش داریم، قضیه زیر ما را یک قدم جلوتر می برد.



شکل ۳: نحوه ساختن عملگرهای دوترازی با استفاده از عملگرهای کنترلی. مثال ۳.

قضیه: تمام عملگرهای کنترلی n بیتی را می توان از عملگرهای کنترلی یک بیتی ساخت.

اثبات: برای سادگی نخست نشان می دهیم که تمام عملگرهای کنترلی دو بیتی را می توان از عملگرهای کنترلی یک بیتی ساخت. فرض کنید می خواهیم عملگر $\Lambda^2(U)$ را بسازیم. می دانیم که عملگر U یکانی است و بنابراین جذر آن وجود دارد. قرار می دهیم $V := U^{\frac{1}{2}}$. حال از این رابطه استفاده می کنیم که

$$x \oplus y = x + y - 2xy \quad (31)$$

و آن را به صورت زیر می نویسم

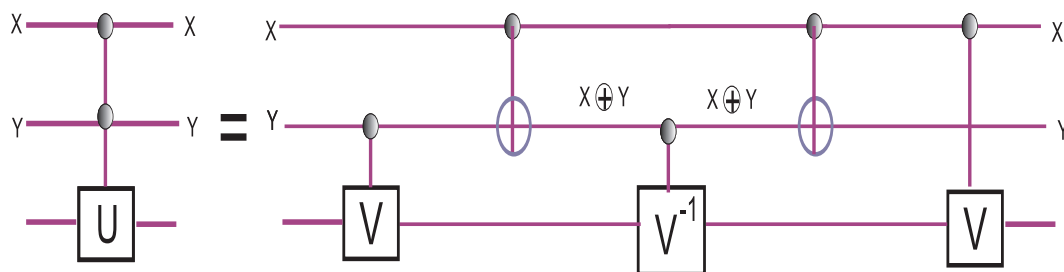
$$2xy = x + y - x \oplus y. \quad (32)$$

در نتیجه می نویسیم

$$U^{xy} = V^{2xy} = V^{x+y-x \oplus y} = V^x V^{-1^{x \oplus y}} V^y \quad (33)$$

می دانیم که بیت $x \oplus y$ خود توسط یک عملگر کنترلی یک بیتی ایجاد می شود. بنابراین رابطه فوق نشان می دهد که عملگر کنترلی دو بیتی $\Lambda^2(U)$ به صورت حاصلضربی از عملگرهای کنترلی یک بیتی ساخته شده است. مدار شکل 4 چگونگی ترکیب این عملگرها را نشان می دهد. این روش به همین ترتیب به عملگرهای کنترلی چند بیتی نیز تعمیم داده می شود. نکته مهم در اثبات تمام این قضیه اتحاد های زیراست:

$$2xy = x + y - x \oplus y$$



شکل ۴: چگونگی ساخت یک عملگر کنترلی دو بیتی از عملگرهای کنترلی یک بیتی.

$$4xyz = x + y + z - (x \oplus y) - (y \oplus z) - (x \oplus z) + x \oplus y \oplus z$$

$$\dots = \dots$$

$$2^{n-1}x_1x_2\cdots x_n = \sum_i x_i - \sum_{i<j} x_i \oplus x_j + \sum_{i<j<k} x_i \oplus x_j \oplus x_k \cdots \pm x_1 \oplus x_2 \oplus \cdots x_n. \quad (34)$$

به عنوان مثال برای ساختن یک عملگر کنترلی ۳ کیوبیتی از اتحاد دوم استفاده می کنیم و می نویسیم

$$U^{xyz} = V^4xyz = V^{x+y+z-(x\oplus y)-(y\oplus z)-(x\oplus z)+x\oplus y\oplus z} \quad (35)$$

که در آن $V^4 = U$. در نتیجه در طرف راست تنها عملگرهای کنترلی ای داریم که یک بیت کنترل کننده ی آنهاست. این بیت البته ممکن است به صورت یک بیت از نوع $x \oplus y$ باشد ولی می دانیم که چگونه با استفاده از عملگرهای $CNOT$ که خود یک عملگر کنترلی یک بیتی است چنین بیت هایی را ایجاد کنیم. برای آنکه به تعداد کمتری از عملگرهای $CNOT$ استفاده کنیم می بایست طرف راست تساوی 35 طوری بسط دهیم که توان هر عملگر با عملگر قبلی اش تنها در یک بیت اختلاف داشته باشد. یعنی باید بنویسیم

$$U^{xyz} = V^x V^{-1x\oplus y} V^y V^{-1y\oplus z} V^{x\oplus y\oplus z} V^{-1x\oplus z} V^z \quad (36)$$

این نحوه مرتب کردن به معنای آن است که ما در نوشتن ترتیب جملات طرف راست در تساوی 35 از کد گری $Gray Code$ استفاده می کنیم، که یک نمونه از آن در جدول 3 نشان داده شده است.

سوالی که با آن مواجه هستیم آن است که چگونه عملگرهای کنترلی یک بیتی را بسازیم. در زیر نشان می دهیم که تنها کافی است یک عملگر

	x	y	z
	0	0	0
x	1	0	0
$x \oplus y$	1	1	0
y	0	1	0
$y \oplus z$	0	1	1
$x \oplus y \oplus z$	1	1	1
$x \oplus z$	1	0	1
z	0	0	1

