فهرست مطالب

۱ آشنایی با مفاهیم اولیه ۵

۱.۱ کیوبیت ۵

۱.۱.۱ کیوبیت واحد ۵

۲.۱.۱ کیوبیت‌های چندتایی ۸

۲.۱ اندازه‌گیری در فضای هیلبرت ۹

۳.۱ گیت‌های کوانتومی ۱۱

۱.۳.۱ انواع گیت کوانتومی ۱۱

۲.۳.۱ گیت مبادله ۱۹

۴.۱ مدارهای کوانتومی ۲۱

۱.۴.۱ نحوه‌ی نمایش مدارهای کوانتومی ۲۴

۲ برنامه‌نویسی کوانتومی ۲۵

۱.۲ کامپیوترهای کوانتومی در مقابل کامپیوترهای کلاسیک ۲۵

۲.۲ شبیه‌سازی کلاسیک در مقابل کامپیوتر کوانتومی ۲۶

۱.۲.۲ تفاوت کامپیوترهای کوانتومی و شبیه‌سازهای کلاسیک ۲۷

۳.۲ شبیه‌سازی کلاسیک ۲۸

۴.۲ کامپیوترکوانتومی IBM و زبان برنامه‌نویسی QisKit ۲۹

۱.۴.۲ معرفی QisKit ۲۹

۲.۴.۲ کدنویسی به زبان QisKit ۲۹

۳.۴.۲ قواعد نوشتاری و ساختار داده ۲۹

۴.۴.۲ پیاده‌سازی گیت‌های کوانتومی ۳۰

۵.۴.۲ تصویر سازی ۳۱

۳ الگوریتم‌های کوانتومی **۳۳**
۱.۳ موازی سازی کوانتومی ۳۳
۱.۱.۳ مدل محاسباتی استاندارد ۳۷
۲.۳ مدل کوئری ۳۷
۳.۳ معرفی و پیاده سازی الگوریتم دوچ ۳۸
۱.۳.۳ مسئله‌ی دوچ ۳۸
۲.۳.۳ الگوریتم دوچ ۳۹
۳.۳.۳ پیاده‌سازی الگوریتم دوچ در کیس کیت ۴۲

۴ شبیه‌سازی پدیده‌های کوانتومی **۴۳**
۱.۴ حالات بل ۴۳
۲.۴ درهمتنیدگی ۴۵
۱.۲.۴ پیاده‌سازی درهمتنیدگی در کیس کیت ۴۶
۳.۴ رمزگذاری متراکم کوانتومی ۴۷
۱.۳.۴ پیاده سازی رمزگذاری متراکم در کیس کیت ۵۰
۴.۴ دوربری ۵۱
۱.۴.۴ پیاده‌سازی دوربری در کیس کیت ۵۴

مقدمه

در عصر حاضر به واسطه رشد و توسعه‌ی نظریه‌ی اطلاعات کوانتومی و سرمایه‌گذاری های مالی و انسانی بسیار در این زمینه،شاهد افزایش تعداد علاقمندان به این حوزه هستیم. در این پا

فصل ۱

آشنایی با مفاهیم اولیه

۱.۱ کیوبیت

یک کیوبیت[۱]، معادل یک واحد اطلاعات کوانتومی می‌باشد. این مفهوم معادل مفهوم کلاسیک بیت[۲] می‌باشد. به طور کلی هر کیوبیت حاوی دو بیت اطلاعات است. برای تبیین یک کیوبیت از خصوصیات سامانه های کوانتومی، بهره می‌بریم. کیوبیت یک سیستم کوانتومی با فضای دوبعدی است. برای تعیین این دوبعد می‌توان ا ز یکی از خصویات سامانه های کوانتومی استفاده کرد.

۱.۱.۱ کیوبیت واحد

برخلاف بیت ها که مقادیر ثابت ۰ یا ۱ را به خود می‌گیرند؛ یک کیوبیت می‌تواند در یک حالت «برهمنهی کوانتومی[۳]» باشد؛ این بدان معناست که یک کیوبیت بواسطه‌ی مشاهده ناظر به یکی از حالات ۰ یا یک تبدیل شود. این مهم‌ترین مزیت استفاده از کیوبیت‌هاست.

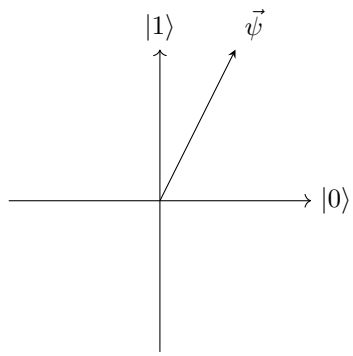
---

[۱] Qubit
[۲] Binary Bit
[۳] Quantum Superposition

بیان ریاضی یک کیوبیت ،در حالت برهمنهی، به شرح زیر است:

$$\begin{cases} |\psi\rangle = \alpha|0\rangle + \beta|1\rangle \\ \alpha^2 + \beta^2 = 1 \end{cases} \tag{۱.۱}$$

کت‌های $|0\rangle$ و $|1\rangle$ بیانگر پایه‌های فضای محاسباتی[۴] هستند؛ و مقادیر α^2 و β^2 بیانگر احتمال وقوع هر یک از این حالات، در صورت مشاهده، می‌باشند. نمایش بردار ψ به شکل زیر است:



در بسیاری از مواقع برای سهولت در محاسبات، عملگرها و حالات کوانتومی به کمک ماتریس‌ها نمایش داده می‌شوند. فرم ماتریسی هر یک از حالات ذکر شده در بالا به شرح زیر است:

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{۲.۱}$$

برای تعریف کیوبیت ها، راه های زیادی وجود دارد، حالات قطبش فوتون،اسپین الکترون،یا سطوح انرژی اتم،هریک می‌توانند تعیین کننده‌ی بردارهای فضای کیوبیت باشند.

به طور کلی، حالت کیوبیت یک بردار واحد در فضای برداری دو بعدی پیچیده است.

[۴] Computational Basis Vectors

در بیشتر مدل های انتزاعی ما از جهان، یک ارتباط مستقیم بین عناصر انتزاع و دنیای واقعی وجود دارد، درست همانطور که طرح های یک معمار برای یک ساختمان با ساختمان نهایی مطابقت دارد. فقدان این ارتباط مستقیم در مکانیک کوانتوم باعث می شود که درک رفتار سیستم های کوانتومی دشوار باشد؛ با این حال، یک ارتباط غیرمستقیم وجود دارد، زیرا می توان حالت های کیوبیت را دستکاری و تبدیل کرد به وضعیت‌هایی که منجر به نتایج اندازه گیری می شود. نتایج حاصل از اندازه‌گیری به خواص مختلف حالت بستگی دارد. بنابراین، این حالت های کوانتومی دارای پیامدهای واقعی و قابل آزمایش تجربی هستند.

مفهوم کیوبیت، با «فهم رایج» ما از جهان فیزیکی اطراف ما مغایرت دارد. یک بیت کلاسیک مانند سکه است: یا رو یا پشت. برای سکه های غیراایده آل، ممکن است حالت های واسطه ای مانند قرار گرفتن آن روی لبه وجود داشته باشد، اما در حالت ایده آل می توان آنها را نادیده گرفت.

در مقابل، یک کیوبیت می تواند در یک طیف پیوسته از حالت ها بین $|0\rangle$ و $|1\rangle$ وجود داشته باشد - تا زمانی که مشاهده شود. بار دیگر تاکید می کنیم که وقتی یک کیوبیت اندازه گیری می شود، فقط یکی از اازمقادیر «۰» یا «۱» را به عنوان نتیجه اندازه گیری می دهد. به عنوان مثال، یک کیوبیت می تواند در حالت $|0\rangle + |1\rangle$ باشد، که به این معنی است که با احتمال ۵۰/۵۰ می تواند به عنوان ۰ یا ۱ اندازه گیری شود.

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \tag{۳.۱}$$

حالت $|+\rangle$ حالتی از کیوبیت است که با یک بردار ۲ بعدی واحد نشان داده می شود. این حالت، زمانی که اندازه گیری شود، نتیجه ۰ را ۵۰ درصد از زمان و نتیجه ۱ را ۵۰ درصد از زمان می دهد. این حالت را می توان به عنوان یک ترکیب خطی از دو حالت پایه $|0\rangle$ و $|1\rangle$ در نظر گرفت.

این حالت به دلیل عجیب بودنش جالب است. حالت های پایه $|0\rangle$ و $|1\rangle$ تنها حالاتی هستند که می توانند به طور مستقیم مشاهده شوند. حالت $|+\rangle$ ، با این حال، یک حالت ترکیبی است که به طور مستقیم قابل مشاهده نیست. تنها زمانی می توان آن را مشاهده کرد که اندازه گیری شود.

با وجود غیرقابل مشاهده بودن، حالت $|+\rangle$ واقعی است. وجود آن توسط آزمایشات به طور گسترده ای تأیید شده است. همچنین می توان از آن برای انجام محاسبات کوانتومی استفاده کرد.

در آینده، ممکن است حالت $|+\rangle$ برای اهداف مختلف دیگری نیز استفاده شود. به عنوان مثال، می تواند برای ذخیره اطلاعات یا برای ایجاد ارتباطات امن استفاده شود.

۲.۱.۱ کیوبیت‌های چندتایی

Hilbert space is a big place.

– Carlton Caves

فرض کنید دو کیوبیت داریم. اگر این دو بیت کلاسیک بودند، چهار حالت ممکن وجود داشت: ۰۰، ۰۱، ۱۰ و ۱۱. به همین ترتیب، یک سیستم دو کیوبیتی دارای چهار حالت محاسباتی است که با $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ نشان داده می شود. یک جفت کیوبیت همچنین می تواند در برهمنهی این چهار حالت وجود داشته باشد. بنابراین حالت کوانتومی دو کیوبیت با اختصاص یک عدد مختلط - گاهی اوقات به عنوان یک دامنه شناخته می شود - به هر حالت محاسباتی، بیان می‌شود. بردار حالت توصیف کننده دو کیوبیت به شکل زیر است:

$$|\Psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \tag{۴.۱}$$

جایی که a، b، c و d دامنه های چهار حالت را نشان می دهند. دامنه ها می توانند هر عدد مختلطی باشند، اما معمولاً به گونه ای نرمال می شوند که مجموع آنها برابر ۱ باشد. این بدان معناست که بردار حالت یک حالت کوانتومی معتبر را نشان می دهد و کیوبیت ها به طور مساوی احتمال اندازه گیری در هر یک از چهار حالت محاسباتی را دارند.

به عنوان مثال، بردار حالت:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

یک سیستم دو کیوبیتی را نشان می دهد که در یک برهمنهی مساوی از حالت های ۰۰ و ۱۱ است. این بدان معناست که کیوبیت ها به طور مساوی احتمال اندازه گیری در حالت ۰۰ یا ۱۱ را دارند.

بردار حالت یک سیستم دو کیوبیتی را می توان برای محاسبه احتمال اندازه گیری کیوبیت ها در هر یک از چهار حالت محاسباتی استفاده کرد. به عنوان مثال، احتمال اندازه گیری کیوبیت ها در حالت ۰۰ با فرمول زیر داده می شود:

$$P(|00\rangle) = |a|^2 = \frac{1}{2} \tag{۵.۱}$$

احتمال اندازه گیری کیوبیت ها در هر حالت دیگر را می توان به روشی مشابه محاسبه کرد.

نتیجه اندازه گیری $x(= 00, 01, 10, 11)$ با احتمال $|a_x|^2$ رخ می دهد، با حالت کیوبیت ها پس از اندازه گیری$|x\rangle$. این بدان معناست که اگر ما یک سیستم دو کیوبیتی را در حالت $= |\Psi\rangle$ $a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ داشته باشیم، و اگر ما اولین کیوبیت را اندازه گیری کنیم، احتمال اینکه ۰ را اندازه گیری کنیم برابر $|a\rangle^2 + |b\rangle^2$ خواهد بود. در این حالت، حالت کیوبیت ها پس از اندازه گیری $|0\rangle$ خواهد بود.

$$|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}} \tag{۶.۱}$$

توجه داشته باشید که حالت پس از اندازه گیری با عامل $\sqrt{|_{00}|^2 + |_{01}|^2}$ نرمال می شود تا همچنان شرط نرمال سازی را، درست همانطور که برای یک حالت کوانتومی معتبر انتظار می‌رود، برآورده کند. این بدان معناست که حالت پس از اندازه گیری به گونه ای تغییر می کند که احتمالات آن جمع شده و برابر ۱ شود.

۲.۱ اندازه‌گیری در فضای هیلبرت

ما تاکنون اندازه گیری های کوانتومی یک کیوبیت در حالت $\alpha|0\rangle + \beta|1\rangle$را به عنوان نتیجه ۰ یا ۱ توصیف کرده ایم که کیوبیت را در حالت $|0\rangle$ یا $|1\rangle$مربوطه باقی می گذارد، با احتمالات $|\alpha|^2$ و $|\beta|^2$. در حقیقت، مکانیک کوانتوم به اندازه کافی انعطاف پذیری در کلاس اندازه گیری هایی که می توان انجام داد، اگرچه مطمئناً به اندازه کافی نیست که α و β را از یک اندازه گیری واحد بازیابی کند!

