فهرست مطالب

۱.۰ مقدمه

در عصر حاضر بواسطه‌ی 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، بهره‌می‌بریم. 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

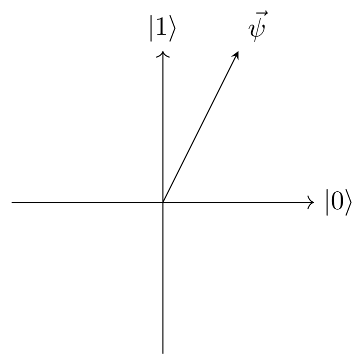
برخلاف بیت ها که مقادیر ثابت ۰ یا ۱ را به خود می‌گیرند؛ یک کیوبیت می‌تواند در یک حالت «برهمنهی کوانتومی» باشد؛ این بدان معناست که یک کیوبیت بواسطه‌ی مشاهده ناظر به یکی از حالات ۰ یا یک تبدیل شود. این مهم‌ترین مزیت استفاده از کیوبیت‌هاست. بیان ریاضی یک کیوبیت ،در حالت برهمنهی، به شرح زیر است:

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

[۱] Qubit

[۲] Binary Bit

کت‌های $|0\rangle$ و $|1\rangle$ بیانگر پایه‌های فضای محاسباتی[۳] هستند؛ و مقادیر α^2 و β^2 بیانگر احتمال وقوع هر یک از این حالات، در صورت مشاهده، می‌باشند. نمایش بردار ψ به شرح 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:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{۱.۱}$$

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 کوبیت یک بردار واحد در فضای برداری دو بعدی پیچیده است. 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 رفتار سیستم های کوانتومی دشوار باشد؛ با این حال، یک ارتباط غیرمستقیم وجود دارد، زیرا می توان حالت های کوبیت را دستکاری و تبدیل کرد به روش هایی که منجر به نتایج اندازه گیری می شود که به طور متمایز 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 کوبیت می تواند در یک طیف پیوسته از حالت ها بین $|0\rangle$ و $|1\rangle$ وجود داشته باشد

[۳] Computational Basis Vectors

- تا زمانی که مشاهده شود. بار دیگر تاکید می کنیم که وقتی یک کوبیت اندازه گیری می شود، فقط «۰» یا «۱» را به عنوان نتیجه اندازه گیری می دهد - به صورت تصادفی. به عنوان مثال، یک کوبیت می تواند در حالت |۰⟩ + |۱⟩ باشد، که به این معنی است که با احتمال ۵۰/۵۰ می تواند به عنوان ۰ یا ۱ اندازه گیری شود.

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

حالت $\langle +|$ حالتی از کوبیت 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 $\langle 0|$ و $\langle 1\langle$ در نظر گرفت.

این حالت به دلیل عجیب بودنش جالب است. حالت های پایه $\langle 0\langle$ و $\langle 1\langle$ تنها حالاتی هستند که می توانند به طور مستقیم مشاهده شوند. حالت $\langle +\langle$ ، 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 $\langle +\langle$ 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 $\langle +\langle$ 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 کوبیت داریم. اگر این دو بیت کلاسیک بودند، چهار حالت ممکن وجود داشت: ۰۰، ۰۱، ۱۰ و ۱۱. به همین ترتیب، یک سیستم دو کوبیتی دارای چهار حالت محاسباتی است که با $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ نشان داده می شود. یک جفت کوبیت همچنین می تواند در برهمنهی این چهار حالت وجود داشته باشد. بنابراین حالت کوانتومی دو کوبیت 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 کوبیت به شکل زیر است:

$$|\Psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$

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

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

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

احتمال اندازه گیری کوبیت 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 کوبیت ها پس از اندازه گیری$\langle x|$. این بدان معناست که اگر ما یک سیستم دو کوبیتی را در حالت $|\Psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ داشته باشیم، و اگر ما اولین کوبیت را اندازه گیری کنیم، احتمال اینکه ۰ را اندازه گیری کنیم برابر $|a\rangle^2 + |b\rangle^2$ خواهد بود. در این حالت، حالت کوبیت ها پس از اندازه گیری $|0\rangle$ خواهد بود.

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

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

۱.۲.۱ vector bloch

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:

$$|-\rangle \equiv (|0\rangle - |1\rangle)\sqrt{2} \; |+\rangle \equiv (|0\rangle + |1\rangle)\sqrt{2}$$

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

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

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 پایگاه 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، با حالت های پس از اندازه گیری $|+\rangle$ و $|-\rangle$ به ترتیب.

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 $|\beta|^2$ می دهد.

محدودیت متعامد 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.