جدول ۱: کد گری برای سه متغیر

کنترلی یک بیتی یعنی $CNOT$ را بسازیم، زیرا به کمک آن می توانیم تمام عملگرهای کنترلی یک بیتی دیگر را بسازیم. دقت کنید که در آزمایشگاه ساختن یک عملگر مثل $CNOT$ بخودی خود دشوار است، زیرا عمل این عملگر بستگی به مقدار کیوبیت هدف آن دارد و این کار را بدون اینکه هیچ نوع اندازه گیری روی کیوبیت اول انجام دهد می بایست انجام دهد. گزارش هایی که از گروه های تجربی در مورد ساختن عملگر $CNOT$ و عملگرهای نزدیک به آن منتشر شده است، جزء پیشرفت های مهم تجربی در زمینه ساخت کامپیوترهای کوانتومی محسوب می شود. این موضوع نشان می دهد که اولاً ساختن عملگرهای کنترلی از نظر تجربی تا چه اندازه دشوار است، ثانیاً ساختن عملگر $CNOT$ تا چه اندازه اهمیت دارد. دلیل این اهمیت این است که همه عملگرهای کنترلی تک کیوبیتی را می توان با ترکیب عملگر $CNOT$ و عملگرهای یک کیوبیتی معمولی ساخت. برای اثبات این قضیه احتیاج به یک لم داریم. می دانیم که هر عملگر تک کیوبیتی ماتریسی است متعلق به گروه $U(2)$ که می توان آن را به صورت $e^{i\phi}W$ نوشت که در آن W یک ماتریس متعلق به گروه $SU(2)$ است، یعنی دترمینان اش برابر با یک است و بنابراین نشان دهنده یک دوران است. فعلاً توجه خود را به همین ماتریس معطوف می کنیم و یک لم را ثابت می کنیم.

لم: برای هر ماتریس یکانی $W \in SU(2)$ می توان ماتریس های یکانی A ، B و C را چنان یافت که در شرایط زیر صدق کنند:

$$\begin{aligned}
 ABC &= I \\
 A\sigma_x B\sigma_x C &= W.
 \end{aligned}
 \tag{۳۷}$$

اثبات: می دانیم که عملگر W را می توان به شکل زیر نوشت:

$$W = R_z(\alpha)R_y(\theta)R_z(\beta). \quad (۳۸)$$

با توجه به شرایط یاد شده می خواهیم W را به شکل زیر بنویسیم

$$W = A\sigma_x B\sigma_x B^{-1}A^{-1}. \quad (۳۹)$$

ضرایب α و β را به شکل زیر بازتعریف می کنیم:

$$\alpha = \frac{\gamma + \delta}{2} \quad \beta = \frac{\gamma - \delta}{2} \quad (۴۰)$$

بنابراین W برابر خواهد بود با:

$$R_z\left(\frac{\gamma + \delta}{2}\right)R_y(\theta)R_z\left(\frac{\gamma - \delta}{2}\right). \quad (۴۱)$$

مقایسه 39 و 41 نشان می دهد که عملگر A را می بایست به شکل زیر در نظر گرفت:

$$A = R_z\left(\frac{\delta}{2}\right) \quad (۴۲)$$

و در نتیجه

$$R_z\left(\frac{\gamma}{2}\right)R_y(\theta)R_z\left(\frac{\gamma}{2}\right) = \sigma_x B\sigma_x B^{-1}. \quad (۴۳)$$

ماتریس B را به شکل زیر می نویسم:

$$B = R_z(\xi)R_y(\theta_1). \quad (۴۴)$$

جایگذاری این رابطه در رابطه بالا منجر می شود به:

$$\begin{aligned} R_z\left(\frac{\gamma}{2}\right)R_y(\theta)R_z\left(\frac{\gamma}{2}\right) &= \sigma_x B\sigma_x B^{-1} \\ &= \sigma_x R_z(\xi)R_y(\theta_1)\sigma_x R_y(-\theta_1)R_z(-\xi) \end{aligned}$$

$$= R_z(-\xi)R_y(-2\theta_1)R_z(-\xi). \quad (45)$$

مقایسه دو طرف این رابطه نشان می دهد که

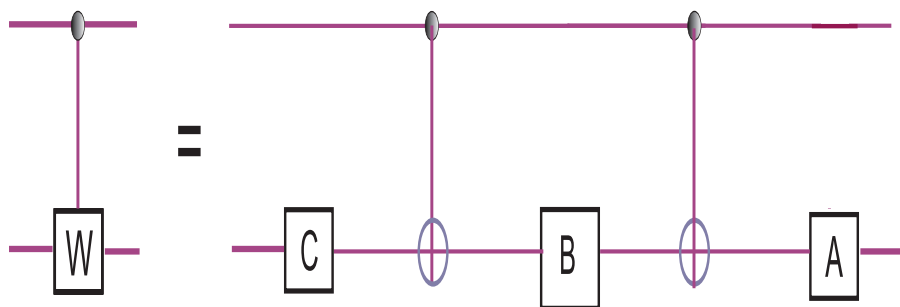
$$\xi = -\frac{\gamma}{2}, \quad \theta = -2\theta_1. \quad (46)$$

بنابراین بدست می آوریم:

$$A = R_z\left(\frac{\alpha - \beta}{2}\right) \quad B = R_z\left(\frac{-\alpha - \beta}{2}\right)R_y\left(-\frac{\theta}{2}\right), \quad C = R_y\left(\frac{\theta}{2}\right)R_z(\beta). \quad (47)$$

می توان دراین جا تحقیق کرد که روابط 37 برقرار هستند.

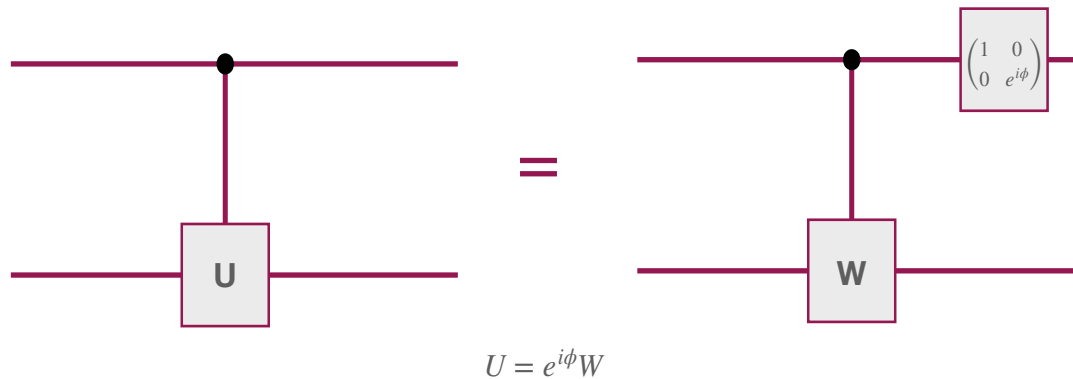
نتیجه هر عملگر یکانی $U \in U(2)$ را می توان به شکل $U = e^{i\phi} A\sigma_x B\sigma_x C$ نوشت که در آن A ، B و C عملگرهای یکانی هستند که در شرط $ABC = I$ صدق می کنند.