توجه داشته باشید که $|0\rangle$ و $|1\rangle$ فقط یکی از بسیاری از انتخاب های ممکن برای پایه های حالت برای یک کیوبیت هستند. یک انتخاب دیگر مجموعه به شرح زیر است:

$$\begin{aligned} |+\rangle &\equiv (|0\rangle + |1\rangle)\sqrt{2} \\ |-\rangle &\equiv (|0\rangle - |1\rangle)\sqrt{2} \end{aligned} \tag{۷.۱}$$

یک حالت دلخواه $|\Psi\rangle = \alpha 0\rangle + \beta 1\rangle$ را می توان با استفاده از حالت های $|+\rangle$ و $|-\rangle$ بازنویسی کرد:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle = \frac{(\alpha+\beta)}{2}|+\rangle + \frac{(\alpha-\beta)}{2}|-\rangle \qquad (۸.۱)$$

در این بیان، $|+\rangle$و $|-\rangle$ به عنوان پایه های "پایه +" و "پایه -" شناخته می شوند. اندازه گیری در پایه + یا پایه - یک کیوبیت را در حالت $|+\rangle$ یا $|-\rangle$قرار می دهد.

اندازه گیری در پایه های دیگر به غیر از پایه محاسباتی یک ابزار قدرتمند در محاسبات کوانتومی است. این امکان را می دهد تا ما در حالت های کوانتومی که در پایگاه محاسباتی قابل اندازه گیری نیستند، اندازه گیری کنیم. این امکان را می دهد تا ما از روش های محاسباتی جدیدی استفاده کنیم که در محاسبات کلاسیک غیرممکن است.

در واقع، این امکان وجود دارد که حالت های $|+\rangle$ و $|-\rangle$ را به گونه ای که گویی آنها حالت های پایه محاسباتی هستند، در نظر بگیریم و با توجه به این پایه جدید اندازه گیری کنیم. طبیعی است که اندازه گیری با توجه به پایه $|-\rangle$، $|+\rangle$ منجر به نتیجه "+" با احتمال $\frac{|\alpha+\beta|}{2}^2$ و نتیجه "-" با احتمال $\frac{|\alpha-\beta|}{2}^2$ می شود.

در این بیان، $|+\rangle$ و $|-\rangle$ به عنوان "پایه +" و "پایه -" شناخته می شوند. اندازه گیری در پایه + یا پایه - یک کیوبیت را در حالت $|+\rangle$ یا $|-\rangle$ قرار می دهد.

به طور کلی تر، با توجه به هر دو پایه حالت $|a\rangle$ و $|b\rangle$ برای یک کیوبیت، می توان هر حالت دلخواهی را به عنوان یک ترکیب خطی $\alpha|a\rangle + \beta|b\rangle$ از آن حالات بیان کرد. علاوه بر این، اگر این حالات متعامد باشند، می توان با توجه به پایه $|a\rangle$، $|b\rangle$ اندازه گیری کرد، که نتیجه a با احتمال $|\alpha|^2$ و b با احتمال $|\beta|^2$ قابل رخداد است.

با توجه به بیان احتمالاتی مفهوم کیوبیت و نرمال بودن مقادیر احتمالات و متعامد بودن پایه‌ها، لازم است تا $|\alpha|^2 + |\alpha|^2 = 1$ باشد همانطور که برای احتمالات انتظار می رود. به طور مشابه، در اصل می توان یک سیستم کوانتومی از بسیاری از کیوبیت ها را با توجه به یک پایه متعامد دلخواه اندازه گیری کرد.

اندازه گیری در پایه های دیگر یک ابزار قدرتمند در محاسبات کوانتومی است. این امکان را می دهد تا ما در حالت های کوانتومی که در پایگاه محاسباتی قابل اندازه گیری نیستند، اندازه گیری کنیم. این امکان را می دهد تا ما از روش های محاسباتی جدیدی استفاده کنیم که در محاسبات کلاسیک غیرممکن است.

دلایل زیادی برای استفاده از این مدل توسعه‌یافته برای اندازه گیری های کوانتومی وجود دارد، اما در نهایت بهترین دلیل این است: این مدل به ما امکان توصیف نتایج تجربی مشاهده شده نظیر نتایج

آزمایش اشترن-گرلاخ[۵] را می دهد.

۳.۱ گیت‌های کوانتومی

گیت‌های کوانتومی[۶] یکی از اولین و مهم‌ترین اجزای مدارهای کوانتومی می‌باشند. این گیت‌ها عملگرهایی با قابلیت اثرگذاری روی کیوبیت‌ها می‌باشند. با اعمال یک گیت کوانتومی بر روی یک یا چند کیوبیت، می‌توان تغییرات مدنظر خود را روی کیوبیت اعمال کرد. با کمک این گیت‌ها می‌توان باعث برهم‌نهی کوانتومی یا رمزگذاری داده در داخل یک یا چند کیوبیت شد.

۱.۳.۱ انواع گیت کوانتومی

گیت‌های کوانتومی، دارای انواع مختلف گوناگونی می‌باشند. به طور کلی گیت‌های کوانتومی، عملگرهایی یکه و بازگشت‌پذیر می‌باشند. به‌طور کلی گیت‌های‌کوانتومی متناسب با تعداد کیوبیت‌هایی که از آنها اثرمیگیرند؛ دسته‌بندی می‌کنیم. در این گفتار به گیت‌های تک کیوبیتی و دو کیوبیتی می‌پردازیم.

گیت هادامارد

مهم‌ترین گیت کوانتومی،گیت هادامارد[۷] است. با اعمال اثر این گیت روی یک کیوبیت، آن کیوبیت به‌یک حالت برهم نهی کوانتومی گذار می‌کند. به عبارت دیگر هر یک از زیرحالات این حالت برهم‌نهی، با احتمال یکسانی قابل رخ دادن هستند.

$$H\left|0\right\rangle = \frac{1}{\sqrt{2}}(\left|0\right\rangle + \left|1\right\rangle) \tag{۹.۱}$$

$$H\left|1\right\rangle = \frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle) \tag{۱۰.۱}$$

[۵] Stern–Gerlach
[۶] Quantum Gates
[۷] Hadamard gate

این گیت کوانتومی به صورت خطی روی یک دسته کت اثر می‌کند. نمایش ماتریسی این گیت‌کوانتومی به شرح زیر است:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{۱۱.۱}$$

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{۱۲.۱}$$

$$H|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{۱۳.۱}$$

این گیت کوانتومی، یک گیت بازگشت‌پذیر است؛ یعنی اگر این گیت روی یک حالت کوانتومی اثر کند؛ می‌تواند آن را از حالت برهمنهی خارج کند.

برای اعمال این گیت کوانتومی، فقط به یک کیوبیت نیاز داریم. به اصطلاح این گیت، یک گیت تک کیوبیت [۸] می‌باشد.

نمایش این گیت‌کوانتومی در مدار با علامت زیر است: $-\boxed{H}-$

گیت NOT

گیت کوانتومی U_{NOT} یک عملگر یکه و بازگشت‌پذیر است.

$$\begin{aligned} U_{NOT}|0\rangle &= |1\rangle \\ U_{NOT}|1\rangle &= |0\rangle \end{aligned} \tag{۱۴.۱}$$

[۸] Single-Qubit Quantum gate

نمایش ماتریسی گیت NOT

می بینید که اگر فقط پایه را در نظر بگیریم، دقیقاً مانند دروازه کلاسیک NOT است. نمایش ماتریسی این گیت به شکل زیر است:

$$U_{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

از آنجایی که یک حالت کیوبیت در فضای هیلبرت دو بعدی تعریف شده است. ابعاد ماتریس باید ۲ × ۲ باشد. از این رو می‌توان نوشت:

$$\begin{aligned} U_{NOT}|0\rangle &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} |0\rangle \\ &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \end{aligned}$$

$$\begin{aligned} \boldsymbol{U}_{\text{NOT}}|1\rangle &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} |1\rangle \\ &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \end{aligned}$$

مدار NOT و خصوصیات آن

با اعمال گیت U_{NOT} به حالت $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ خواهیم داشت:

$$\begin{aligned} \boldsymbol{U}_{\text{NOT}}|\Psi\rangle &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} |\Psi\rangle \\ &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix} = \beta|0\rangle + \alpha|1\rangle \end{aligned}$$

علاوه بر دروازه NOT یک کیوبیتی، می‌توانیم دو کیوبیتی نیز بسازیم. می‌بایست حاصل ضرب تانسوری دو دروازه NOT یک کیوبیتی را محاسبه کنیم؛ تا یک دروازه NOT دو کیوبیتی بدست آوریم زیرا یک بردار دو کیوبیتی در فضای$\mathbb{C}^4$ قرار دارد. که حاصل ضرب تانسور دو فضای$\mathbb{C}^2$است. از این رو:

$$U_{NOT_2} = U_{NOT} \otimes U_{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
$$= \begin{pmatrix} 0\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & 1\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ 1\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & 0\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

نمایش یک گیت NOT به صورت زیر است:

$$-\boxed{X}-$$

با اعمال گیت دوکیوبیتی NOT به یک سیستم دو کیوبیتی نظیر $|\Psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$ خواهیم داشت:

$$\boldsymbol{U_{NOT_2}}|\Psi\rangle = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \delta \\ \gamma \\ \beta \\ \alpha \end{pmatrix}$$

گیت CNOT

گیت کوانتومی CNOT[۹]، به عنوان گیت منطقی نیز یاد می‌شود. این گیت کوانتومی معادل گیت NOT کلاسیک می‌باشد. به‌طور معمول، برای اعمال اثر این گیت کوانتومی نیاز به دو کیوبیت داریم. این گیت کوانتومی فقط و فقط در مواقعی که «کیوبیت کنترل[۱۰]» دارای مقدار $|1\rangle$ باشد، باعث تغییر وضعیت «کیوبیت هدف[۱۱]» می‌شود.

[۹] gate controlled-X or gate controlled-NOT
[۱۰] Qubit Controled
[۱۱] Qubit Target

کیوبیت کنترلی: کیوبیتی است که عملکرد کیوبیت دیگری به نام کیوبیت هدف را کنترل می کند. کیوبیت کنترل تعیین می کند که آیا کیوبیت هدف برگردانده شود یا خیر. اگر کیوبیت کنترل در حالت $|0\rangle$ باشد، کیوبیت هدف بدون تغییر باقی می‌ماند. اگر کیوبیت کنترل در حالت $|1\rangle$ باشد، کیوبیت هدف برگردانده می شود.

کیوبیت هدف: همان کیوبیتی است که توسط کیوبیت کنترل بر روی آن عمل می شود. بسته به وضعیت کیوبیت کنترل، کیوبیت هدف را می توان برگرداند یا بی‌تغییر رها کند.

$$U_{CNOT}|ab\rangle = |a\ a\oplus\rangle b$$

$|ab\rangle$ چیست؟ این یک بردار در فضای $\mathbb{C}^4$ و a و b دارای مقدار ۰ یا ۱ هستند. $|ab\rangle$ می تواند هر یک از حالت های پایه(یعنی $|00\rangle, |01\rangle, |10\rangle, |11\rangle$) باشد.
این معادله به ما می گوید؛ که پس از اعمال گیت CNOT به یکی از پایه‌ها، آن حالت به حالت پایه دیگری تبدیل خواهد شد. که این حالت برابر $|a\ a \oplus b\rangle$ می‌باشد. به‌طوری که:

$$|a\ a \oplus b\rangle = |a\rangle \otimes |a \oplus b\rangle$$

بعد از عمل، عدد اول همچنان a است، اما عدد دوم به $a \oplus b$ تبدیل می شود، جایی که $\oplus$ عملیات منطقی کلاسیک انحصاری یا (XOR) است. توجه کنید که:

$$0 \oplus 0 = 0$$
$$0 \oplus 1 = 1$$
$$1 \oplus 0 = 1$$
$$1 \oplus 1 = 0$$

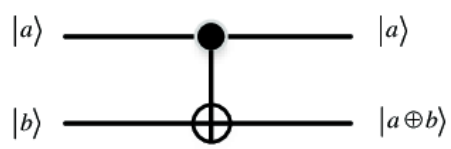
$$U_{CNOT}|00\rangle = |0, 0 \oplus 0\rangle = |0, 0\rangle = |00\rangle$$
$$U_{CNOT}|01\rangle = |0, 0 \oplus 1\rangle = |0, 1\rangle = |01\rangle$$
$$U_{CNOT}|10\rangle = |1, 1 \oplus 0\rangle = |1, 1\rangle = |11\rangle$$
$$U_{CNOT}|11\rangle = |1, 1 \oplus 1\rangle = |1, 1\rangle = |10\rangle$$

خلاصه‌ای از عملکرد این عملگر به شرح زیر است:

$\|A$	$B\rangle$		$\|A$	$B \oplus A\rangle$
$\|control\rangle$	$\|target\rangle$	Effect CNOT Gate	$\|control\rangle$	$\|target\rangle$
$\|0\rangle$	$\|0\rangle$	$\Longrightarrow$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\Longrightarrow$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\Longrightarrow$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\Longrightarrow$	$\|1\rangle$	$\|0\rangle$

نمایش ماتریسی این گیت کوانتومی به شکل زیر است:

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



شکل ۱.۱: نمایش ماتریسی و نمایش گیت کوانتومی CNOT

در شکل بالا گیت CNOT در مدار کوانتومی به تصویر درآمده است. کیوبیت کنترل شده حالت $|a\rangle$ و کیوبیت هدف حالت $|b\rangle$ می‌باشد.