با این حال، فقط به این دلیل که در اصل امکان پذیر است، به این معنی نیست که چنین اندازه گیری به راحتی انجام می شود، و ما بعداً به این سوال که چگونه می توان اندازه گیری در یک پایه دلخواه را

به طور کارآمد انجام داد، باز می گردیم. در این پاراگراف، نویسنده در مورد اندازه گیری در پایه های دیگر به غیر از پایه محاسباتی بحث می کند. آنها نشان می دهند که می توان هر حالت کوانتومی را به عنوان یک ترکیب خطی از دو پایه دلخواه بیان کرد و سپس با توجه به آن پایه ها اندازه گیری کرد. آنها همچنین اشاره می کنند که این اندازه گیری ها در اصل امکان پذیر است، اما لزوماً کارآمد نیستند.

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 گسترش یافته برای اندازه گیری های کوانتومی وجود دارد، اما در نهایت بهترین دلیل این است: این مدل به ما امکان توصیف نتایج تجربی مشاهده شده را می دهد، همانطور که در بحث ما در مورد آزمایش Stern–Gerlach در بخش ۱.۵.۱ خواهیم دید. یک مدل حتی پیچیده تر و راحت تر (اما اساساً معادل) برای توصیف اندازه گیری های کوانتومی در فصل بعدی، در بخش ۳.۲.۲ توصیف شده است.

در این پاراگراف، نویسنده در مورد مدل گسترش یافته برای اندازه گیری های کوانتومی بحث می کند. آنها استدلال می کنند که این مدل بهترین روش برای توصیف نتایج تجربی مشاهده شده است. آنها همچنین اشاره می کنند که یک مدل حتی پیچیده تر و راحت تر برای توصیف اندازه گیری های کوانتومی وجود دارد، اما این مدل اساساً معادل است.

اندازه گیری های کوانتومی یکی از مهمترین مفاهیم در مکانیک کوانتوم است. آنها به ما امکان می دهند تا اطلاعات را در مورد سیستم های کوانتومی استخراج کنیم. مدل گسترش یافته برای اندازه گیری های کوانتومی یک ابزار قدرتمند برای توصیف اندازه گیری های کوانتومی است. این امکان را می دهد تا ما نتایج تجربی مشاهده شده را توصیف کنیم و همچنین به ما امکان می دهد تا اندازه گیری های کوانتومی را در سیستم های پیچیده تر انجام دهیم.

۳.۱ گیت‌های کوانتومی

گیت‌های کوانتومی[۴] 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[۵] 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.

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

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

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

[۴] Quantum Gates

[۵] Hadamard gate

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

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

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 Single-Qubit Quantum gate می‌باشد.

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

گیت NOT

به دلیلی به آن gate X می گویند تا به زودی روشن شود باز هم، از آنجایی که هر دروازه کوانتومی یک دروازه واحد است، من آن را برچسب گذاری می کنم ماتریس به عنوان NOT U . به آن دروازه NOT می گویند زیرا به این صورت تعریف شده است:

$$U_{NOT}|0\rangle = |1\rangle$$
$$U_{NOT}|1\rangle = |0\rangle$$

نمایش ماتریسی گیت CNOT

می بینید که اگر فقط پایه را در نظر بگیریم، دقیقاً مانند دروازه کلاسیک NOT است به عنوان ارزش های کلاسیک بیان می کند. این با آنچه در فصل بحث کردیم مطابقت دارد. ۱۳ که یک ثبات کوانتومی دقیقاً مشابه یک ثبات کلاسیک است اگر فقط مجاز باشد برای ذخیره حالت های پایه برای دستیابی به تابع در معادله (۵.۱۵)، ما متوجه شدیم که

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

شما ممکن است با آن به عنوان داده شده رفتار کنید. یا از آنجایی که یک حالت کیوبیت در C۲ دو بعدی است فاصله، ماتریس (اپراتور) باید ۲ × ۲ باشد و اگر تمام موارد ممکن را طی کنید ترکیبات، متوجه می شوید که این تنها ماتریسی است که معادله را برآورده می کند. (۵.۱۵). به ما اجازه دهید بررسی کنید که آیا این مورد است. چگونه |۰⟩ را در شکل ستونی نشان می دهیم؟ این است (۱ ۰) . و بگذارید یادآوری کنم که این منطقی است زیرا |۰⟩ اولین حالت پایه و عناصر ستون است. به ما بگویید که دارای یک جزء از حالت پایه اول و جزء صفر است حالت پایه دوم به طور مشابه، ما |۱⟩ = را نشان می دهیم (۰ ۱) . از این رو

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

مدار NOT و خصوصیات آن

درست مانند قدرت یک ثبات کوانتومی این است که می تواند برهم نهان ها را ذخیره کند از حالت های پایه، قدرت دروازه های کوانتومی این است که می توانند آن ها را پردازش کنند برهم نهی های حالت های پایه حالا بیایید ببینیم اگر NOT U اعمال شود چه اتفاقی می افتد به حالت کلی ?| ? = α |۰⟩ + ? |۱⟩