چگونگی ساخت عملگرهای کنترلی یک بیتی با استفاده از عملگر CNOT و عملگرهای یک بیتی معمولی، ترتیب عمل کردن عملگر ها از چپ به راست است.

لم ای که ثابت کردیم و شکل بالا نشان می دهد که چگونه می بایست عملگرهای یک کیوبیتی را با CNOT ترکیب کرد تا بتوان هر عملگر

کنترلی یک کیوبیتی $\Lambda^1(W \in SU(2))$ را ساخت. با اضافه کردن یک گیت ساده می توانیم هر عملگر کنترلی یک کیوبیتی $\Lambda^1(U \in SU(2))$ را بسازیم. مدار نشان داده شده در شکل (۳) نشان می دهد که چگونه این کار انجام می شود.



شکل ۶: چگونگی ساختن یک گیت کنترلی $\Lambda^1(U \in U(2))$ از یک گیت کنترلی $\Lambda^1(W \in SU(2))$.

بنابراین نشان داده ایم که هرگاه عملگرهای یک کیوبیتی دلخواه و هم چنین عملگر $CNOT$ را بسازیم با ترکیب آنها می توانیم هر عملگر دلخواه متعلق به $U(N = 2^n)$ را بسازیم. اما می توان از این هم فراتر رفت و نشان داد که می توان تنها با استفاده از دو نوع خاص از عملگرهای یک کیوبیتی به هدف بالا نائل شد. البته در این صورت چون از یک مجموعه عملگرهای گسسته استفاده می کنیم ساخت عملگرهای دلخواه به صورت تقریبی ممکن خواهد بود. اما می توان با افزایش تعداد عملگرها به هر دقتی که می خواهیم برسیم.

۴ مجموعه متناهی از گیت های یونیورسال

برای تولید عملگرهای یکانی با دقت دلخواه می توانیم از یک مجموعه متناهی از گیت های تک کیوبیتی و دو کیوبیتی استفاده کنیم. برای این مجموعه انتخاب یکتایی وجود ندارد. علاوه بر ملاحظات تجربی و سخت افزاری، ملاحظات دیگری هم برای انتخاب این مجموعه وجود دارد. در زیر به چند انتخاب معمول برای این مجموعه گیت اشاره می کنیم.

■ یک : مجموعه گیت های

$$\{R_y, R_z, CNOT\}$$

که در آن R_n دوران حول محور n به اندازه زاویه دلخواه است. برای نشان دادن این که این مجموعه یونیورسال است، باید نشان دهیم که هر عملگر یکانی تک-کیوبیتی را می توان از R_y و R_z ساخت. دقت کنید که منظور از این دو گیت، دوران های حول محوره های مربوطه به اندازه زاویه دلخواه است. بنابراین واقعا این مجموعه را نمی توان یک مجموعه متناهی نامید. برای این کار به یک قضیه ساده احتیاج داریم:

قضیه: تجزیه XYZ از یک عملگر یکانی یک بیتی فرض کنید که U یک عملگریکانی دلخواه تک کیوبیتی است. در این صورت اعداد حقیقی $\alpha, \beta, \gamma, \delta$ وجود دارند به قسمی که:

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta). \quad (48)$$

اثبات: چون U یکانی است می توان نوشت $U = e^{i\alpha} V$ که در آن $V \in SU(2)$. اما ماتریس های $SU(2)$ یک شکل استاندارد دارند به این معنا که

$$V = \begin{pmatrix} a & b \\ -b^* & a^* \end{pmatrix} \quad (49)$$

که در آن $|a|^2 + |b|^2 = 1$. بنابراین

$$a = e^{i\theta} \cos \frac{\gamma}{2}, \quad b := e^{i\phi} \sin \frac{\gamma}{2}. \quad (50)$$

و در نتیجه

$$V = \begin{pmatrix} e^{i\theta} \cos \frac{\gamma}{2} & e^{i\phi} \sin \frac{\gamma}{2} \\ -e^{-i\phi} \sin \frac{\gamma}{2} & e^{-i\theta} \cos \frac{\gamma}{2} \end{pmatrix} \quad (51)$$

از طرفی می دانیم که

$$V = R_z(\beta)R_y(\gamma)R_z(\delta) = \begin{pmatrix} e^{i\frac{\beta}{2}} & 0 \\ 0 & e^{-i\frac{\beta}{2}} \end{pmatrix} \begin{pmatrix} \cos \frac{\gamma}{2} & \sin \frac{\gamma}{2} \\ -\sin \frac{\gamma}{2} & \cos \frac{\gamma}{2} \end{pmatrix} \begin{pmatrix} e^{i\frac{\delta}{2}} & 0 \\ 0 & e^{i\frac{-\delta}{2}} \end{pmatrix} \quad (52)$$

مقایسه این رابطه با رابطه قبلی نشان می دهد که

$$\theta = \frac{\beta + \delta}{2}, \quad \phi = \frac{\beta - \delta}{2}. \quad (53)$$

به این ترتیب قضیه ثابت می شود.

■ دو: مجموعه گیت های

$$\{R_x, R_z, CNOT\}$$

که در آن به جای دوران های دلخواه حول محور y را با دوران حول محور x جایگزین کرده ایم. دلیل این امر هم این است که می توان یک عملگر یکانی را به صورت های مختلف به دوران های حول محورهای سه گانه تجزیه کرد. به عنوان مثال رابطه 48 موسوم به تجزیه ZYZ را در نظر بگیرید. می دانیم که عملگردوران $R_z(\frac{-\pi}{2})$ محور x را به محور y تبدیل می کند. به عبارت دیگر

$$R_z(\frac{-\pi}{2})(x \cdot \sigma)R_z(\frac{\pi}{2}) = (y \cdot \sigma), \quad (54)$$

که از آن نتیجه می گیریم

$$R_z(\frac{-\pi}{2})R_x(\gamma)R_z(\frac{\pi}{2}) = R_y(\gamma). \quad (55)$$

به این ترتیب با در دست داشتن دوران های دلخواه حول هر کدام از محورهای سه گانه عمود بر هم برای ساختن گیت های تک کیوبیتی کافی است.