با اعمال این عملگر به حالت $|10\rangle$ داریم:

$$\text{CNOT}\,|10\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = |11\rangle$$

این فرآیند به صورت معکوس نیز قابل رخ دادن است:

$$\text{CNOT}\,|11\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = |10\rangle$$

از این گیت کوانتومی، برای بسیاری مدارها و شبیه‌سازی‌های کوانتومی، از جمله تلپورت، درهمتنیدگی و ...،استفاده می‌شود.

گیت تغییر فاز

گیت تغییر فاز که به آن گیت P یا گیت فاز نیز می گویند، یک کیوبیت است. دروازه ای که فاز نسبی را بین دو بردار پایه جابجا می کند. به عنوان زیر تعریف شده است:

$$\boldsymbol{U_{PS,\phi}}|0\rangle = |0\rangle$$
$$\boldsymbol{U_{PS,\phi}}|1\rangle = e^{i\Phi}|1\rangle$$

که در آن Φ فاز و $e^{i\Phi}$ عامل فاز است. زمانی که گیت تغییر فاز بر حالت $|0\rangle$ اثرکند، هیچ تغییری حاصل نمی‌شود. اما با اعمال این گیت به بردار حالت $|1\rangle$، یک فاز اضافه به بردار افزوده خواهد شد. برای افزدون فاز اضافه باید یک عامل نظیر $e^{i\Phi}$ در بردارد حالت ضرب شود. برای درک بهتر مطلب باید به حالت ماتریسی این گیت رجوع کنیم.

نمایش ماتریسی گیت تغییر فاز

نمایش ماتریسی گیت تغییر فاز $\boldsymbol{U_{PS,\Phi}}$ به صورت زیر است:

$$\boldsymbol{U_{PS,\Phi}} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\Phi} \end{pmatrix}$$

با استفاده از روابط بالا می‌توان به راحتی اثبات کرد:

$$U_{PS,\phi}|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\Phi} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ e^{i\Phi} \end{pmatrix} = e^{i\Phi} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = e^{i\Phi}|1\rangle$$

گیت تغییر فاز در مدار و خصوصیات آن

درحالت کلی برای سیستم های تک کیوبیتی می‌توان نوشت:

$$\begin{aligned} \boldsymbol{U_{PS,\Phi}}|\Psi\rangle &= \begin{pmatrix} 1 & 0 \\ 0 & e^{i\Phi} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ e^{i\Phi}\beta \end{pmatrix} \\ &= \alpha|0\rangle + e^{i\Phi}\beta|1\rangle \end{aligned}$$

در بردار اصلی، α و β اعداد مختلط می‌باشند؛ به همین دلیل این اعداد را می‌توان به به عنوان یک ضریب فاز معرفی کرد:

$$\alpha = e^{i\theta_1|\alpha|}, \beta = e^{i\theta_2|\beta|}$$

که در آن $\theta 1$ و $\theta 2$ به ترتیب فازهای α و β هستند.

بنابراین، اختلاف فاز آنها ۱ - ۲ است. با توجه به رفتارگیت تغییر فاز، تغییر فاز α صفر می‌باشد؛اما فاز به + ۲ تغییر می کند. بنابراین، خویشاوندان آنها فاز با تغییر می کند.

state basis second the to applied only is shift phase the why explains also This phase the in change no be will there both، to applied is it If meaningful. be to difference.

(۱ ۰ ۰ -۱) = (۱ ۰ ۰ e iπ) زیرا e iπ = cos π + i sin π = -۱.

این ماتریس پائولی σ_z می‌باشد؛ که به آن Z-gate نیز می گویند. گیت تغییر فاز، فاز نسبی $vert0\rangle$و ۱ را با تغییر می دهد. و به این ترتیب گیت Z فاز نسبی را با π تغییر می دهد.

۲.۳.۱ گیت مبادله

یک گیت مبادله[۱۲] اعداد را در حالت های پایه یک رجیستر ۲ کیوبیتی جابجا می کند. اگر فقط حالت های پایه را در نظر بگیریم، معادل مبادله حالات دو الکترون است. این گیت به صورت زیر تعریف می‌شود:

$$U_{SWAP}|ab\rangle = |ba\rangle$$

که در آن a و b فقط اعداد کیوبیت اول و دوم در پایه هستند. a و b می‌توانند مقادیر ۰ و ۱ را اتخاذ کنند. بنابرین می‌توان نوشت:

$$U_{SWAP}|00\rangle = |00\rangle$$
$$U_{SWAP}|01\rangle = |10\rangle$$
$$U_{SWAP}|10\rangle = |01\rangle$$
$$U_{SWAP}|11\rangle = |11\rangle$$

بنابراین، تنها $|01\rangle$ و $|10\rangle$ تحت مبادله (به یکدیگر) تغییر می کنند. اعمال این گیت برای حالات $|00\rangle$ و $|11\rangle$، بدون اثر است؛ زیرا "۰" و "۰" یا "۱" و "۱" تعویض می‌شوند؛ که پیامد خاصی در پی ندارد.

نمایش ماتریسی گیت مبادله

نمایش ماتریسی U_{SWAP} به شکل زیر است:

$$U_{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

از آنجایی که این یک گیت ۲ کیوبیتی برای عملیات است یک بردار در فضای چهار بعدی ^{4}، ماتریس

[۱۲] Swap gate

(یا عملگر) باید ۴ × ۴ باشد. علاوه بر این، فقط حالت پایه دوم و سوم را جابجا می کند. بنابراین، تنها ردیف دوم و سوم با ماتریس یکه متفاوت هستند. به طور مثال:

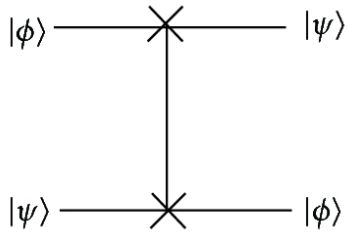
$$U_{SWAP}|10\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = |01\rangle$$

این رابطه بصورت معکوس نیز برقرارست.

گیت مبادله در مدار و خصوصیات آن

به طور کلی، برای یک بردار ۲ کیوبیتی، نظیر $|\Psi\rangle = \alpha|00\rangle + \gamma|01\rangle + \beta|10\rangle + \delta|11\rangle$ داریم:

$$\boldsymbol{U_{SWAP}}|\Psi\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha \\ \gamma \\ \beta \\ \delta \end{pmatrix}$$
$$= \alpha|00\rangle + \gamma|01\rangle + \beta|10\rangle + \delta|11\rangle$$



شکل ۲.۱: نمایش گیت کوانتومی مبادله در مدار کوانتومی

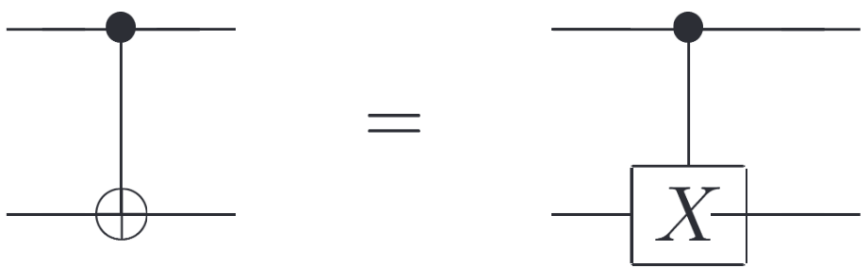
همانطور که انتظار می رود، ضرایب حالت های پایه دوم و سوم با هم مبادله می شوند.

۴.۱ مدارهای کوانتومی

مدارهای کوانتومی[۱۳]، یک دسته از گیت های کوانتومی،که با یک توالی بخصوص قرار گرفته اند، می‌باشند. این کیوبیت ها، با توالی یاد شده، روی یک یا چند دسته کیوبیت، اثر داده می‌شوند.

مدارهای کوانتومی، یکی از اولین مفهوم‌های بکاررفته برای تعریف کامپیوترهای کوانتومی می‌باشند. برای تعریف و شبیه‌سازی هریک از پدیده‌ها و الگوریتم‌های کوانتومی، نیاز به پیاده‌سازی یک مدار به‌خصوص داریم.

مدارهای کوانتومی یک ابزار قدرتمند برای محاسبات کوانتومی هستند. آنها می توانند برای پیاده سازی طیف گسترده ای از الگوریتم های کوانتومی، از جمله الگوریتم شاور برای رمزگشایی اعداد صحیح و الگوریتم گروور برای جستجوی پایگاه داده های بدون ترتیب استفاده شوند.



شکل ۳.۱: نمایش‌های مختلف گیت CNOT در مدار کوانتومی

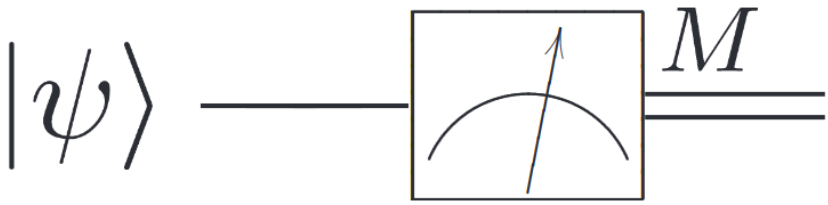
یکی دیگر از عملگرهای مهم در مدار کوانتومی، عملگر اندازه‌گیری است. که در شکل زیر نشان داده شده است. همانطور که پیش از این بیان شد؛ در بردار حالت $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ هنگام مشاهده به یک حالت کلاسیکی رمبش می‌کند؛احتمال اینکه به حالت $|0\rangle$رمبش کند، $|\alpha|^2$، و احتمال اینکه به حالت $|1\rangle$ رمبش کند، $|\beta|^2$، می‌باشد.

مدارهای کوانتومی مدلی بسیار سودمند برای شبیه‌سازی فرآیندهای کوانتومی است. این فرآیندها محدود به عملیات‌های محاسباتی نخواهد شد؛ بلکه در اغلب حوزه‌ها اعم از ارتباطات، اختلالات کوانتومی[۱۴] و ... بکارخواهدرفت.

---

[۱۳] circuit quantum

[۱۴] noise quantum



شکل ۴.۱: نمایش‌های مختلف گیت CNOT در مدار کوانتومی

شباهت ها و تفاوت های مدارهای کلاسیک و کوانتومی

مدارهای کوانتومی مشابه مدارهای کلاسیک هستند، اما از دروازه های کوانتومی به جای دروازه های منطقی کلاسیک استفاده می کنند. دروازه های کوانتومی عملیات قابل برگشت هستند که می توانند برای دستکاری حالت کوانتومی یک کیوبیت استفاده شوند.

شباهت ها

- هر دو مدار کوانتومی و کلاسیک از یک دنباله عملیاتی تشکیل شده اند که به یک مجموعه داده اعمال می شوند.
- هر دو مدار را می توان به صورت گرافیکی با نماد مشابهی نشان داد.
- هر دو مدار می توانند برای پیاده سازی الگوریتم ها استفاده شوند.

تفاوت ها

- مدارهای کوانتومی از کیوبیت ها، که معادل کوانتومی مفهوم بیت هستند، به عنوان واحد پایه داده خود استفاده می کنند.
- مدارهای کلاسیک از بیت ها ، که بیت های کلاسیک هستند ، به عنوان واحد پایه داده خود استفاده می کنند.
- مدارهای کوانتومی از دروازه های کوانتومی ، که عملیات قابل برگشت هستند ، به عنوان عملیات پایه خود استفاده می کنند.
- مدارهای کلاسیک از دروازه های منطقی ، که عملیات برگشت ناپذیر هستند ، به عنوان عملیات پایه خود استفاده می کنند.

- مدارهای کوانتومی می توانند خواص مکانیک کوانتوم را ، مانند برهمنهی و درهمتنیدگی ، برای انجام کارهایی که برای رایانه های کلاسیک غیرممکن است ، بهره مند شوند.

ویژگی	مدار کوانتومی	مدار کلاسیک
واحد پایه داده	کیوبیت	بیت
عملیات پایه	دروازه های کوانتومی	دروازه های منطقی
برگشت پذیری	قابل برگشت	برگشت ناپذیر

جدول ۱.۱: شباهت‌ها و تفاوت های مدارهای کلاسیک و کوانتومی

اجزای مدارهای کوانتومی و سایز آن

اندازه مدار کوانتومی اندازه یک مدار کوانتومی تعداد دروازه های موجود در مدار است. پیچیدگی یک الگوریتم کوانتومی اغلب با اندازه مدار کوانتومی مورد نیاز برای پیاده سازی آن اندازه گیری می شود.