۹.۱۵

بنابراین، ما همچنین می توانیم UNOT را به عنوان دروازه ای که ضرایب را مبادله می کند درک کنیم از حالت های پایه (یعنی α تبدیل به ? می شود و بالعکس). اکنون، احتمالاً قبلاً متوجه شده اید که چرا دروازه NOT نیز نامیده می شود دروازه ایکس؟ این به این دلیل است که ماتریس در معادله (۶.۱۵) فقط x? است. شکل ۲.۱۵ نشان می دهد NOT عملیات و مدارهای آن. علاوه بر دروازه NOT یک کیوبیتی، می‌توانیم یک کیوبیتی یا دو کیوبیتی نیز بسازیم. دروازه نیست. ما فقط باید یک حاصل ضرب تانسور دو دروازه NOT یک کیوبیتی را انجام دهیم تا یک دروازه NOT دو کیوبیتی بدست آوریم زیرا

یک بردار دو کیوبیتی در فضای C۴ قرار دارد. که حاصل ضرب تانسور دو فضای C۲ است. از این رو،
۱۰.۱۵
fig ۲.۱۵
حال اجازه دهید دروازه NOT ۲ کی روش را به بردار کلی اعمال کنیم ⍰| ⍰ = α |۰۰⍰ + ⍰ |⍰ ۰۱⍰
+ ⍰ |۱۰⍰ + ⍰ |۱۱⍰
۱۱.۱۵

گیت CNOT

گیت کوانتومی CNOT[۶]، 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[۷]» دارای مقدار $\langle 1|$ باشد، باعث تغییر وضعیت «کیوبیت هدف[۸]» می‌شود.

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 |۰⍰ باشد، کیوبیت هدف بدون تغییر باقی می‌ماند. اگر کیوبیت کنترل در حالت |۱⍰ 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.

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

من عمداً آن را با نمادی بسیار گیج کننده نوشتم که از شما انتظار دارم در نهایت بسیار آشنا باشید |ab⍰ چیست؟ این یک بردار در فضای C۴ و یک و b یا ۰ یا ۱ هستند. |ab⍰ می تواند هر یک از حالت های پایه باشد، یعنی |۰۰⍰، |۰۱⍰، |۱۰⍰، و |۱۱. این معادله به ما می گوید که پس از اعمال گیت XOR به یکی از پایه ها حالت، به حالت پایه دیگری تبدیل خواهد شد |aa ⍰ b⍰. |aa b⍰ ⍰ فقط ،|a a ⍰ b⍰ ⍰ یا است |a⍰ ⍰ |a ⍰ .b⍰ بعد از عمل، عدد اول همچنان a است، اما عدد دوم به

gate controlled-X or gate controlled-NOT[۶]
Qubit Controled[۷]
Qubit Target[۸]

a ⍰ b تبدیل می شود، جایی که ⍰ عملیات منطقی کلاسیک انحصاری یا (XOR) است. مانند یک یادآوری، ۰ ⍰ ۰ = ۰، ۰ ⍰ ۱ = ۱، ۱ ⍰ ۰ = ۱، و ۱ ⍰ ۱ = ۰. اجازه دهید ببینیم چگونه وضعیت پایه فردی را تغییر می دهد.

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

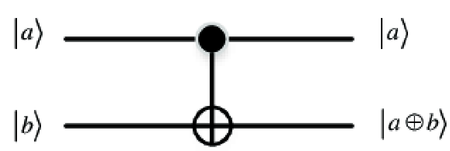
خلاصه‌ای از عملکرد این عملگر به شرح زیر است:

ببین چرا از این نماد به جای تنسور پراداکت استفاده شده

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

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:

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

این فرآیند به صورت معکوس نیز قابل رخ دادن است:

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

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: ۶.۱۶

که در آن ⍰ فاز و e ⍰i فاکتور فاز است. زمانی که گیت شیفت فاز باشد اعمال بر بردار پایه |۰⍰، هیچ کاری انجام نمی دهد. اما زمانی که آن را به بردار پایه |۱⍰، یک فاز اضافی به آن اضافه می کند. اضافه کردن یک فاز اضافی به معنای که بردار در e ⍰i ضرب شود. چرا ما فقط فاز اضافی را اعمال می کنیم به پایه دوم؟ منظور از جابجایی فاز نسبی بین چیست؟ دو بردار پایه؟ اگر به شکل ماتریس آن نگاه کنیم و مشاهده کنیم، درک آن آسانتر است چگونه یک بردار کلی را ایجاد می کند

نمایش ماتریسی گیت تغییر فاز

۷.۱۶ شما می توانید آن را به راحتی بررسی کنید که معادله. (۷.۱۶) معادله را برآورده می کند. (۶.۱۶).
مثلا ۸.۱۶