مجموعه گیت هایی که تا کنون نوشتیم، واقعا مجموعه ای متناهی نیستند، چرا که دوران های حول محورها می بایست به اندازه دلخواه می بودند. حال یک مجموعه واقعا متناهی سه تایی را معرفی می کنیم. طبیعتا این مجموعه به دلیل متناهی بودن، نمی تواند هر گیت یکانی دلخواه را بسازد، اما می تواند با هر تقریب دلخواهی به آن گیت نزدیک شود و تعداد دفعاتی نیز که از این مجموعه متناهی برای این تقریب های بهتر استفاده میشود، بنابر قضیه سولوی - کیتایف به آرامی رشد می کند.

■ سه: مجموعه گیت های

$$\{H, T, CNOT\}$$

که در آن H گیت هادامارد، و T گیت زیر است که به آن گیت $\frac{\pi}{8}$ نیز گفته می شود:

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix} = e^{i\frac{\pi}{8}} \begin{pmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{pmatrix}. \quad (56)$$

دقت کنید که با این گیت می توان به طریق زیر گیت های تک کیوبیتی را ساخت:

$$T^2 = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad T^4 = Z, \quad HTH \equiv e^{i\frac{\pi}{8}} \begin{pmatrix} \cos \frac{\pi}{8} & \sin \frac{\pi}{8} \\ \sin \frac{\pi}{8} & \cos \frac{\pi}{8} \end{pmatrix} \equiv \cos \frac{\pi}{8} I + i \sin \frac{\pi}{8} X. \quad (57)$$

آخرین رابطه نشان می دهد که

$$HTH = R_x\left(\frac{\pi}{8}\right)$$

یک دوران حول محور x به اندازه زاویه $\frac{\pi}{8}$ است.

حال دو عملگر T و HTH را در نظر می گیریم. حاصلضرب این دو عملگر منهای یک فاز کلی برابر است با:

$$\begin{aligned} T(HTH) &\equiv R_z(-\pi/4)R_x(-\pi/4) = (\cos \frac{\pi}{8} - i \sin \frac{\pi}{8} Z)(\cos \frac{\pi}{8} - i \sin \frac{\pi}{8} Y) \\ &= \cos^2 \frac{\pi}{8} - i \left[\cos \frac{\pi}{8} \sin \frac{\pi}{8} X + \sin^2 \frac{\pi}{8} Y + \cos \frac{\pi}{8} \sin \frac{\pi}{8} Z \right] \end{aligned} \quad (58)$$

این عملگر بازهم یک عملگر دوران است که می توان آن را به شکل زیر نوشت:

$$Q := THTH = R_{\mathbf{n}}(\phi), \quad (59)$$

که در آن $\mathbf{n}$ بردار یکه ای است در امتداد بردار زیر:

$$\mathbf{n} = \left(\cos \frac{\pi}{8}, \sin \frac{\pi}{8}, \cos \frac{\pi}{8} \right) \quad (60)$$

و زاویه دوران θ از رابطه زیر بدست می آید:

$$\cos \phi = \cos^2 \frac{\pi}{8}. \quad (61)$$

می توان نشان داد که $\frac{\phi}{2\pi}$ یک عدد گنگ است. در نتیجه عملگرهای $Q^m = R_n(m\phi)$ که در آن m یک عدد صحیح است مجموعه تمام دوران های حول محور n را پوشش می دهند. اصطلاحاً گفته می شود که توان های این عملگر در مجموعه تمام دوران های حول محور n یک زیر مجموعه چگال تشکیل می دهند. اما هنوز این عملگرها در مجموعه تمام دوران ها چگال نیستند، زیرا محور آنها ثابت است. برای پوشش دادن تمام عملگرها احتیاج داریم که محور جدیدی برای دوران درست کنیم. برای این کار عملگر هادامارد را روی عملگر Q اثر می دهیم و بدست می آوریم:

$$S := HQH = R_m(\theta), \quad (۶۲)$$

که در آن $m = (\cos \frac{\pi}{8}, -\sin \frac{\pi}{8}, \cos \frac{\pi}{8})$. بردارهای m و n دو بردار غیر متعامد هستند و می توان نشان داد که با دوران های متناوب حول آنها هر دوران دلخواه بدست می آید. کامل کردن این قضیه را به عنوان تمرین به عهده خواننده می گذاریم.

۵ مفهوم دقت در گیت های کوانتومی

در این بخش می خواهیم مفهوم عملی رابطه 1 را بفهمیم. فرض کنید که قرار است روی حالت اولیه $|\psi\rangle$ ، گیت U اثر کند و حالت $|\phi\rangle$ تولید شود ولی اشتباهاً یا به خاطر عدم دقتی که ما در ساخت گیت های کوانتومی داریم گیت $\tilde{U}$ روی این حالت اثر می کند و حالت $|\tilde{\phi}\rangle$ تولید می شود. در این صورت می خواهیم ببینیم که نتایج اندازه گیری روی حالت های $|\phi\rangle$ و $|\tilde{\phi}\rangle$ جقدر با هم تفاوت دارند. به هر حال آنچه که نهایتاً مهم است، نتایج آماری ای است که از اندازه گیری روی این حالت ها بدست می آید. در این بخش نخست به این مسئله می پردازیم و نشان می دهیم که اختلاف نتایج اندازه گیری رابطه مستقیمی با فاصله یکانی های U و $\tilde{U}$ دارد.