کیوبیت کیوبیت ها واحد پایه اطلاعات در محاسبات کوانتومی هستند. آنها می توانند در یک برهنهی کوانتومی از دو حالت ، ۰ و ۱ باشند. این بدان معنی است که یک کیوبیت می تواند هم ۰ و هم ۱ باشد ، که یک ویژگی به نام برهمنی کوانتومی است. کیوبیت ها همچنین می توانند به هم متصل شوند ، که به این معنی است که حالت یک کیوبیت به حالت کیوبیت دیگر وابسته است.

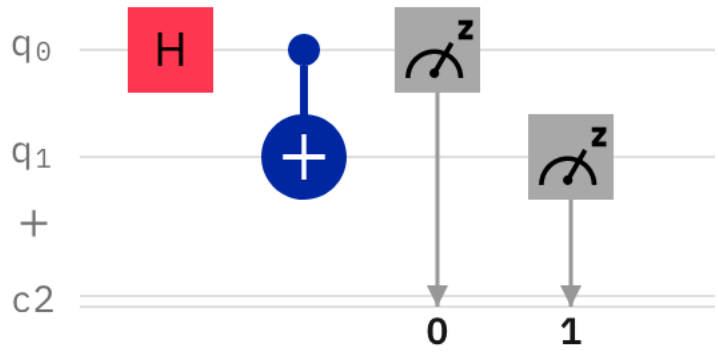
دروازه دروازه ها عملیاتی هستند که روی کیوبیت ها اعمال می شوند. آنها می توانند برای ایجاد برهمنهی ، انجام چرخش ها و درهم تنیدگی کیوبیت ها استفاده شوند. انواع مختلفی از دروازه ها وجود دارد ، اما برخی از رایج ترین آنها شامل گیت هادامارد ، گیت CNOT و گیت توفولی است.

عملیات عملیات اقداماتی هستند که روی کیوبیت ها انجام می شوند. آنها می توانند اندازه گیری ها یا سایر اقدامات باشند. اندازه گیری ها برای رمبش حالت کوانتومی یک کیوبیت به یک مقدار قطعی ، ۰ یا ۱ استفاده می شود.

اجزای اساسی یک مدار کوانتومی کیوبیت ها ، دروازه ها و عملیات هستند. این اجزا برای ایجاد الگوریتم های کوانتومی استفاده می شوند که الگوریتم هایی هستند که فقط می توانند روی یک رایانه کوانتومی اجرا شوند. مدارهای کوانتومی یک ابزار قدرتمند برای محاسبات کوانتومی هستند و پتانسیل انقلابی در بسیاری از زمینه های مختلف ، از جمله رمزنگاری ، شیمی و یادگیری ماشین را دارند.

۱.۴.۱ نحوه‌ی نمایش مدارهای کوانتومی

مدارهای کوانتومی با استفاده از نماد گرافیکی مشابه نمودارهای مدار استفاده شده در محاسبات کلاسیک نوشته می شوند. محور افقی یک مدار کوانتومی زمان را نشان می دهد و محور عمودی کیوبیت ها را نشان می دهد. دروازه ها توسط جعبه ها نشان داده می شوند و خطوط بین جعبه ها نشان دهنده ارتباطات بین کیوبیت ها است.



شکل ۱.۵: مدارکوانتومی شبیه‌سازی شده برای آزمایش درهمتنیدگی

فصل ۲

برنامه‌نویسی کوانتومی

برنامه نویسی کوانتومی فرآیند طراحی و پیاده‌سازی دنباله هایی از دستورالعمل هایی موسوم مدارهای کوانتومی می‌باشد، با استفاده از گیت ها، سوئیچ ها و عملگرها برای دستکاری وضعیت کوانتومی یک کیوبیت به پردازش مسائل می‌پردازیم.

مدارهای کوانتومی یک نمایش گرافیکی از الگوریتم های کوانتومی هستند، این الگوریتم هایی فقط روی یک کامپیوتر کوانتومی قابل اجرا هستند.

برنامه نویسی کوانتومی یک زمینه نسبتاً جدید است و تعدادی زبان برنامه نویسی کوانتومی مختلف در دسترس است. برخی از محبوب ترین زبان های برنامه نویسی کوانتومی عبارتند از Qiskit، Cirq و Quil.

برنامه نویسی کوانتومی یک زمینه پیچیده و چالش برانگیز است، اما این پتانسیل را دارد که در بسیاری از زمینه های مختلف از جمله رمزنگاری، شیمی و یادگیری ماشین انقلابی ایجاد کند. با قدرتمندتر شدن کامپیوترهای کوانتومی، برنامه نویسی کوانتومی اهمیت فزاینده ای پیدا خواهد کرد.

۱.۲ کامپیوترهای کوانتومی در مقابل کامپیوترهای کلاسیک

کامپیوترهای کوانتومی و کامپیوترهای کلاسیک دو نوع بسیار متفاوت از رایانه هستند. کامپیوترهای کوانتومی از بیت‌های کوانتومی (کیوبیت‌ها) برای ذخیره اطلاعات استفاده می‌کنند، در حالی که کامپیوترهای کلاسیک از بیت‌ها استفاده می‌کنند. کیوبیت‌ها می‌توانند در حالت برهم‌نهی دو حالت، ۰ و ۱، به‌طور همزمان باشند، در حالی که بیت‌ها فقط می‌توانند در یک حالت به‌طور همزمان باشند. این تفاوت در نحوه ذخیره اطلاعات امکان محاسباتی را برای کامپیوترهای کوانتومی فراهم می‌کند که برای کامپیوترهای

کلاسیک غیرممکن است.

علاوه بر تفاوت در نحوه ذخیره اطلاعات، کامپیوترهای کوانتومی و کلاسیک در نحوه انجام محاسبات نیز متفاوت هستند. کامپیوترهای کوانتومی از مکانیک کوانتوم برای انجام محاسبات استفاده می‌کنند، در حالی که کامپیوترهای کلاسیک از منطق بولی استفاده می‌کنند. این تفاوت در نحوه انجام محاسبات نیز به کامپیوترهای کوانتومی امکان می‌دهد تا برای برخی از وظایف، محاسباتی را بسیار سریع‌تر از کامپیوترهای کلاسیک انجام دهند.

کاربردهای بالقوه کامپیوترهای کوانتومی بسیار گسترده است. آنها می‌توانند برای رمزگشایی روش‌های رمزنگاری فعلی، شبیه‌سازی مولکول‌ها و آموزش مدل‌های یادگیری ماشینی که بسیار دقیق‌تر از مدل‌های فعلی هستند، استفاده شوند. کامپیوترهای کوانتومی هنوز در مراحل اولیه توسعه هستند، اما پتانسیل تغییر جهان را دارند. هنگامی که کامپیوترهای کوانتومی قدرتمندتر شوند، قادر به حل مشکلاتی خواهند بود که برای کامپیوترهای کلاسیک در حال حاضر غیرممکن است.

برخی از مثال‌های خاص از نحوه استفاده از کامپیوترهای کوانتومی:

رمزنگاری : کامپیوترهای کوانتومی می‌توانند برای رمزگشایی روش‌های رمزنگاری فعلی استفاده شوند، که تأثیر عمده‌ای بر امنیت آنلاین خواهد داشت.

شبیه‌سازی مواد در علم شیمی :کامپیوترهای کوانتومی می‌توانند برای شبیه‌سازی مولکول‌ها استفاده شوند، که می‌تواند به دانشمندان در توسعه داروها و مواد جدید کمک کند.

یادگیری ماشینی : کامپیوترهای کوانتومی می‌توانند برای آموزش مدل‌های یادگیری ماشینی که بسیار دقیق‌تر از مدل‌های فعلی هستند، استفاده شوند.

آینده محاسبات کوانتومی بسیار روشن است. هنگامی که کامپیوترهای کوانتومی قدرتمندتر شوند، قادر به حل مشکلاتی خواهند بود که برای کامپیوترهای کلاسیک در حال حاضر غیرممکن است. این می‌تواند منجر به پیشرفت‌های عمده در بسیاری از زمینه‌های مختلف شود.

۲.۲ شبیه‌سازی کلاسیک در مقابل کامپیوتر کوانتومی

بسیاری از مسائل کوانتومی و بسیاری از الگوریتم‌های کوانتومی قابل شبیه‌سازی روی کامپیوترهای کوانتومی می‌باشند. بنابرین یک سوال به‌واقع مهم مطرح می‌شود: **چرا به یک کامپیوتر کوانتومی نیاز داریم؟**

در هنگام محاسبات کوانتومی، کامپیوترهای کلاسیک دارای محدودیت‌هایی هستند. به طور مشابه کامپیوترهای کوانتومی نیز دارای معایبی هستند؛ که قابل بحث و بررسی هستند. دراین بخش به این مزایا و معایب هرکدام از کامپیوترها می‌پردازیم و در ادامه به اهداف تعریف شده برای کامپیوترهای کوانتومی می‌پردازیم.

۱.۲.۲ تفاوت کامپیوترهای کوانتومی و شبیه‌سازهای کلاسیک

همانطور که در بخش‌های قبلی گفته شد؛ کامپیوترهای کوانتومی با استفاده از کیوبیت‌ها تعریف می‌شوند. یک کیوبیت به صورت یک ترکیب خطی از حالت $|0\rangle$ و $|1\rangle$ تعریف می‌شود:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

هریک از حالات داخل رابطه‌ی بالا به صورت یک ماتریس قابل تعریف هستند. به طور مشابه هریک از عملگر های کوانتومی را می‌توان به صورت یک ماتریس تعریف کرد. ماتریس‌هایی مشابه ماتریس پائولی یا در مقیاس‌های بالاتر ماتریس فردکین که برای سه کیوبیت تعریف می‌شود؛ و محاسبات را سریع می‌سازد.

از طرفی دیگر تعداد محاسبات در مدارهای کلاسیک به تعداد حالات مسأله بستگی دارد. در محاسبات کلاسیک هرچه تعداد حالات بالاتر برود؛ پیچیدگی محاسبات بالاترمی‌رود و حتی اغلب با حالت نمایی رشد می‌کنند. این درحالیست که در محاسبات کوانتومی هر یک حالات مختلف مسأله به یک دنیای موازی کوانتومی شیفت داده می‌شود و از این طریق محاسبات به زمان و منابع کمتری نیاز دارد.

مهم‌ترین عامل در سطح پیچیدگی محاسبات کوانتومی همدوسی می‌باشد. همدوسی در محاسبات کوانتومی اصلی ترین منبع خطا در این سیستم ها است. کیوبیت ها بسیار به محیط خود هستند و می توانند به راحتی توسط تعامل با فوتون ها، الکترون ها و سایر ذرات با آن‌ها دچار ناهمدوسی شوند. این می تواند باعث شود که کیوبیت ها خواص کوانتومی خود را مانند برهمنهی کوانتومی و درهمتنیدگی که برای انجام محاسبات کوانتومی ضروری هستند، از دست بدهند.

ناهمدوسی می‌تواند به دلایل مختلفی ایجاد شود:

دما کیوبیت ها در دماهای بالاتر مستعد دکوراسیون هستند. این به این دلیل است که هرچه دما بالاتر باشد، کیوبیت ها انرژی بیشتری دارند و بیشتر احتمال دارد با محیط خود تعامل داشته باشند.

برخورد کیوبیت ها همچنین می توانند توسط ارتعاشات دکور شوند. این به این دلیل است که ارتعاشات می توانند باعث حرکت کیوبیت ها شوند، که می تواند حالت های کوانتومی آنها را مختل کند.

تابش الکترومغناطیسی کیوبیت ها می توانند توسط تابش الکترومغناطیسی، مانند نور و امواج رادیویی، دکور شوند. این به این دلیل است که تابش الکترومغناطیسی می تواند با الکترون های کیوبیت ها تعامل داشته باشد و باعث از دست رفتن خواص کوانتومی آنها شود.

ناهمدوسی یک مانع بزرگ برای توسعه ابررایانه های کوانتومی است. برای ساخت یک رایانه کوانتومی عملی، باید راه هایی برای کاهش ناهمدوسی پیدا کرد. این یک مشکل بزرگ ولی قابل حل است؛ اما تعدادی از مسیرهای تحقیقاتی امیدوار کننده وجود دارد، مانند:

سردسازی کیوبیت‌ها این می تواند انرژی کیوبیت ها را کاهش دهد و آنها را کمتر مستعد تعامل با محیط خود کند.

استفاده از مواد با همدوسی بالا برخی از مواد، مانند ابررساناها، زمان های همدوسی بسیار طولانی دارند که آنها را برای استفاده در رایانه های کوانتومی بسیار مناسب می کند.

توسعه‌ی الگوریتم‌های جایگزین برای تصحیح خطای کوانتومی الگوریتم های تصحیح خطا کوانتومی می توانند برای تشخیص و تصحیح خطاهایی که توسط ناهمدوسی ایجاد می شوند استفاده شوند.

۳.۲ شبیه‌سازی کلاسیک

حال که به اهمیت مسأله‌ی همدوسی در حل محاسبات پی بردیم لازم‌است به نارسایی کامپیوترهای کلاسیک در برخورد با این مفهوم بپردازیم:

عکس از چنل یوتیب بذار و کدها رو باهم مقایسه کن.