گیت تغییر فاز در مدار و خصوصیات آن

۹.۱۶ در بردار اصلی، α و ? که به طور کلی اعداد مختلط هستند، می توانند باشند به عنوان حاصل ضرب ضریب فاز و بزرگی آنها نشان داده می شود. به عنوان مثال α = e ۱?i |α| و ? = e ۲?i ،|?| که در آن ۱? و ۲? به ترتیب فازهای α و ? هستند. بنابراین، اختلاف فاز آنها ۱? - ۲? است. با توجه به گیت شیفت فاز، فاز از α بدون تغییر است اما فاز ? به ? + ۲? تغییر می کند. بنابراین، خویشاوندان آنها فاز با ? تغییر می کند. این همچنین توضیح می دهد که چرا تغییر فاز فقط در مورد اعمال می شود حالت پایه دوم معنادار باشد. اگر برای هر دو اعمال شود، تغییری ایجاد نمی شود در اختلاف فاز ? پارامتری از گیت تغییر فاز است. هنگامی که ? = ،π دروازه تبدیل می شود (۱ ۰ ۰ e iπ) = (۱ ۰ ۰ -۱) زیرا e iπ = cos π + i sin π = -۱. و این فقط ماتریس ،z? یکی از ماتریس های مهم پائولی. و به آن Z-gate نیز می گویند. گیت تغییر فاز فاز نسبی |۰?و |۱? را با ? تغییر می دهد. و به این ترتیب گیت Z فاز نسبی را با π تغییر می دهد. این باعث می شود Z-gate بسیار خاص باشد و بچرخد در مبنای |+? / |–?، دروازه Z به عنوان یک دروازه NOT (دروازه (X عمل می کند. این ممکن است صدای گیج کننده بیایید به یاد بیاوریم که معنای دروازه NOT چیست. وقتی NOT گیت به حالت پایه اعمال می شود، حالت پایه به حالت پایه دیگر تبدیل می شود. از آنجایی که یک گیت ۱ کیوبیتی است، تنها ۲ بردار پایه وجود دارد. این به این معنی است که NOT گیت حالت پایه را به یکدیگر تبدیل می کند. به عنوان مثال، در فضای تشکیل شده توسط بردارهای پایه |۰?و |۱?، دروازه NOT |۰? به |۱? و بالعکس تبدیل می کند. از این رو، انتظار می رود یک دروازه NOT در فضای |+? / |–? |+? به |–? و بالعکس تبدیل شود. اجازه دهید بررسی کنیم که آیا دروازه Z در مبنای |+? / |–? به عنوان یک گیت NOT رفتار می کند. ۱۰.۱۶ fig ۲.۱۶

می بینیم که گیت Z |+? را به |–? تبدیل می کند. در اینجا من از ماتریس استفاده نمی کنم نمایندگی. من از درک خود از Z-gate استفاده می کنم که تغییر فاز را اضافه می کند از π به ضریب حالت پایه دوم (یعنی |۱?). بنابراین، من فقط ضرب می کنم -۱ تا |۱?. امیدوارم بتوانید آموزش خود را در مورد این مهارت شروع کنید زیرا چنین است درک و بینش برای شما مهم است که بتوانید کوانتومی جدید طراحی کنید الگوریتم ها ضرب ماتریس درست مانند شبیه سازی مدار است که باید اجازه دهید کامپیوتر این کار را انجام دهد. درک ماهیت دروازه درست مانند آنچه ما هستیم درک مدار آنالوگ از طریق بازرسی شکل ۲.۱۶ مدار یک گیت شیفت فاز و گیت Z را نشان می دهد

۲.۳.۱ gate Swap

یک گیت SWAP، همانطور که از نامش پیداست، اعداد را در حالت های پایه یک ۲ کیوبیتی مبادله می کند. ثبت نام. اگر فقط حالت های پایه را در نظر بگیریم، معادل مبادله حالات است از دو الکترون تعریف این است ۱.۱۶

که در آن a و b فقط اعداد کیوبیت اول و دوم در پایه هستند ایالت ها به ترتیب. آنها می توانند ۰ یا ۱ باشند. ساده ترین راه برای به دست آوردن عمق بیشتر درک فقط برای وصل کردن همه حالت های پایه است و ما دریافت می کنیم ۲.۱۶

بنابراین، تنها |۰۱⟩ و |۱۰⟩ تحت SWAP (به یکدیگر) تغییر می کنند. عمل. برای |۰۰⟩ و |۱۱⟩، آنها بدون تغییر هستند زیرا "۰" و "۰" تعویض می شوند. یا "۱" و "۱" معادل انجام هیچ کاری است.