فرض کنید که E یک عملگر $POVM$ باشد که مربوط به یک نتیجه (یا خروجی) خاص باشد. در این صورت احتمال مشاهده این نتیجه خاص را برای دو حالت باهم مقایسه می کنیم. داریم

$$P = \langle \phi | E | \phi \rangle = \langle \psi | U^\dagger E U | \psi \rangle, \quad \tilde{P} = \langle \tilde{\phi} | E | \tilde{\phi} \rangle = \langle \psi | \tilde{U}^\dagger E \tilde{U} | \psi \rangle. \quad (۶۳)$$

بنابراین

$$|\tilde{P} - P| = |\langle \tilde{\phi} | E | \tilde{\phi} \rangle - \langle \phi | E | \phi \rangle|. \quad (۶۴)$$

حال طرف راست این عبارت را به شکل زیر بازنویسی می کنیم:

$$|\tilde{P} - P| = |\langle \tilde{\phi} | E | \tilde{\phi} \rangle - \langle \phi | E | \tilde{\phi} \rangle + \langle \phi | E | \tilde{\phi} \rangle - \langle \phi | E | \phi \rangle|. \quad (۶۵)$$

با تعریف $|\chi\rangle := |\tilde{\phi}\rangle - |\phi\rangle$ ، رابطه قبلی به صورت زیر در می آید:

$$|\tilde{P} - P| = |\langle \chi | E | \tilde{\phi} \rangle + \langle \phi | E | \chi \rangle|. \quad (۶۶)$$

حال با استفاده از نامساوی کوشی-شوارتز و توجه به اینکه اندازه $|\phi\rangle$ و $|\tilde{\phi}\rangle$ برابر با یک است، بدست می آوریم:

$$|\tilde{P} - P| \leq 2\|E|\chi\rangle\|.$$

با توجه به این که E یک عملگر مثبت با نرم کوچکتر از یک است، نتیجه نهایی این است که :

$$|\tilde{P} - P| \leq 2\|\chi\| = 2\|\tilde{\phi} - \phi\| = 2\|(\tilde{U} - U)|\psi\rangle\| \leq 2\|\tilde{U} - U\|. \quad (۶۷)$$

بنابراین اگر فاصله $\|\tilde{U} - U\|$ از ϵ کمتر باشد، این امر به این معناست که نتایج همه اندازه گیری های ممکن که روی یک حالت دلخواه $|\psi\rangle$ انجام می دهیم حداکثر به اندازه 2ϵ دچار خطا می شود. این رابطه نشان می دهد که رابطه مستقیمی بین خطای اعمال گیت ها و نتایج آزمایشگاهی حاصل از آن ها وجود دارد.

حال به قسمت دوم بحث خود می پردازیم. یعنی می خواهیم بدانیم که خطاهای متوالی در اعمال گیت های کوانتومی چگونه روی هم انباشته می شوند. حالت دلخواه ما آن است که خطای انباشته شده متناسب با تعداد گیت ها باشد و نه بیشتر از آن و این همان چیزی است که نشان خواهیم داد.

۱.۵ انباشته شدن خطاها در گیت های متوالی

طبیعی است که با تعداد گسسته ای از گیت های کوانتومی تک کیوبیتی بعلاوه یک گیت $CNOT$ نمی توان هر گیت دلخواهی را ساخت. اما شاید بتوان به اندازه کافی به هر گیت دلخواهی که می خواهیم بسازیم نزدیک شویم. در این بخش نشان می دهیم که این کار به صورت کارآمدی

^۲ امکان پذیر است. منظور از کارآمد بودن هم این است که تعداد گیت هایی که باید برای رسیدن به یک دقت مورد نظر به کار ببریم به صورت نمایی با افزایش دقت زیاد نمی شود. نخست اندازه یک عملگر را تعریف می کنیم:

■ **تعریف:** هرگاه U یک عملگر دلخواه باشد، اندازه این عملگر به شکل زیر تعریف می شود:

$$\|U\| := \sup_{|\psi\rangle} \|U|\psi\rangle\|, \quad (۶۸)$$

که در آن ماکزیمم روی تمام حالت های بهنجار صورت می گیرد. این رابطه تمام خواص اندازه را دارد به این معنا که:

$$\begin{aligned} \|A\| &\geq 0, \quad \|A\| = 0 \leftrightarrow A = 0, \\ \|cA\| &= |c|\|A\|, \\ \|A + B\| &\leq \|A\| + \|B\|. \end{aligned} \quad (۶۹)$$

علاوه براین، اندازه تعریف شده یک خاصیت مهم دیگر هم دارد که دیگر تعریف های اندازه فاقد آنند و آن اینکه:

$$\|AB\| \leq \|A\|\|B\|. \quad (۷۰)$$

به عنوان یک تمرین ساده این خاصیت را ثابت کنید. هم چنین برای عملگرهای یکانی واضح است که؛

$$\|U\| = 1. \quad (۷۱)$$

با این تعریف از اندازه یک عملگر می توانیم یک نوع فاصله نیز بین دو عملگر به صورت زیر تعریف کنیم:

$$d(A, B) := \|A - B\|. \quad (۷۲)$$

حال فرض کنید که در ساختن گیت U به دلیل نقص ها و نویزهای موجود در محیط گیت V اشتباهات گیت U در نزدیکی آن ساخته می شود، یعنی

$$d(U, V) \leq \epsilon. \quad (۷۳)$$

می خواهیم ببینیم که اگر یک مدار کوانتومی نیازمند ساختن رشته ای از گیت ها باشد، خطاهای ساخته شده در گیت ها چگونه در گیت نهایی انباشته می شود. یعنی اگر بخواهیم یک مدار بزرگ برای ساختن یک گیت $\Omega = U_1 U_2 U_3 \dots U_n$ بسازیم و در ساختن هر گیت

^۲ efficient

U_i به اندازه ϵ_i خطا داشته باشیم، خطای گیت نهایی چقدر خواهد بود. برای پاسخ به این سوال حالت ساده $n = 2$ را در نظر بگیرید. داریم:

$$\begin{aligned} d(\Omega, \Omega') &= d(U_1 U_2, V_1 V_2) = \|U_1 U_2 - V_1 V_2\| = \|U_1 U_2 - U_1 V_2 + U_1 V_2 - V_1 V_2\| \\ &\leq \|U_1 U_2 - U_1 V_2\| + \|U_1 V_2 - V_1 V_2\| = \|U_1(U_2 - V_2)\| + \|(U_1 - V_1)V_2\| \\ &\leq \|(U_2 - V_2)\| + \|(U_1 - V_1)\| = d(U_1, V_1) + d(U_2, V_2), \end{aligned} \quad (۷۴)$$

که در خط آخر از خواص (۷۰) و (۷۱) استفاده کرده ایم. این استدلال را می توانیم برای n دلخواه تکرار کنیم که نتیجه آن این خواهد بود که

$$d(U_1 U_2 U_3 \cdots U_n, V_1 V_2 V_3 \cdots V_n) \leq \sum_i d(U_i, V_i). \quad (۷۵)$$

بنابراین اگر در هر کدام از گیت های مقدماتی دچار خطای ϵ شویم، در مدار نهایی دچار خطای $n\epsilon$ خواهیم شد که نشان می دهد خطا به صورت خطی و قابل کنترل افزایش می یابد.