۴.۲ کامپیوترکوانتومی IBM و زبان برنامه‌نویسی QisKit

۱.۴.۲ معرفی QisKit

یک زبان برنامه‌نویسی کوانتومی است. این زبان دارای مشابهت‌های زیادی با زبان پایتون می‌باشد. دو دلیل عمده برای این شباهت وجود دارد:

۱. این زبان براساس زبان پایتون و برخی کتابخانه‌های آن ساخته شده است.

۲. جامعه دانشمندان کوانتوم و به‌طور کلی فیزیکدانان از سابق برای انجام شبیه‌سازی‌های خود از زبان پایتون استفاده می‌کنند و پایتون نیز کتابخانه‌هاي بسیار کارآمدی - نظیر نامپای[۱] ، پانداس[۲] ، سایپای[۳] و .. - ارائه کرده است.

۲.۴.۲ کدنویسی به زبان QisKit

برای کدنویسی به زبان QisKit می‌توان از محیط Jupyter notebook استفاده کرد. پس از نصب Qiskit برای فرخواندن این کتابخانه به راحتی می‌توان نوشت:

```
import qiskit
```

هدف از برنامه نویسی کوانتومی پیاده‌سازی مسائل کوانتومی روی کامپیوترکوانتومی واقعی است. بدین منظور ابتدا یک شبیه سازی روی سیستم خود انجام داده و سپس کد خود را به کامپیوترکوانتومی IBM ارسال می‌کنیم.بدین منظور می‌بایست یک حساب کاربری در سایت مرتبط به کامپیوتر کوانتومی IBM ایجاد کنیم.

۳.۴.۲ قواعد نوشتاری و ساختار داده

هرزبان برنامه نویسی دارای ساختار داده و دستورات نگارشی مخصوص به‌خود است؛ QisKit نیز از این قاعده مستثنی نیست. بدین دلیل در ادامه به اختصار به معرفی برخی دستورات این زبان می‌پردازیم. باید خاطر نشان کرد که این متن براساس QisKit نسخه‌ی ۰.۴۴.۰ نوشته شده‌است.

هدف نهایی این برنامه‌ها، پیاده‌سازی یک مدار کوانتومی منتسب به یک مسئله‌ی خاص است. پس نیاز به تعریف و ایجاد کیوبیت داریم. برای تعریف کیوبیت از راه زیر استفاده می‌کنیم:

```
quantum_register = QuantumRegister(n)
```

---

[۱] Numpy
[۲] Pandas
[۳] Scipy

که در آن n تعداد کیوبیت‌های داخل کوانتوم رجیستر مدنظر برنامه نویس است.

```
classic_register = ClassicalRegister(n)
```

که در آن n تعداد بیت‌های داخل رجیستر کلاسیک مدنظر برنامه نویس است.

درنهایت می‌توان با قرار دادن این دو رجیسترایجاد شده، در یک مدار، یک مدار کوانتومی ایجاد کنیم:

```
circuit = QuantumCircuit(quantum_register, classic_register)
```

پس از ایجاد مدار می‌توان عملگرهای مدنظر خود نظیر هادامارد و CNOT و ... را روی بخش‌های مختلف مدار اثر داد. از طرفی می‌توان مدار ایجاد شده را به صورت یک تصویر به کاربر نشان داد.

۴.۴.۲ پیاده‌سازی گیت‌های کوانتومی

برای اعمال یک گیت کوانتومی روی اجزای یک مدار کوانتومی،ابتدا باید نام مدار کوانتومی را نوشت؛ سپس نام گیت کوانتومی را نوشت؛ سپس نام کیوبیت یا بیت مدنظر را نوشت:

```
circuit.gate_sing_inQisKit(Qubit_name, Bit_name)
```

در کد بالا به جای gate_sing_inQisKit() نام هر گیت کوانتومی مدنظر برنامه‌نویس می‌تواند باشد.

۵.۴.۲ تصویر سازی

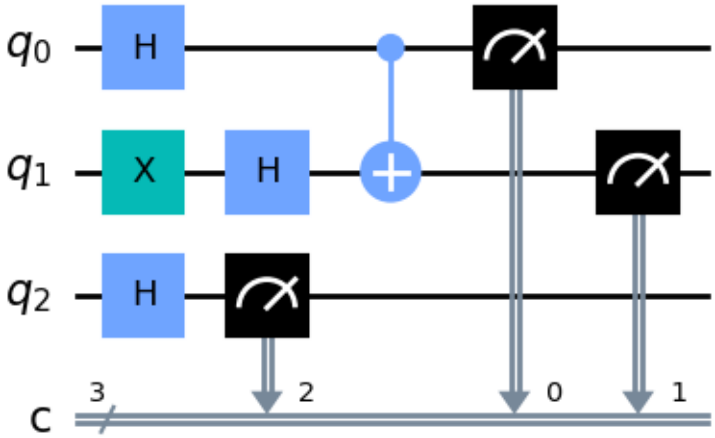
برای تصویر کردن وضعیت مدار کوانتومی می‌بایست از راه زیر استفاده کرد:

```
# to run commands and show diagram in a easier way.
%matplotlib inline

# draw circuit
circuit.draw()

# we can change look of diagram.
circuit.draw(output = "mpl")  # output = "mpl" is defining type of circuit output
```

درنهایت خروجی مشابه خروجی های زیر را می‌توان از این زبان برنامه نویسی دریافت کرد:



شکل ۱.۲: نمونه‌ای از خروجی Qiskit

فصل ۳

الگوریتم‌های کوانتومی

چه گونه‌ای از مسائل محاسباتی قابل اجرا با مدارهای کوانتومی می‌باشند؟ تفاوت و برتری مدارهای کوانتومی نسبت به مدارهای کلاسیک چیست؟ آیا می‌توان یک حوزه‌ی خاص را تعیین کرد؛ به گونه‌ای که عملکرد کامپیوترهای‌کوانتومی نسبت به کامپیوترهای کلاسیک مزیت داشته باشند؟

در این بخش می‌خواهیم به طور خلاصه این سوالات را پاسخ دهیم و توضیح دهیم چگونه می‌توان از کامپیوترهای کوانتومی به شکلی سودمند استفاده کنیم.

۱.۳ موازی سازی کوانتومی

موازی‌سازی کوانتومی[۱]، پایه‌واساس بسیاری از الگوریتم‌های کوانتومی است. با گذار یک حالت کوانتومی به حالت برهمنهی کوانتومی، درحین محاسبات کوانتومی یک تابع نظیر $\mathrm{f(x)}$، می‌تواند مقادیر مختلف x را به طور همزمان بررسی کند. این درحالیست که در محاسبات کلاسیک به دلیل ماهیت بیت‌های اطلاعات، تابع $\mathrm{f(x)}$ فقط می‌تواند یکی از مقادیر مجاز برای x را بررسی کند.

فرض کنید تابع f ،یک تابع تک‌ـ کیوبیت، به صورت زیر تعریف شده است:

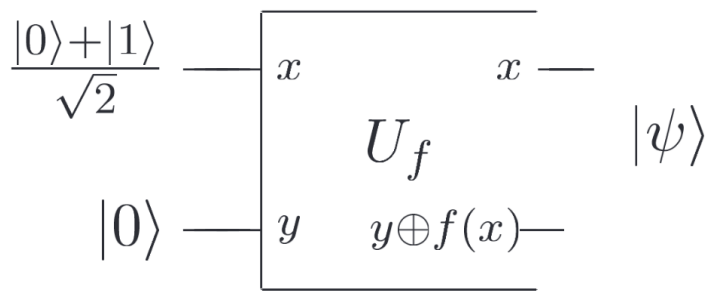
$$f(x) : \{0,1\} \to \{0,1\}$$

روش مناسب برای محاسبه این تابع در یک کامپیوتر کوانتومی، با در نظر گرفتن دو کیوبیت که در حالت $|x,y\rangle$شروع می شود. با یک توالی مناسب از گیت های منطقی می توان این حالت را به

[۱] parallelism Quantum

$|f(x) \oplus x, y\rangle$ تبدیل کرد که در آن $\oplus$ بیانگر جمع مدوله با پایه۲ می‌باشد.
۲

هریک از دسته‌های کیوبیت، **رجیستر کوانتومی** نامیده‌می‌شوند. اولین رجیستر، «رجیستر داده» و دومین رجیستر «رجیستر هدف» نامیده می‌شود.
ازین پس در این بخش به عامل گذار $|x, y\rangle \to |x, y \oplus f(x)\rangle$، عنوان «تابع U_f» را اطلاق خواهیم کرد. لازم به ذکرست که این تبدیل، یک تبدیل یکه به شمار می‌آید.[۳]
اگر $y = 0$ آنگاه مقدار دومین کیوبیت بعد از اعمال تابع U_f برابر با مقدار $f(x)$ خواهد بود.



شکل ۱.۳: مدار کوانتومی برای ارزیابی $f(0)$ و $f(1)$ به طور همزمان. Uf مدار کوانتومی است که ورودی هایی مانند $|x, y\rangle$ را به $|x, y \oplus f(x)\rangle$، تصویر می‌کند.

در شکل بالا مقادیر ورودی داده شده به تابع U_f در پایه‌های محاسباتی قرار ندارند. رجیستر داده در حالت برهمنهی قرار دارد. این حالت برهمنهی را می‌توان با اعمال گیت هادامارد بر حالت کوانتومی $|0\rangle$

[۲] Modulo ۲ is a mathematical operation that returns the remainder of a division by ۲. For ex-
ample، ۵ mod ۲ is ۱، because ۵ divided by ۲ has a quotient of ۲ and a remainder of ۱.
The symbol "⊕" is often used to indicate modulo addition ۲. So، the expression "۵ ⊕ ۳" would
be evaluated as follows:
۵ ⊕ ۳ = (۵ + ۳) mod ۲ = ۸ mod ۲ = This is because ۸ divided by ۲ has a quotient of ۴ and a
remainder of ۰.
Modulo ۲ is a useful operation in many different areas of mathematics، computer science،
and cryptography. It also is used in everyday life، for example، checking whether a number is
even or odd.
Here are some other examples of modulo ۲:
۱ = ۲ mod ۱ ۱ = ۲ mod ۲ ۰ = ۲ mod ۳ ۱ = ۲ mod ۴ ۰ = ۲ mod ۵ = ۱

[۳] اثبات این مطلب از حوصله‌ی بحث خارج است.

ایجاد کرد. پس از ایجاد این حالت، تابع U_f را به حالت جدید اعمال می‌کنیم:

$$\frac{|0,f(0)\rangle+|1,f(1)\rangle}{\sqrt{2}}$$

این یک حالت استثنایی است! جملات مختلف کسر بالا حاوی اطلاعاتی در مورد$f(0)$ و$f(1)$ می‌باشند؛ به‌نحوی که انگار $f(x)$ را برای دو مقدار x به طور همزمان ارزیابی کرده ایم، این ویژگی به "موازی سازی کوانتومی" موسوم می‌باشد. بر خلاف موازی سازی کلاسیک، که در آن هر یک مدارهای متعددی دارند ساخته شده برای محاسبه $f(x)$ به طور همزمان اجرا می شوند، در اینجا برای ارزیابی تابع برای چندین مقدار x به طور همزمان، یک مدار $f(x)$ (با قابلیت برهمنهی کوانتومی)استفاده می شود.

این فرآیند را می توان به راحتی با استفاده از یک عمل کلی به نام تبدیل هادامارد، به توابعی با تعداد بیت دلخواه تعمیم داد. این عمل فقط تعداد n گیت هادامارد است که به طور موازی روی nکیوبیت عمل می کنند.

برای مثال در شکل زیر؛ دو کیوبیت در حالت $|0\rangle$ آماده شده‌اند. پس از اعمال گیت‌های هادامارد بر روی این رجیستر به خروجی زیر خواهیم رسید:

$$\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)=\frac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{\sqrt{2}}$$

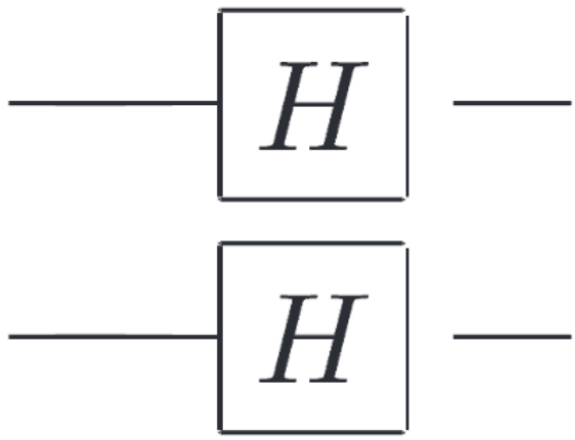
از نماد $\mathrm{H}\otimes 2$ به عنوان نشانه‌ی عملکرد موازی دو گیت هادامارد استفاده می‌کنیم؛از علامت $\otimes$ به عنوان تانسور یاد می‌کنیم. به طور کلی نتایج اعمال موازی گیت هادامارد روی n کیوبیت روی حالت کوانتومی برابرست با:

$$\frac{1}{\sqrt{2}}\sum_x |x\rangle$$

در اینجا، $\sum$ نشان دهنده جمع بر روی همه مقادیر ممکن x است، و ما$\mathrm{H}\otimes n$ را برای نشان دادن این عمل می نویسیم. اعمال تبدیل هادامارد روی یک بهمنهی کوانتومی برابر از همه حالت های محاسباتی تولید می کند؛ و با استفاده از فقط n گیت، یک برهمنهی از $2n$ حالت تولید می کند.