نمایش ماتریسی گیت swap

۳.۱۶

از این طریق می توانیم آن را درک کنیم. از آنجایی که این یک گیت ۲ کیوبیتی برای عملیات است یک بردار در فضای چهار بعدی، C۴، ماتریس (اپراتور) باید ۴ × ۴ باشد. علاوه بر این، فقط حالت پایه دوم و سوم را مبادله می کند. بنابراین، تنها ردیف دوم و سوم با ماتریس هویت متفاوت هستند. بیایید امتحان کنیم مثال عددی ۴.۱۶ این رابطه بصورت معکوس نیز برقرارست.

گیت swap در مدار و خصوصیات آن

به طور کلی، برای یک بردار ۲ کیوبیتی، |⟩ = α |۰۰⟩ + |۰۱⟩ + |۱۰⟩ + |۱۱⟩ داریم

fig۱۶.۱ ۵.۱۶

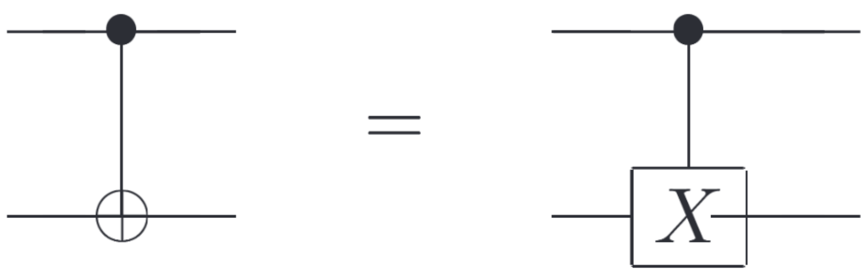
همانطور که انتظار می رود، ضرایب حالت های پایه دوم و سوم با هم مبادله می شوند. شکل ۱.۱۶ مدار یک عملیات SWAP را نشان می دهد. توجه داشته باشید که دوباره کیوبیت پایین MSB است. همانطور که تاکید کردیم، یک مدار کوانتومی یک جریان را نشان می دهد زمان نه یک جریان سیگنال بنابراین، بر خلاف عملیات مبادله کلاسیک، اجرای یک گیت SWAP پیچیده است و به این سادگی نیست مدار را نشان می دهد برای انجام یک عملیات SWAP، باید مقداری خارجی صحیح اعمال کنیم پالس می کند تا حالت های دو اسپین الکترون مبادله شود.

۴.۱ مدارهای کوانتومی

مدارهای کوانتومی[۹]، 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 ۲.۱: نمایش‌های مختلف گیت CNOT در مدار کوانتومی

converts operation this described، previously As .۱۰.۱ Figure in shown as (dis- M bit classical probabilistic a into ?|۱? + α|۰? = |?? state qubit single a with ۰ is which wire)، double-line a as it drawing by qubit a from tinguished . |?|۲ probability with ۱ or ، |α|۲ probability

book chuang L fig۱.۱۰

processes، quantum all of models as useful circuits quantum find shall We quantum even and communication، computation، to limited not but including below. this illustrate examples simple Several noise.

[۹] circuit quantum

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 کوبیت 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: This is a table with ۳ rows and ۳ columns.

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.

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

دروازه دروازه ها عملیاتی هستند که روی کوبیت ها اعمال می شوند. آنها می توانند برای ایجاد superpositions ، انجام چرخش ها و درهم تنیدگی کوبیت ها استفاده شوند. انواع مختلفی از دروازه ها وجود دارد ، اما برخی از رایج ترین آنها شامل دروازه Hadamard ، دروازه CNOT و دروازه Toffoli است.

عملیات عملیات اقداماتی هستند که روی کوبیت ها انجام می شوند. آنها می توانند اندازه گیری ها ، راه اندازی ها یا سایر اقدامات باشند. اندازه گیری ها برای فروپاشی حالت کوانتومی یک کوبیت به یک مقدار قطعی ، ۰ یا ۱ استفاده می شود. راه اندازی ها برای تنظیم حالت یک کوبیت به یک مقدار خاص ، ۰ یا ۱ استفاده می شوند.

اجزای اساسی یک مدار کوانتومی کوبیت 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 کوبیت ها را نشان می دهد. دروازه ها توسط جعبه ها نشان داده می شوند و خطوط بین جعبه ها نشان دهنده ارتباطات بین کوبیت ها است.