بحث ما در مورد نحوه ساختن عملگرهای دلخواه از یک مجموعه یونیورسال در این جا به پایان می رسد. این درس را می بایست با یک سوال مهم و پاسخ آن به انتها ببریم. سوال این است که اگر بخواهیم یک عملگریکانی تک کیوبیتی را با دقت ϵ بسازیم و تنها یک مجموعه ثابت (مثل دو عملگر Q, S) در اختیار داشته باشیم، کوچکتر کردن ϵ به چه صورت تعداد گیت های مورد استفاده (یعنی تعداد گیت های Q, S را در مثال فوق) افزایش می دهد. اگر این تعداد به صورت نمایی زیاد شود معنایش این است که ساختن دقیق عملگرها کاری است عملاً غیر ممکن. قضیه *Kitaev – Solovay* که آن را بدون اثبات ذکر می کنیم، پاسخی بسیار امیدوار کننده به این سوال است.

■ قضیه سولوی – کیتائف: ۳

هرگاه از یک مجموعه ثابت از گیت های یک کیوبیتی بخواهیم یک عملگریکانی یک کیوبیتی را با دقت ϵ بسازیم، تعداد گیت های مورد نیاز به صورت $O([\log(\frac{1}{\epsilon})]^c)$ افزایش می یابد که در آن c عددی نزدیک به ۲ است و O نشان دهنده مرتبه است.

■ **یک نکته:** آنچه که در این درس در مورد ساخت مدارهای کوانتومی گفتیم یک اثبات وجودی است به این معنا که علی الاصول می توان با دقت دلخواه و با استفاده از یک مجموعه گیت های عام هر مدار کوانتومی یا هر عملگریکانی بزرگی را ساخت. در عمل لازم نیست که برای ساخت یک مدار کوانتومی این راه طی شود. این که یک مجموعه گیت عام کدام ها هستند بستگی به این دارد که کامپیوتر کوانتومی خود را با استفاده از چه نوع کیوبیت هایی ساخته ایم. هم چنین برای ساخت یک مدار معین اغلب راه هایی برای بهینه سازی اجزای مدار کوانتومی طی می شود که با آنچه که در این درس گفتیم تفاوت دارد و بستگی زیادی نیز به این دارد که از چه نوع کیوبیت هایی برای ساخت کامپیوتر کوانتومی استفاده کرده ایم.

■ قضیه گوتسمان-نیل: ۴

برای بیان این قضیه نخست می بایست گیت های کلیفورد^۵ را معرفی کنیم. می دانیم که مجموعه عملگرهای پاوولی تشکیل یک گروه نمی دهند (این موضوع را بیازمایید) ولی اگر این مجموعه را در اعداد $\pm 1, \pm i$ ضرب کنیم آنگاه یک گروه تشکیل می دهند یعنی مجموعه 16 عضوی حاصل تحت عمل ضرب بسته است. این گروه را گروه پاوولی روی یک کیوبیت می نامیم. بنابراین داریم:

■ **تعریف:** گروه پاوولی روی یک کیوبیت عبارت است از مجموعه زیر:

$$P_1 = \{\pm 1, \pm i\} \times \{I, X, Y, Z\}, \quad (۷۶)$$

مرتبه این گروه متناهی یعنی تعداد اعضای آن برابر است با $|P_1| = 16$.

■ **تمرین:** گروه بودن این مجموعه را بیازمایید. خودتان را قانع کنید که اگر بعضی از ضرایب مثلا $\pm i$ را حذف کنیم، مجموعه حاصل دیگر گروه نخواهد بود.

به همین نحو می توانیم گروه پاوولی روی n کیوبیت را تعریف کنیم. بازهم نیازمند این هستیم که ماتریس های پاوولی را که این بار روی n کیوبیت اثر می کنند همراه با ضرایب چهارگانه فوق در نظر بگیریم تا مجموعه حاصل تشکیل یک گروه بدهد. بنابراین داریم:

■ **تعریف:** گروه پاوولی روی n کیوبیت به صورت زیر تعریف می شود:

$$P_n = \{\pm 1, \pm i\} \times \{\sigma_{i_1} \otimes \sigma_{i_2} \otimes \cdots \sigma_{i_n}, \mid i_1, i_2, \dots, i_n = 0, 1, 2, 3\}. \quad (77)$$

تعداد اعضای این گروه برابر است با $|P_n| = 4^{n+1}$.

■ **تعریف:** عملگرها یا گیت های کلیفورد، گیت هایی هستند که دارای خاصیت زیر هستند:

$$U \sigma_\alpha U^\dagger = \sigma_{\alpha'}, \quad \forall \sigma_\alpha, \sigma_{\alpha'} \in P_n. \quad (78)$$

در این رابطه σ_α و $\sigma_{\alpha'}$ دو عضو دلخواه چند کیوبیتی از گروه پاوولی هستند.

■ **تمرین:** نشان دهید که عملگرهای

$$\{H, S = T^2, CNOT\}$$

عملگرهای کلیفورد هستند. (به تمرین دوم همین درس رجوع کنید.)

حال برای بیان قضیه گوتسمان - نیل آماده هستیم. این قضیه بیان می کند که هر کامپیوتر کوانتومی (شامل تهیه یک حالت اولیه، مدار کوانتومی و اندازه گیری نهایی) که در آن از گیت های کلیفورد استفاده شده باشد، قابل شبیه سازی توسط کامپیوترهای کلاسیک نیز هست. به این ترتیب این گونه کامپیوترها هیچ گونه برتری بر کامپیوترهای کلاسیک ندارند.