تبدیل هادامارد $\mathrm{H}\otimes 2$ روی دو بیت کوانتومی پیاده می‌شود. ارزیابی موازی کوانتومی یک تابع f(x) با ورودی n بیتی x و خروجی ۱ بیتی، به روش زیر قابل پیاده‌سازی می‌باشد:

۱. ابتدا حالت $n+1$ کیوبیت $|0\rangle^{\otimes n}|0\rangle$ را آماده کنید،



شکل ۲.۳: اعمال تبدیل هادامارد $\mathrm{H}\otimes n$ روی دو کیوبیت

۲. سپس تبدیل هادامارد را به n کیوبیت اول و به دنبال آن مدار کوانتومی اعمال کنید.

۳. اعمال تابع U_f به کیوبیت‌هایی که در حالت برهمنهی قرار دارند.

درنهایت حالت زیر تولید می‌شود:

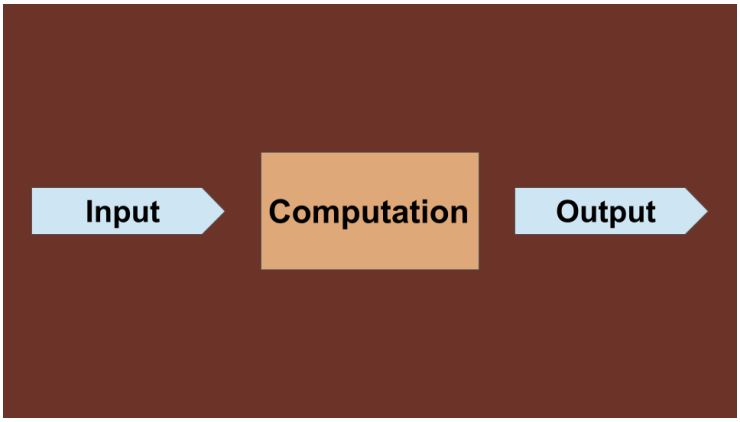
$$\frac{1}{\sqrt{2^n}}\sum_x |x\rangle|f(x)\rangle$$

به طور کلی موازی‌سازی کوانتومی امکان ارزیابی همزمان همه مقادیر ممکن تابع f را فراهم می‌کند، حتی اگر ظاهراً فقط یک بار f را ارزیابی کرده باشیم. با این حال، این موازی‌سازی بلافاصله مفید نیست.

در مثال تک کیوبیتی ما، اندازه‌گیری حالت فقط $|0, f(0)\rangle$ یا $|1, f(1)\rangle$ را می‌دهد! به طور مشابه، در حالت کلی، اندازه‌گیری حالت $\sum_x |x, f(x)\rangle$ فقط $f(x)$ را برای یک مقدار x خاص می‌دهد. البته یک کامپیوتر کلاسیک می‌تواند این کار را به راحتی انجام دهد! محاسبات کوانتومی برای مفید بودن به چیزی بیش از موازی‌سازی کوانتومی نیاز دارد؛ به توانایی استخراج اطلاعات مربوط به بیش از یک مقدار $f(x)$ از حالت‌های برهمنهی مانند $\sum_x |x, f(x)\rangle$ نیاز دارد. در بخش های بعدی به مثال‌های خواهیم پرداخت که این مسائل را حل کند.

۱.۱.۳ مدل محاسباتی استاندارد

پیش از بررسی مدل کوئری، مدل ساده و استاندارد محاسباتی را بررسی می‌کنیم. به تصویر زیر دقت کنید:



شکل ۳.۳: یک واحد محاسباتی که مقادیری را به عنوان ورودی گرفته، پردازش کرده و سپس مقدار/مقادیر خروجی را ارائه کرده است.

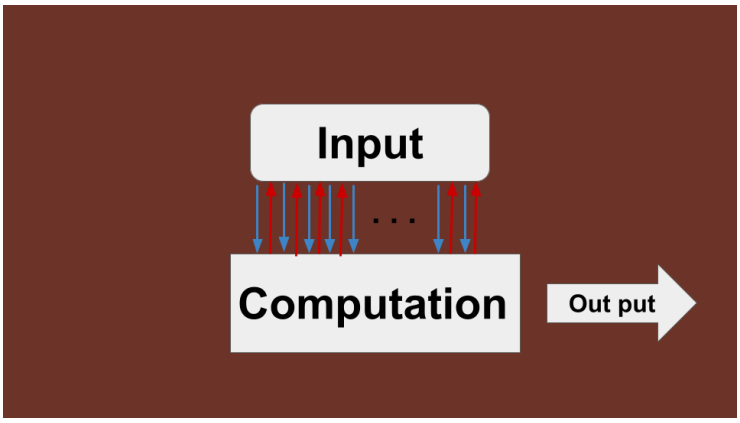
در تصویر بالا یک نمود ساده از کامپیوترهای امروزی ارائه شده است. در دنیای واقعی مقدار ورودی می‌تواند از هر منبعی تأمین شده باشد. با این وجود هدف ما بررسی منابع تولید ورودی نیست؛ بلکه هدف بررسی مقادیر ورودی (به صورت ایزوله) می‌باشد. می‌توان درنظر گرفت که ورودی داده شده و خروجی نهایی،هر دو در قالب یک رشته از اعداد باینری، ماتریس و یا هرقالب مدنظر کاربر باشند.

مهم‌ترین نکته درباره‌ی این واحد محاسباتی، **در دسترس بودن کل مقادیر ورودی برای واحد پردازش** است. به عبارت دیگر **واحد پردازش می‌تواند تمامی مقادیر ورودی را دریافت کرده و تشخیص** دهد.

۲.۳ مدل کوئری

در مدل کوئری، داده‌های ورودی توسط یک تابع تولید می‌شوند. واحد محاسباتی دسترسی به تابع تولیدورودی دارد و می‌تواند برای دریافت داده‌های جدید،از تابع یاد شده،درخواست کند.

در این مدل واحد محاسباتی دیگر داده‌ها را در قالب رشته‌ای از اطلاعات دردسترس ندارد؛ بلکه می‌تواند آن‌ها را از بخش تولید ورودی دریافت کند. در گاهی از مواقع به سیستم ورودی، Oracle یا جعبه‌ی سیاه می‌گویند. تابع Oracle یا جعبه‌ی سیاه یک سیستم است که ما به عنوان ناظر به سازوکار داخلی آن و تمامی اطلاعات آن دسترسی نداریم و فقط می‌توانیم مقادیر مجاز را به آن داده و مقادیر خروجی



شکل ۴.۳: شکل بالا نمود مدل محاسباتی‌کوئری است. واحد محاسباتی برای دریافت داده‌های جدید نیاز به درخواست از تابع input دارد. خطوط قرمز و روبه‌بالا نشان از درخواست واحد محاسباتی و خطوط آبی روبه‌پایین نشان از پاسخ واحد inputمی‌باشد.

را دریافت کنیم.

تابع oracle به صورت زیر تعریف می‌شود:

$$\begin{cases} f : \sum^n = \sum^m \\ Which : m, n \in \mathbb{N} \end{cases}$$

ما در این نظریه کوئری‌ها را می‌شماریم و وضعیت آن‌ها را بررسی می‌کنیم.

۳.۳ معرفی و پیاده سازی الگوریتم دوچ

۱.۳.۳ مسئله‌ی دوچ

الگوریتم دوچ اولین و ساده‌ترین الگوریتم کوانتومی است. این الگوریتم برای اولین بار در سال ۱۹۸۵ در مقاله‌ای مطرح شد؛ که توسط دیوید دوچ[۴] نوشته شده‌بود. این الگوریتم نقطه‌ی شروعی برای اثبات برتری کامپیوترهای کوانتومی نسبت به کامپوترهای کلاسیک است.

مسئله‌ی Deutsch یکی از ساده‌ترین مفاهیم ممکن را مطرح می‌کند. اگر یک تابع به فرم زیر تعریف شود:

[۴] David Deutsch

$$f : \sum \to \sum$$

هدف بررسی ثابت بودن یا متعادل[۵] بودن تابع f است. به‌طور کلی، درساده‌ترین حالت، می‌توان چهار وضعیت را برای تابع $f : \sum \to \sum$ درنظر گرفت:

a	$f_1(a)$
0	0
1	0

a	$f_2(a)$
0	0
1	1

a	$f_3(a)$
0	1
1	0

a	$f_4(a)$
0	1
1	1

شکل ۵.۳:

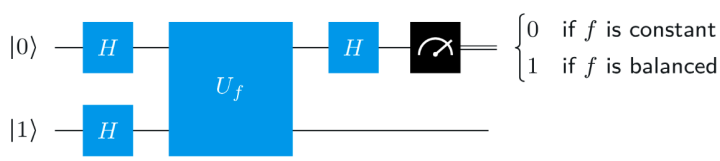
در شکل بالا توابع f 1 ، f 4 توابع ثابت و توابع f 2 و f 3 توابع متعادل هستند.

مسئله‌ی دوچ	
ورودی	$f : \sum \to \sum$
خروجی	صفر اگر تابع ثابت بود؛ یک اگر تابع متعادل بود.

در الگوریتم‌های کلاسیک برای حل این مسئله، حداقل دو حالت باید بررسی شود.

۲.۳.۳ الگوریتم دوچ

حال به بررسی الگوریتم دوچ می‌پردازیم. الگوریتمی که مسئله‌ی دوچ را با یک مدار کوانتومی حل می‌کند:



شکل ۶.۳:

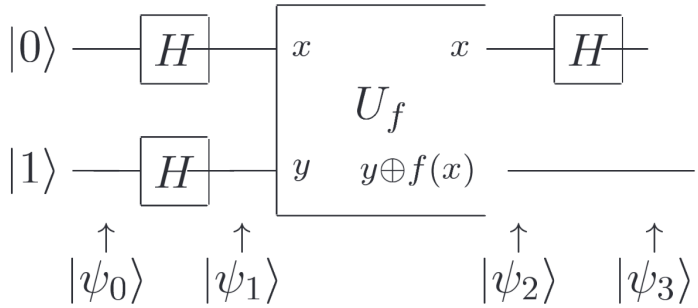
[۵] Constante or balanse.

مدار زیر نشان می دهد که چگونه مدارهای کوانتومی می توانند با پیاده سازی الگوریتم دوچ از مدارهای کلاسیک پیشی بگیرند[۶]. الگوریتم دوچ ترکیبی از موازی سازی کوانتومی با خاصیتی از مکانیک کوانتوم به نام تداخل[۷] است. مشابه قبل،ابتدا از گیت هادامارد برای آماده سازی اولین کیوبیت به عنوان برهمنهی $\frac{(|0\rangle+|1\rangle)}{\sqrt{2}}$ استفاده کنیم، اما اکنون کیوبیت دوم y را با اعمال یک گیت هادامارد به حالت $|1\rangle$ به عنوان بهرهمنهی $\frac{(|0\rangle-|1\rangle)}{\sqrt{2}}$ آماده کنیم. به‌شکل زیر دقت کنید:

---

[۶] ما در واقع یک نسخه ساده شده و بهبود یافته از الگوریتم اصلی را ارائه می دهیم.

[۷] how using in deutsch algorithm : Interference is used in the Deutsch algorithm
constant and balanced between distinguish to functions. A constant function is that function a
returns always the same value، regardless of its input. A balanced function is that function a
returns ۰ for half of its inputs and ۱ for the other half.
The Deutsch algorithm works by preparing two qubits in a superposition of states. First
the qubit prepared in the state |+⟩، which is equal superposition of |0⟩ and |1⟩. The second qubit
prepared in the state |−⟩، which is a superposition of |0⟩ and |1⟩ states with opposite phases.
The two qubits then are passed through a quantum circuit that includes a Hadamard gate and a
CNOT gate. The Hadamard gate transforms |+⟩ into the superposition |0⟩ + |1⟩، and the CNOT
gate copies the state of first qubit to the second qubit.
After the quantum circuit has been executed، the two qubits are measured. If the first qubit is
measured to be |0⟩، then the function f is constant. This is because the state |−⟩ is orthogonal to
the state |0⟩، so the interference between the two states will destructively interfere.
If the first qubit is measured to be |1⟩، then the function f is balanced. This is because the
state |−⟩ is parallel to the state |1⟩، so the interference between the two states will
constructively interfere.
The Deutsch algorithm is a simple example of how quantum interference can be used to solve
problems that are difficult to solve classically. In this case، the Deutsch algorithm can distinguish
between constant and balanced functions in a single step، while a classical computer would need
to take an exponential number of steps.