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 Cirq Qiskit، 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 تفاوت کامپیوتر کلاسیک و کوانتومی

کامپیوترهای کوانتومی در مقابل کامپیوترهای کلاسیک

کامپیوترهای کوانتومی و کامپیوترهای کلاسیک دو نوع بسیار متفاوت از رایانه هستند. کامپیوترهای کوانتومی از بیت‌های کوانتومی (کوبیت‌ها) برای ذخیره اطلاعات استفاده می‌کنند، در حالی که کامپیوترهای کلاسیک از بیت‌ها استفاده می‌کنند. کوبیت‌ها 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. * 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 simulation vs comp

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 کوانتمی 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. ? : درکودانس در محاسبات کوانتومی مهم است زیرا اصلی ترین منبع خطا در این سیستم ها است. کوبیت ها، واحد های اصلی اطلاعات در محاسبات کوانتومی، بسیار حساس به محیط خود هستند و می توانند به راحتی توسط interactions با فوتون ها، الکترون ها و سایر ذرات دکور شوند. این می تواند باعث شود که کوبیت ها خواص کوانتومی خود را مانند superposition و entanglement که برای انجام محاسبات کوانتومی ضروری هستند، از دست بدهند.

Decoherence می تواند توسط عوامل مختلفی ایجاد شود، از جمله:

* **دما:** کوبیت ها در دماهای بالاتر مستعد دکوراسیون هستند. این به این دلیل است که هرچه دما بالاتر باشد، کوبیت ها انرژی بیشتری دارند و بیشتر احتمال دارد با محیط خود تعامل داشته باشند. * **تکان ها:** کوبیت ها همچنین می توانند توسط ارتعاشات دکور شوند. این به این دلیل است که ارتعاشات می توانند باعث حرکت کوبیت ها شوند، که می تواند حالت های کوانتومی آنها را مختل کند. * **تابش الکترومغناطیسی:** کوبیت 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 کوبیت ها تعامل داشته باشد و باعث از دست رفتن خواص کوانتومی آنها شود.

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

* **کوبیت ها را تا دماهای بسیار پایین سرد کنید:** این می تواند انرژی کوبیت ها را کاهش دهد و آنها را کمتر مستعد تعامل با محیط خود کند. * **استفاده از مواد با زمان های coherence طولانی:** برخی از مواد، مانند ابررساناها، زمان های coherence بسیار طولانی دارند که آنها را برای استفاده در رایانه های کوانتومی بسیار مناسب می کند. * **توسعه الگوریتم های جدید تصحیح خطا کوانتومی:** الگوریتم های تصحیح خطا کوانتومی می توانند برای تشخیص و تصحیح خطاهایی که توسط decoherence ایجاد می شوند استفاده شوند.

Decoherence یک مشکل پیچیده و چالش برانگیز است، اما یکی از مهمترین مشکلاتی است که در حال حاضر توسعه رایانه های کوانتومی را پیش رو دارد. با ادامه تحقیقات، به احتمال زیاد قادر خواهیم بود دکوراسیون را برطرف کنیم و رایانه های کوانتومی عملی بسازیم که می توانند مشکلاتی را حل کنند که برای رایانه های کلاسیک غیرقابل حل هستند.

+++++++

در شبیه‌سازی با کامپیوترکلاسیک نمی‌توان میزان ناهمدوسی را شبیه سازی کرد. عکس از چنل یوتیب بذار و کدها رو باهم مقایسه کن.

۳.۲ Qiskit and computer Quantum IBM

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 $f(x)$، می‌تواند مقادیر مختلف x را به طور همزمان بررسی کند. این درحالیست که در محاسبات کلاسیک به دلیل ماهیت بیت‌های اطلاعات، تابع $f(x)$ فقط می‌تواند یکی از مقادیر مجاز برای x را بررسی کند.

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

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

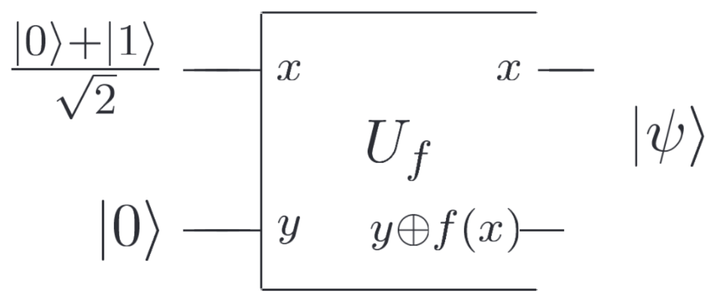
روش مناسب برای محاسبه این تابع در یک کامپیوتر کوانتومی، با در نظر گرفتن دو کیوبیت که در حالت $|x, y\rangle$شروع می شود. با یک توالی مناسب از گیت های منطقی می توان این حالت را به