۶ تمرین ها

■ فقط با استفاده از عملگرهای $CNOT$ یک عملگر دوکیوبیتی $SWAP$ بسازید که کار زیر را انجام دهد:

$$SWAP|j, k\rangle = |k, j\rangle. \quad (۷۹)$$

■ اتحادهای زیر را نشان دهید:

$$\begin{aligned} (X \otimes I)CNOT &= CNOT(X \otimes X) \\ (I \otimes Z)CNOT &= CNOT(Z \otimes Z). \end{aligned} \quad (۸۰)$$

شکل مداری این اتحادها را رسم کنید. دقت کنید که در یک مدار عملگرها از چپ به راست عمل می کنند. اثبات شما باید خیلی ساده و برای هر کدام از روابط فوق در یک سطر نوشته شود.

■ در تمرین های زیر فرض کنید که عملگرهای دلخواه یک کیوبیتی را در اختیار دارید مگر آنکه خلاف آن صریحا گفته شده باشد .

■ یک مدار کوانتومی بسازید که بتواند از یک حالت $|000\rangle$ حالت GHZ یعنی $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ را درست کند. خروجی های مدار را برای وقتی که ورودی آن یک حالت ضربی دلخواه به صورت

$$|i, j, k\rangle, \quad i, j, k = 0, 1$$

باشد پیدا کنید.

■ یک مدار کوانتومی بسازید که بتواند از یک حالت $|000\rangle$ حالت زیر را درست کند:

$$|\psi\rangle = \cos \theta |100\rangle + \sin \theta \cos \phi |010\rangle + \sin \theta \sin \phi |001\rangle. \quad (۸۱)$$

■ یک مدار بسازید که با ورودی های مناسبی که به صورت ضربی هستند بتواند حالت های درهم تنیده زیر را درست کند:

$$|\phi^+\rangle = \cos \theta |00\rangle + \sin \theta |11\rangle, \quad (۸۲)$$

$$|\phi^-\rangle = \cos \theta |00\rangle - \sin \theta |11\rangle, \quad (۸۳)$$

$$|\psi^+\rangle = \cos \theta |01\rangle + \sin \theta |10\rangle, \quad (۸۴)$$

$$|\psi^-\rangle = \cos \theta |01\rangle - \sin \theta |10\rangle. \quad (۸۵)$$

■ یک مدار کوانتومی بسازید که بتواند با ورودی های مناسبی که به صورت ضربی هستند، حالت های زیر را درست کند:

$$|\phi_+^0\rangle = \cos \theta |000\rangle + \sin \theta |111\rangle, \quad (۸۶)$$

$$|\phi_-^0\rangle = -\sin \theta |000\rangle + \cos \theta |111\rangle, \quad (۸۷)$$

$$|\phi_+^1\rangle = \cos \theta |001\rangle + \sin \theta |110\rangle, \quad (۸۸)$$

$$|\phi_-^1\rangle = -\sin \theta |001\rangle + \cos \theta |110\rangle, \quad (۸۹)$$

$$|\phi_+^2\rangle = \cos \theta |010\rangle + \sin \theta |101\rangle, \quad (۹۰)$$

$$|\phi_-^2\rangle = -\sin \theta |010\rangle + \cos \theta |101\rangle, \quad (۹۱)$$

$$|\phi_+^3\rangle = \cos \theta |011\rangle + \sin \theta |100\rangle \quad (۹۲)$$

$$|\phi_-^3\rangle = -\sin \theta |011\rangle + \cos \theta |100\rangle. \quad (۹۳)$$

■ با استفاده از عملگرهای $CNOT$ و عملگرهای تک کیوبیتی عملگر $\Lambda^2(Z)$ را بسازید. سعی کنید که از کمترین تعداد عملگرهای $CNOT$ استفاده کنید.

■ به همان شیوه مسئله قبلی سعی کنید عملگر $\Lambda^3(Z)$ را بسازید.

■ یک عملگر دوترازی که روی دو کیوبیت اثر می کند در نظر بگیرید. این عملگر روی زیر فضای تشکیل شده از $|01\rangle$ و $|10\rangle$ به صورت U عمل می کند و روی بقیه فضا به صورت عملگر واحد عمل می کند. با استفاده از عملگرهای $CNOT$ و گیت کنترلی $\Lambda^1(U)$ را این عملگر را بسازید.

■ الف: یک عملگر دوترازی که روی سه کیوبیت اثر می کند در نظر بگیرید. این عملگر روی زیر فضای تشکیل شده از $|001\rangle$ و $|100\rangle$ به صورت U عمل می کند و روی بقیه فضا به صورت عملگر واحد عمل می کند. با استفاده از عملگرهای $CNOT$ و گیت کنترلی $\Lambda^1(U)$ را این عملگر را بسازید. با دادن ورودی های مختلف به این مدار واقعا تحقیق کنید که این مدار عمل خواسته شده را انجام می دهد.

ب: قسمت الف را برای وقتی که عملگر دو ترازوی روی زیرفضای تشکیل شده از $|111\rangle$, $|000\rangle$ عمل می کند حل کنید.

■ یک عملگر دوترازی که روی سه کیوبیت اثر می کند در نظر بگیرید. این عملگر روی زیر فضای تشکیل شده از $|0011\rangle$ و $|1100\rangle$ به صورت U عمل می کند و روی بقیه فضا به صورت عملگر واحد عمل می کند. با استفاده از عملگرهای $CNOT$ و گیت کنترلی $\Lambda^1(U)$ را این عملگر را بسازید. با دادن ورودی های مختلف به این مدار واقعا تحقیق کنید که این مدار عمل خواسته شده را انجام می دهد.