شکل ۷.۳: پیاده‌سازی مدارکوانتومی الگوریتم دوچ

حالت ورودی:

$$|\psi_0\rangle = |01\rangle$$

سیستم دو کیوبیتی تشکیل شده، پس از اعمال اثر دو گیت هادامارد می‌دهد:

$$|\psi_1\rangle = \left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$

با کمی تأمل می‌توان دریافت که اگر U_f را به حالت $|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$ اعمال کنیم، سپس به حالت $(-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$ می رسیم. بنابرین اعمال U_f به $|\Psi_1\rangle$ ما را با یکی از دو امکان زیر مواجه می کند:

$$|\psi_2\rangle = \begin{cases} \pm\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } f(0) = f(1) \\ \pm\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } f(0) \neq f(1) \end{cases}$$

با اعمال آخرین گیت هادامارد روی کیوبیت اول به حالت زیر خواهیم رسید:

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } f(0) = f(1) \\ \pm|1\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } f(0) \neq f(1) \end{cases}$$

با درنظر گرفتن شرایط زیر می‌توان $|\psi_3\rangle$ را به شکل زیر بازنویسی کرد:

$$\begin{cases} f(0) = f(1) \implies & f(0) \oplus f(1) \quad = 0 \\ f(0) \neq f(1) \implies & f(0) \oplus f(1) \quad = 1 \end{cases}$$

از این رو:

$$|\psi_3\rangle = \pm|f(0) \oplus f(1)\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

بنابراین با اندازه گیری کیوبیت اول می توانیم $f(0) \oplus f(1)$ را تعیین کنیم. واقعاً جالب است! مدار کوانتومی به ما توانایی تعیین یک ویژگی جهانی از $f(x)$، یعنی$f(0) \oplus f(1)$ را داده است، با استفاده از تنها یک ارزیابی از $f(x)$!این سریعتر از آن چیزی است که با یک دستگاه کلاسیک امکان‌پذیر است،یک دستگاه کلاسیک حداقل به دو ارزیابی نیاز دارد. این مثال تفاوت بین موازی‌سازی کوانتومی و الگوریتم‌های تصادفی کلاسیک را برجسته می‌کند. به سادگی، ممکن است تصور شود که حالت $|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle$ مطابقت نزدیکی با یک رایانه کلاسیک تصادفی دارد که هرکدام از حالات $f(0)$ یا$f(1)$ با احتمال $1/2$ اندازه‌گیری می‌کند. تفاوت این است که در یک رایانه کلاسیک این دو گزینه همیشه یکدیگر را حذف می‌کنند. در یک رایانه کوانتومی، امکان دارد که دو گزینه با یکدیگر تداخل داشته باشند تا برخی از خواص کلی تابع f را با استفاده از چیزی شبیه به گیت هادامارد برای بازترکیب گزینه‌های مختلف، مانند آنچه در الگوریتم دوچ انجام شد، به دست آورند. اساس طراحی بسیاری از الگوریتم‌های کوانتومی این است که یک انتخاب هوشمندانه از تابع و تبدیل نهایی اجازه می‌دهد تا اطلاعات جهانی مفیدی در مورد تابع تعیین شود - اطلاعاتی که نمی‌توان به سرعت در یک رایانه کلاسیک به دست آورد.

۳.۳.۳ پیاده‌سازی الگوریتم دوچ در کیس کیت

فصل ۴

شبیه‌سازی پدیده‌های کوانتومی

در این بخش قصد داریم به بررسی پروتکل‌های ابتدایی در نظریه‌ی اطلاعات کوانتومی بپردازیم. تمامی این پروتکل‌ها به تعداد کمی کیوبیت نیاز دارند؛ و در آزمایشگاه به صورت تجربی پیاده‌سازی شده‌اند.

۱.۴ حالات بل

به مدار نمایش داده شده در شکل زیر دقت کنید:

این مدار دارای یک گیت هادامارد و سپس CNOT است و چهار حالت پایه محاسباتی را مطابق جدول داده شده تبدیل می کند. به عنوان مثال: گیت هادامارد ورودی $|00\rangle$ را به حالت $\frac{(|0\rangle+|1\rangle)}{\sqrt{2}}$ انتقال می‌دهد و سپس CNOT حالت خروجی $\frac{(|00\rangle+|11\rangle)}{\sqrt{2}}$ را آماده می‌کند.

بار دیگر مراحل را مرور می‌کنیم:

ابتدا اعمال تبدیل هادامارد حالت کیوبیت بالایی را به یک برهمنهی کوانتومی منتقل می‌کند. این برهمنهی ایجاد شده، به عنوان کیوبیت کنترل به CNOT عمل می کند و حالت کیوبیت هدف تنها زمانی معکوس می شود که حالت کیوبیت کنترل ۱ باشد.

حالت خروجی را می‌توان به شکل زیر نمایش داد:

۲۶.۱ - ۲۳.۱

از حالت‌های بالا به عنوان حالات بل یا حالات EPR یادمی‌کنیم.

خصوصیات حالات $|\beta_{00}\rangle, |\beta_{01}\rangle, |\beta_{10}\rangle, |\beta_{11}\rangle,$ از طریق فرمول زیر بهتر درک خواهند شد:

۲۷.۱

۱۲.۱ fig y. of negation the is ¯y where

پیاده‌سازی حالات بل در کیس کیت

۲.۴ درهمتنیدگی

در حوزه فیزیک کوانتومی، یکی از گیج کننده ترین پدیده هایی که همچنان توجه دانشمندان و فیلسوفان را به خود جذب می کند، «درهم تنیدگی» است. این مفهوم درک متعارف ما از واقعیت را به چالش می‌کشد و باعث بحث‌ها، آزمایش‌ها و تحقیقات فلسفی بی‌شماری شده است.
درهم تنیدگی به ارتباط فوق‌العاده‌ای اطلاق می‌شود که می‌تواند بین دو یا چند ذره، بدون توجه به فاصله‌ای که آنها را از هم، وجود داشته باشد. هنگامی که ذرات در هم می‌پیچند، ویژگی‌های آن‌ها مانند اسپین، تکانه و قطبش به گونه‌ای به هم مرتبط می‌شوند که تغییر حالت یک ذره بدون توجه به فضای فیزیکی بین آنها، فوراً بر وضعیت ذره دیگر تأثیر می‌گذارد. به نظر می‌رسد این ارتباط آنی با مفاهیم کلاسیک علت و معلول مخالفت می‌کند.

یکی از مشهورترین آزمایش‌های فکری که درهم تنیدگی را نشان می‌دهد، پارادوکس انیشتین-پودولسکی-روزن (EPR) است. در این سناریو، دو ذره درهم تنیده که اغلب به آنها «آلیس» و «باب» گفته می شود، جدا شده و به مکان های مختلف فرستاده می شوند. وقتی اندازه‌گیری روی یک ذره انجام می‌شود، حالت آن فوراً مشخص می‌شود و باعث می‌شود وضعیت ذره دیگر نیز مشخص شود، این تغییر حالت از راه دور حتی اگر دو ذره‌ی درهم‌تنیده سال‌های نوری از هم فاصله داشته باشند؛ رخ خواهد داد. این نقض آشکار محدودیت سرعت نور، درک ما از نحوه انتقال اطلاعات را به چالش کشیده است.

درهم تنیدگی فقط یک مفهوم نظری نیست. به طور تجربی از طریق آزمایش های مختلف مشاهده و تأیید شده است. یکی از مهم‌ترین آزمایش‌هایی که درهم تنیدگی را به صورت تجربی نشان می‌دهد، آزمون بل است. این آزمایش نقض نابرابری‌های بل را آزمایش می‌کند. وقتی اندازه‌گیری‌های ذرات درهم تنیده این نابرابری‌ها را نقض می‌کند، نشان می‌دهد که رفتار آنها توسط فیزیک کلاسیک قابل توضیح نیست و در عوض به واقعیت درهم‌تنیدگی کوانتومی اشاره می‌کند.

پیامدهای درهم تنیدگی عمیق و پیچیده است و فراتر از محدوده آزمایشگاه های فیزیک است. محققان همواره در حال بررسی کاربردهای بالقوه درهم تنیدگی در زمینه هایی مانند محاسبات کوانتومی و رمزنگاری کوانتومی هستند. توانایی درهم تنیدگی برای فعال کردن کیوبیت‌ها (بیت‌های کوانتومی) برای وجود همزمان در چندین حالت، این پتانسیل ایجاد تحولات شگرفی در رمزنگاری کوانتومی و محاسبات کوانتومی دارد و به راه‌حل‌هایی منجر شود که قبلا غیرممکن تلقی می‌شدند.

locality Non

در نتیجه، از درهم تنیدگی به عنوان یکی از جذاب ترین و گیج کننده ترین پدیده ها در قلمرو فیزیک کوانتومی یادمی‌شود. ارتباط اسرارآمیز آن بین ذرات، شهود کلاسیک را به چالش می کشد و همچنان مرزهای درک ما از جهان را پیش می برد. همانطور که دانشمندان عمیق تر به پیچیدگی های درهم تنیدگی و کاربردهای بالقوه آن می پردازند.

۱.۲.۴ پیاده‌سازی درهمتنیدگی در کیس کیت

۳.۴ رمزگذاری متراکم کوانتومی

رمزگذاری متراکم کوانتومی[۱] یک کاربرد ساده اما شگفت‌انگیز از مفاهیم ابتدایی مکانیک کوانتومی است. این کاربرد، همه ایده‌های اساسی و ابتدایی مکانیک کوانتومی را به روشی ملموس و غیرقابل‌توضیح ترکیب می‌کند، بنابراین مثالی ایده‌آل از اهداف و وظایف پردازش اطلاعات است که می‌توان با استفاده از مکانیک کوانتومی انجام داد.

رمزگذاری متراکم شامل دو طرفین است که به طور معمول به عنوان «آلیس» و «باب» شناخته می‌شوند، که از هم فاصله زیادی دارند. هدف آنها انتقال برخی اطلاعات کلاسیک از آلیس به باب است. فرض کنید آلیس قصد دارد دوبیت داده‌ی کلاسیک را برای باب ارسال کند، اما فقط مجاز است یک کیوبیت به باب ارسال کند. آیا می‌تواند به هدف خود برسد؟

رمزگذاری متراکم به ما می‌گوید که پاسخ این سؤال بله است. فرض کنید آلیس و باب در ابتدا یک جفت کیوبیت در حالت درهم‌تنیده زیر به اشتراک می‌گذارند:

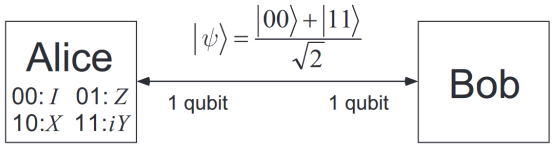
$$|\Psi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$$

آلیس می‌تواند با استفاده از دو کیوبیت درهم‌تنیده، دو بیت کلاسیک را به باب منتقل کند. او این کار را با اعمال یک سری از تبدیلات به کیوبیت خود انجام می‌دهد؛ انتخاب این تبدیلات باتوجه به بیت‌هایی که قصد ارسالشان را دارد؛ تعیین می‌شود. به عنوان مثال، اگر آلیس می‌خواهد بیت‌های ۰۰ را به باب ارسال کند، او تبدیل یکه را به کیوبیت خود اعمال می‌کند.

این تبدیل واحد باعث می‌شود که کیوبیت آلیس و کیوبیت باب در یکی از چهار حالت متعامد بل قرار گیرند. اگر آلیس کیوبیت خود را در حالت $|00\rangle$ قرار دهد، کیوبیت باب به طور خودکار به حالت $|00\rangle$ تبدیل می‌شود. این بدان معناست که آلیس دو بیت اطلاعات $(0,0)$ را به باب منتقل کرده است.

باب سپس کیوبیت خود را اندازه‌گیری می‌کند و یکی از مقادیر ۰ یا ۱ را به دست می‌آورد. بسته به مقداری که باب اندازه‌گیری می‌کند، او می‌تواند دو بیت کلاسیک که آلیس به او ارسال کرده است را بازیابی کند.

[۱] Quantum super dense coding



شکل ۱.۴: تنظیمات اولیه برای کدگذاری فوق متراکم، آلیس و باب که هر کدام یک کیوبیت، از جفت کیوبیت درهمتنیده را در اختیار دارند.

همانطور که در شکل بالا قابل ملاحظه است؛ آلیس و باب، هرکدام یک کیوبیت در اختیار دارند. توجه داشته باشید که Ψ یک حالت ثابت است؛ نیازی نیست که آلیس برای آماده‌سازی این حالت، کیوبیتی را به باب ارسال کند. در عوض، ممکن است یک طرف ثالث قبلاً حالت درهم‌تنیده را آماده کند، یکی از کیوبیت‌ها را به آلیس و دیگری را به باب ارسال کند.