[۱] Quantum parallelism

$|f(x) \oplus x, y\rangle$ 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 $\mathrm{y} = 0$ 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 $|x, y \oplus f(x)\rangle \to |x, y\rangle$، 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] ex- For .۲ by division a of remainder the returns that operation mathematical a is ۲ Modulo
.۱ of remainder a and ۲ of quotient a has ۲ by divided ۵ because ،۱ is ۲ mod ۵ ample،
would "۳ □ ۵" expression the So، .۲ modulo addition indicate to used often is "□" symbol The
follows: as evaluated be
a and ۴ of quotient a has ۲ by divided ۸ because is This ۰ = ۲ mod ۸ = ۲ mod (۳ + ۵) = ۳ □ ۵
.۰ of remainder
cryptography، including mathematics، of areas different many in operation useful a is ۲ Modulo
checking when example، for life، everyday in used also is It theory. number and science، computer
odd. or even is number a whether
:۲ modulo of examples other some are Here
۱ = ۲ mod ۵ ۰ = ۲ mod ۴ ۱ = ۲ mod ۳ ۰ = ۲ mod ۲ ۱ = ۲ mod 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 (۰) وf (۱) 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 n کوبیت 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:

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

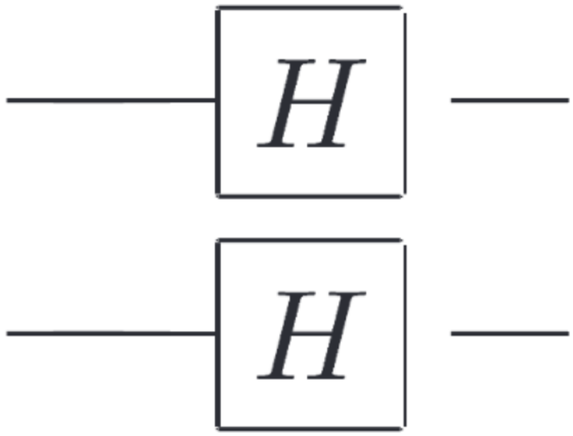
از نماد $H\otimes 2$ به عنوان نشانه‌ی عملکرد موازی دو گیت هادامارد استفاده می‌کنیم؛از علامت $\otimes$ به عنوان تانسور یاد می‌کنیم. به طور کلی نتایج اعمال موازی گیت هادامارد روی n کیوبیت روی حالت کوانتومی برابرست با:

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

در اینجا، $\sum$ نشان دهنده جمع بر روی همه مقادیر ممکن x است، و ما$H\otimes n$ 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 $H\otimes 2$ 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 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:
(x)⍰ ۱√۲n∑x|x⍰|f

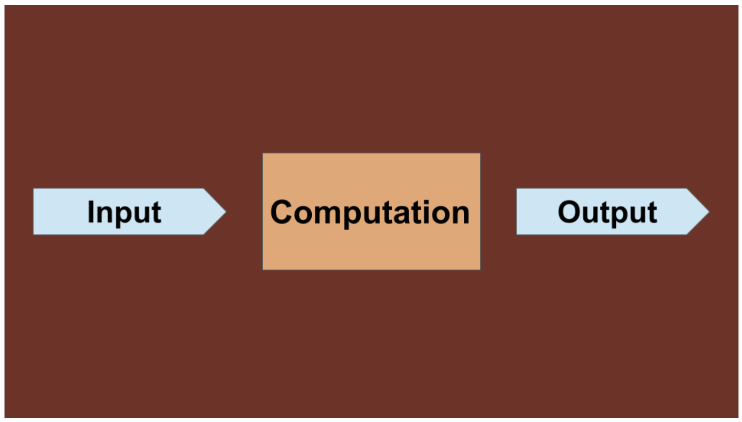
$$\frac{1}{\sqrt{2^n}}\sum_x |x\rangle|f(x)\rangle$$

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 کوبیتی ما، اندازه‌گیری حالت فقط $|0, f(0)\rangle$ یا $|1, f(1)\rangle$ را می‌دهد! به طور مشابه، در حالت کلی، اندازه‌گیری حالت ∑x ،f |x⍰ (x) 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 سوپرپوزیسیون مانند ∑x ،f |x⍰ (x) نیاز دارد. در بخش های بعدی به مثال‌های خواهیم پرداخت که این مسائل را حل کند.

$\sum_x |x, f(x)\rangle$

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.

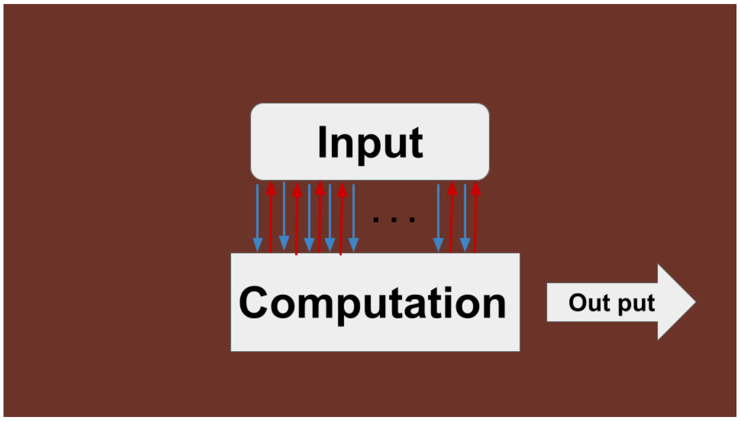
در تصویر بالا یک نمود ساده از کامپیوترهای امروزی ارائه شده است. در دنیای واقعی مقدار ورودی می‌تواند از هر منبعی تأمین شده باشد. با این وجود هدف ما بررسی منابع تولید ورودی نیست؛ بلکه هدف بررسی مقادیر ورودی (به صورت ایزوله) می‌باشد. می‌توان درنظر گرفت که ورودی داده شده و خروجی نهایی،هر دو در قالب یک رشته 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 input دریافت کند. در گاهی از مواقع به سیستم oracle،input 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 را