■ یک مدار کوانتومی بسازید که وقتی ورودی های

$$|i, j\rangle, \quad i, j = 0, 1$$

را می گیرد حالت های زیر را تولید کند:

$$\begin{aligned} & \frac{1}{\sqrt{2}}(|00\rangle + e^{i\phi}|11\rangle) \\ & \frac{1}{\sqrt{2}}(|00\rangle - e^{i\phi}|11\rangle) \\ & \frac{1}{\sqrt{2}}(|01\rangle + e^{i\phi}|10\rangle) \\ & \frac{1}{\sqrt{2}}(|01\rangle - e^{i\phi}|10\rangle). \end{aligned} \quad (94)$$

■ یک مدار کوانتومی بسازید که روی ورودی $|0000\rangle$ اثر کند و حالت زیر را تولید کند:

$$\frac{1}{2}(|1000\rangle + |0100\rangle + |0010\rangle + |0001\rangle) \quad (95)$$

■ یک مدار کوانتومی بسازید که روی ورودی $|0000\rangle$ اثر کند و حالت زیر را تولید کند:

$$\frac{1}{\sqrt{2}}(|1110\rangle + |0111\rangle) \quad (96)$$

■ یک مدار کوانتومی بسازید که روی ورودی $|0000\rangle$ اثر کند و حالت زیر را تولید کند:

$$\cos \theta |1100\rangle + \sin \theta |0011\rangle \quad (97)$$

■ الف: یک مدار کوانتومی بسازید که وقتی دو کیوبیت اول و دوم با هم مخالف هستند روی کیوبیت سوم عمل U را انجام دهد و در غیر این صورت روی کیوبیت سوم عمل همانی را انجام دهد.

ب: قسمت الف را تغییر دهید طوری که وقتی دو کیوبیت اول با هم مساوی هستند عمل U روی کیوبیت سوم اثر کند و در غیر این صورت عمل همانی روی کیوبیت سوم اثر کند.

■ الف: یک مدار کوانتومی بسازید که وقتی دو کیوبیت اول و دوم با هم مخالف هستند روی کیوبیت سوم عمل U را انجام دهد و در غیر این صورت روی کیوبیت سوم عمل همانی را انجام دهد.

ب: قسمت الف را تغییر دهید طوری که وقتی دو کیوبیت اول با هم مساوی هستند عمل U روی کیوبیت سوم اثر کند و در غیر این صورت عمل همانی روی کیوبیت سوم اثر کند.

■ یک مدار کوانتومی بسازید که وقتی سه کیوبیت اول در یکی از حالت های

$$\{100, 010, 001, 111\}$$

باشد روی کیوبیت چهارم عملگر U را اثر دهد و در غیر این صورت عملگر همانی را اثر دهد.

■ یک مدار کوانتومی بسازید که وقتی سه کیوبیت اول در یکی از حالت های

$$\{100, 010, 001\}$$

باشد روی کیوبیت چهارم عملگر U را اثر دهد و در غیر این صورت عملگر همانی را اثر دهد.

■ یک مدار کوانتومی بسازید که حالت $|0000\rangle$ را به حالت زیر تبدیل کند:

$$|\psi\rangle = \frac{1}{2}(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle). \quad (98)$$

راهنمایی: یک راه این است که از حالت

$$|\psi_+\rangle \otimes |\psi_+\rangle \quad (99)$$

شروع کنید که در آن $|\psi_+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ است و سپس 1 های اضافه را با عملگرهای کنترل مناسب به 0 تبدیل کنید. اگر این راه را انتخاب کنید، می بایست یک مدار اولیه نیز بسازید که حالت اولیه (99) را بسازد. البته شاید شما بتوانید راه ساده تر و مبتکرانه ای ارائه دهید.

■ می خواهیم دو کیوبیت را در پایه بل اندازه گیری کنیم. نشان دهید که می توانیم نخست با اعمال گیت های کوانتومی و سپس با اندازه گیری تنها یک کیوبیت این اندازه گیری را انجام دهیم.

■ عملگر زیر را در نظر بگیرید:

$$U := \begin{pmatrix} a & 0 & 0 & b \\ 0 & c & d & 0 \\ 0 & -d^* & c^* & 0 \\ -b^* & 0 & 0 & a^* \end{pmatrix}, \quad (100)$$

که در آن $|a|^2 + |b|^2 = 1$ و $|c|^2 + |d|^2 = 1$. یک مدار کوانتومی با استفاده از گیت های کوانتومی یک کیوبیتی و $CNOT$ بسازید که عملگر فوق را ایجاد کند.

■ تمرین: الف: یک مدار کوانتومی بسازد که عملگر یکانی زیر را روی دو کیوبیت اثر دهد:

$$U_z(\gamma) := e^{i\gamma(\sigma_z \otimes \sigma_z)} \quad (101)$$

ب: از این نکته استفاده کنید که $H \sigma_z H = \sigma_x$ و مداری بسازید که عملگر کوانتومی زیر را روی دو کیوبیت اعمال کند:

$$U_x(\alpha) := e^{i\alpha(\sigma_x \otimes \sigma_x)} \quad (102)$$

ج: مداری کوانتومی بسازید که عملگر زیر را روی دو کیوبیت اعمال کند:

$$U_y(\beta) := e^{i\beta(\sigma_y \otimes \sigma_y)}. \quad (103)$$

د: مداری کوانتومی بسازید که عملگر زیر را روی دو کیوبیت اعمال کند:

$$\Omega(\alpha, \beta, \gamma) := e^{i(\alpha\sigma_x \otimes \sigma_x + \beta\sigma_y \otimes \sigma_y + \gamma\sigma_z \otimes \sigma_z)}. \quad (104)$$

■ تمرین: آیا به همان ترتیبی که گیت های کنترل دوتایی مثل $\Lambda^2(U)$ را از گیت های کنترل $\Lambda^1(U)$ توانستیم بسازیم، می توانیم گیت توفولی را از گیت $CNOT$ بسازیم؟

۷. قدردانی

این درسنامه را حسین محمدی دانشجوی دانشکده فیزیک در آبان ماه ۱۴۰۱ به دقت خوانده و اشکالات متعدد آن را به من یادآوری کردند. برای این لطف بزرگ از ایشان تشکر می کنم. هم چنین نیما کوهی دانشجوی این درس در سال ۱۴۰۴ نیز چندین اشکال درسنامه توسعه یافته را به من یادآوری کرده اند. از او سپاسگزارم.