با ارسال تک کیوبیت آلیس به باب، معلوم می‌شود که آلیس می‌تواند دو بیت اطلاعات کلاسیک را به باب منتقل کند. در اینجا روشی که او استفاده می‌کند؛ آورده شده است. اگر او بخواهد رشته‌بیت :

- "00" را ارسال کند $\Longleftarrow$ هیچ کاری روی کیوبیت خود انجام ندهد.
- "01" را ارسال کند $\Longleftarrow$ تبدیل دگرگونی فاز[۲] را روی کیوبیت خود اثر می‌دهد.
- "10" را ارسال کند $\Longleftarrow$ گیت کوانتومی NOT، X را به کیوبیت خود اعمال می‌کند.
- "11" را ارسال کند $\Longleftarrow$ تبدیل iY را به کیوبیت خود اعمال می‌کند.

چهار حالت حاصل به راحتی قابل مشاهده هستند:

$$
\begin{aligned}
00 : |\psi\rangle &\rightarrow \frac{|00\rangle + |11\rangle}{\sqrt{2}} \\
01 : |\psi\rangle &\rightarrow \frac{|00\rangle - |11\rangle}{\sqrt{2}} \\
10 : |\psi\rangle &\rightarrow \frac{|10\rangle + |01\rangle}{\sqrt{2}} \\
11 : |\psi\rangle &\rightarrow \frac{|01\rangle - |10\rangle}{\sqrt{2}}.
\end{aligned}
$$

[۲] flip phase

همانطور که پیش‌از این اشاره شد؛این چهار حالت به عنوان پایه بل، حالت‌های بل، یا جفت‌های EPR شناخته می‌شوند. توجه داشته باشید که حالت‌های بل؛ پایه‌های متعامد هستند؛ و بنابراین می‌توانند با اندازه‌گیری کوانتومی مناسب از یکدیگر متمایز شوند. اگر آلیس کیوبیت خود را به باب بفرستد، و باب هر دو کیوبیت را در اختیار داشته باشد، سپس با انجام اندازه‌گیری در پایه بل، باب می‌تواند تعیین کند که کدام یک از چهار رشته بیت ممکن را آلیس ارسال کرده است.

به طور خلاصه می‌توان گفت: آلیس، با تعامل و اثرگذاری تنها روی یک کیوبیت، قادر به انتقال دو بیت اطلاعات به باب است. البته دو کیوبیت در پروتکل دخیل هستند، اما آلیس هرگز نیازی به تعامل با کیوبیت دوم ندارد. از نظر کلاسیک، وظیفه‌ای که آلیس انجام می‌دهد، اگر فقط یک بیت کلاسیک ارسال می‌کرد، غیرممکن بود.

علاوه بر این، پروتکل رمزگذاری متراکم، تا حدی در آزمایشگاه تأیید شده است. یک نکته کلیدی را می‌توان در این مثال زیبا مشاهده کرد: اطلاعات فیزیکی است، و نظریه‌های فیزیکی شگفت‌انگیز مانند مکانیک کوانتوم ممکن است توانایی‌های پردازش اطلاعات شگفت‌انگیزی را پیش‌بینی کنند.

مراحل این پروتکل به اختصار به شرح زیر است:

- آلیس و باب یک جفت کیوبیت درهم‌تنیده را با هم به اشتراک می‌گذارند.
- آلیس می‌خواهد دو بیت کلاسیک، ۰۰ یا ۰۱ را به باب ارسال کند.
- آلیس یک عمل واحد بر روی کیوبیت خود اعمال می‌کند که بسته به بیت‌هایی که می‌خواهد به باب ارسال کند متفاوت است.
- آلیس کیوبیت خود را به باب می‌فرستد.
- باب کیوبیت را اندازه‌گیری می‌کند و دو بیت کلاسیکی که آلیس به او ارسال کرده است را دریافت می‌کند.
- اگر آلیس یک عمل یکه بر روی کیوبیت خود اعمال نکند، باب فقط می‌تواند یک بیت کلاسیک را دریافت کند. با این حال، اگر آلیس عمل یکه مناسب را اعمال کند، می‌تواند دو بیت کلاسیک را با ارسال یک کیوبیت انتقال دهد.

پروتکل رمزگذاری متراکم؛ یک مثال عالی از قدرت مکانیک کوانتوم در انتقال اطلاعات است. این پروتکل نشان می‌دهد که می‌توان با استفاده از قوانین مکانیک کوانتوم، اطلاعات را به روش‌های غیرممکن در فیزیک کلاسیک انتقال داد.

۱.۳.۴ پیاده سازی رمزگذاری متراکم در کیس کیت

۴.۴ دوربری

دوربری کوانتومی تکنیکی برای جابجایی حالات کوانتومی به نقاط دیگر است. در اینجا نحوه عملکرد دوربری کوانتومی آمده است:

آلیس و باب مدت ها پیش با هم آشنا شدند اما اکنون دور از هم زندگی می کنند. در حالی که آنها با هم یک جفت EPR تولید کردند، هر کدام یک کیوبیت از جفت EPR را در هنگام جدا شدن می‌گرفتند. سال‌ها بعد، باب مخفی است، و ماموریت آلیس، در صورتی که آن را بپذیرد، تحویل یک کیوبیت $|\Psi\rangle$ به باب است. او وضعیت و خصوصیات کیوبیت را نمی داند و علاوه بر این فقط می تواند اطلاعات کلاسیک را برای باب ارسال کند. آیا آلیس باید این مأموریت را بپذیرد؟

درظاهر، تمام شرایط علیه آلیس است. او وضعیت $|\Psi\rangle$ کیوبیتی را که باید برای باب بفرستد نمی داند، و طبق قوانین مکانیک کوانتومی، او حق تعیین وضعیت $|\Psi\rangle$ را ندارد؛زیرا فقط یک نسخه از جفت کیوبیت را در اختیار دارد. به علاوه، حتی اگر او حالت $|\Psi\rangle$ را می دانست، توصیف دقیق آن به مقدار نامحدودی از اطلاعات کلاسیک نیاز دارد، زیرا $|\Psi\rangle$ مقادیری را در یک فضای پیوسته می گیرد.

بنابراین حتی اگر او $|\Psi\rangle$ را می دانست، برای آلیس تا ابد طول می کشید تا وضعیت را برای باب توصیف کند. دوربری کوانتومی راهی برای استفاده از جفت EPR درهم تنیده به منظور ارسال $|\Psi\rangle$ به باب، تنها با سربار کوچکی از ارتباطات کلاسیک است. این مسأله وضعیت را برای آلیس تغییر می‌دهد.

به طور کلی، مراحل حل به شرح زیر است: آلیس با کیوبیت $|\Psi\rangle$ با یک کیوبیت خود از جفت EPR، و سپس دو کیوبیت در اختیارش را اندازه گیری می کند و یکی از چهار نتیجه کلاسیک ممکن ، ۰۰، ۰۱، ۱۰، ۱۱ را بدست می‌آورد. درنهایت او این اطلاعات را به باب ارسال می‌کند.

بسته به پیام کلاسیک آلیس، باب یکی از چهار عملگر جدول زیر را روی کیوبیت EPR خود اعمال می‌کند. به طرز شگفت انگیزی، با انجام این کار او می تواند حالت اولیه را بازیابی کند $|\Psi\rangle$! مدار کوانتومی نشان داده شده در شکل زیر توصیف دقیق تری از دوربری کوانتومی ارائه می دهد. دوربری حالتی که باید از راه دور منتقل شود عبارت است از $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ که α و β ناشناخته هستند.

$$|\psi_0\rangle = |\psi\rangle\rangle\,|\beta_{00}\rangle$$

۱۳.۱ fig

$$= \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)]$$

جایی که ما از این قاعده استفاده می کنیم که دو کوبیت اول (در سمت چپ) متعلق به آلیس هستند و کوبیت سوم متعلق به باب است. همانطور که قبلا توضیح دادیم ، کوبیت دوم آلیس و کوبیت باب در یک حالت EPR شروع می شوند. آلیس یک گیت $CNOT$ را روی کیوبیت‌های خود اثر می‌دهد. از این رو:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)]$$

سپس گیت هادامارد را روی اولین کیوبیت اثر می‌دهد و به دست می آورد:

$$|\psi_2\rangle = \frac{1}{2}[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)]$$

این حالت را می توان به روش زیر بازنویسی کرد، به سادگی با گروه بندی مجدد عبارات:

$$\begin{aligned}|\psi_2\rangle =& \frac{1}{2}[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) \\ &+ |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)]\end{aligned}$$

این عبارت به طور طبیعی به چهار اصطلاح تقسیم می شود. عبارت اول دارای کیوبیت های آلیس است در حالت $|00\rangle$ و کیوبیت باب، که بیانگر حالت اصلی $|\Psi\rangle$ است؛ در حالت $\alpha|0\rangle + \beta\ vert1\rangle$ قرار دارد.

. اگر آلیس یک اندازه گیری را انجام دهد و نتیجه ۰۰ را به دست آورد، آنگاه کیوبیت باب دقیقا همان $|\Psi\rangle$ می‌باشد.

به طور مشابه:

$$00 \longmapsto |\psi_3(00)\rangle \equiv [\alpha|0\rangle + \beta|1\rangle]$$
$$01 \longmapsto |\psi_3(01)\rangle \equiv [\alpha|1\rangle + \beta|0\rangle]$$
$$10 \longmapsto |\psi_3(10)\rangle \equiv [\alpha|0\rangle - \beta|1\rangle]$$
$$11 \longmapsto |\psi_3(11)\rangle \equiv [\alpha|1\rangle - \beta|0\rangle]$$

بسته به نتیجه اندازه گیری آلیس، کیوبیت باب به یکی از این چهار حالت ممکن قرار خواهد گرفت. البته، برای پیدا کردن حالت کیوبیت، باید نتیجه اندازه‌گیری آلیس را به باب اعلام کرد. کمی پیش‌تر نشان خواهیم داد که همین وضعیت مانع از استفاده از دوربری برای انتقال اطلاعات با سرعتی، سریع‌تر ازسرعت نور می‌شود.

هنگامی که باب نتیجه اندازه گیری را فهمید، باب می تواند حالت کیوبیت خود را «تثبیت» کند و با استفاده از گیت کوانتومی مناسب، $|\Psi\rangle$ را بازیابی کند. به عنوان مثال، در موردی که اندازه گیری نتیجه‌ی ۰۰ را نشان می دهد، باب نیازی به انجام کاری ندارد. اگر نتیجه‌ی اندازه گیری ۰۱ باشد، باب می تواند حالت کیوبیت خود را با اعمال دروازه X اصلاح کند.

اگر نتیجه‌ی اندازه گیری ۱۰ باشد، باب می تواند حالت کیوبیت خود را با استفاده از گیت Z ثابت کند. اگر اندازه‌گیری ۱۱ باشد، باب می‌تواند با اعمال ابتدا یک X و سپس یک گیت Z حالت کیوبیت خود را اصلاح کند. به طور خلاصه، باب باید تبدیل $ZM1XM2$ را در کیوبیت خوداعمال کند [۳]؛ و بدین طریق او می‌تواند حالت $|\Psi\rangle$ را بازیابی می‌کند.

با مطرح کردن مفهوم تلپورت کوانتومی، سوالات زیادی مطرح می‌شود. در اینجا به تعدادی از متداول ترین سوالات مطرح کرده و پاسخ می‌دهیم:

سوال اول

آیا دوربری به فرد اجازه نمی‌دهد حالت‌های کوانتومی را سریع‌تر از نور منتقل کند؟ این امر بسیار جذاب و شگرف است؛ زیرا تئوری نسبیت نشان می دهد که انتقال اطلاعات سریعتر از نور می تواند برای ارسال اطلاعات به عقب در زمان استفاده شود. دوربری کوانتومی ارتباط سریع‌تر از سرعت نور را امکان‌پذیر نمی‌کند، زیرا برای تکمیل دوربری، آلیس باید نتیجه اندازه‌گیری خود را از طریق یک کانال ارتباطی کلاسیک به باب منتقل کند.

می‌توان نشان داد؛ که بدون این کانال ارتباطی کلاسیک، دوربری توان انتقال هیچ اطلاعاتی را ندارد. کانال ارتباط کلاسیک با سرعت نور محدود می شود، بنابراین می‌توان نتیجه گرفت که تله پورت

[۳] توجه داشته باشید که چگونه زمان در نمودارهای مدار از چپ به راست می‌گذرد، اما در عملیات‌های ماتریسی سمت راست اول اتفاق می‌افتد

کوانتومی نمی تواند سریعتر از سرعت نور انجام شود و این تناقض ظاهری را حل می‌شود.

سوال دوم

در فرآیند دوربری به نظر می رسد یک کپی از حالت کوانتومی در حال انتقال از راه دور ایجاد می‌شود؛ در حالی که آشکارا قضیه عدم شبیه سازی[۴] مورد بحث نقض می کند.

این نقض ناشی از دقت کم و یا توهم است؛ زیرا پس از فرآیند دوربری فقط کیوبیت هدف در حالت $|\Psi\rangle$ باقی می ماند و کیوبیت اصلی که حامل داده است؛ با توجه به فرآیند اندازه گیری حالت اصلی به یکی از حالت های پایه محاسباتی $|0\rangle$ یا $|1\rangle$ رمبش می‌کند.

۱.۴.۴ پیاده‌سازی دوربری در کیس کیت

[۴] theorem cloning No