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.

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 Deutsch 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 کامپیوترهای کلاسیک است.

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

[۴] Deutsch David

$$f : \sum \rightarrow \sum$$

هدف بررسی ثابت بودن یا متعادل[5] بودن تابع f است. به‌طور کلی، درساده‌ترین حالت، می‌توان چهار وضعیت را برای تابع $f : \sum \rightarrow \sum$ 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:

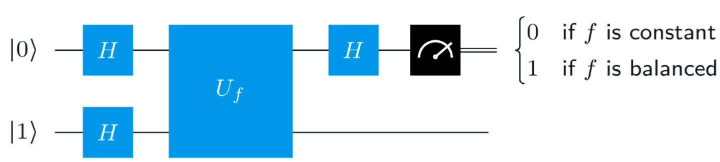
در شکل بالا توابع f 1 ، f 4 توابع ثابت و توابع f 2 و f 3 توابع متعادل هستند.

مسئله‌ی دوچ	
ورودی	$f : \sum \rightarrow \sum$
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:

[5] balanse. or Constante

یک تغییر ساده در مدار شکل ۳.۱ نشان می دهد که چگونه مدارهای کوانتومی می توانند با پیاده سازی الگوریتم Deutsch از مدارهای کلاسیک پیشی بگیرند[۶]. الگوریتم Deutsch 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 کوبیت به عنوان superposition (|۰? + |۱?)/√۲ استفاده کنیم، اما اکنون کوبیت دوم y را با اعمال یک گیت هادامارد به حالت |۱> به عنوان superposition (|۰? - |۱?)/√۲ 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 interference is using in deutsch algorithm : Interference is used in the Deutsch algorithm
to distinguish between constant and balanced functions. A constant function is a function that always returns the same value، regardless of its input. A balanced function is a function that returns ۰ for half of its inputs and ۱ for the other half.

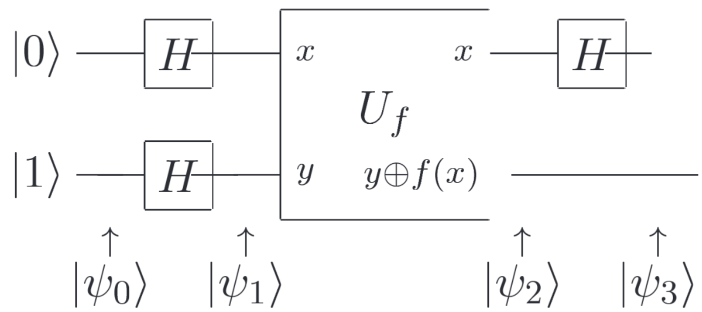
The Deutsch algorithm works by first preparing two qubits in a superposition of states. The first qubit is prepared in the state |+?، which is the equal superposition of |۰? and |۱?. The second qubit is prepared in the state |??، which is a superposition of the states |۰? and |۱? with opposite phases.

The two qubits are then passed through a quantum circuit that includes a Hadamard gate and a CNOT gate. The Hadamard gate transforms |+? into the superposition |۰? + |۱?، and the CNOT gate copies the state of the 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 |۰?، then the function f is constant. This is because the state |?? is orthogonal to the state |۰?، so the interference between the two states will destructively interfere.

If the first qubit is measured to be |۱?، then the function f is balanced. This is because the state |?? is parallel to the state |۱?، 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 a problem that is 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 Uf را به حالت ⍰|۰⍰)|x⍰ - |۱⍰)/√۲ اعمال کنیم، سپس به حالت f(۱-) ⍰|۰⍰)|x⍰(x) - |۱⍰)/√۲ می رسیم. بنابرین اعمال Uf به ⍰۱⍰| 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:

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

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.

۴.۳ الگوریتم دوچ - جوزا

algorithm، quantum general more a of case simple a is algorithm Deutsch's known application، The algorithm. Deutsch–Jozsa the as to refer shall we which Ams- in Alice، game. following the as described be may problem، Deutsch's as in Bob، to letter a in it mails and ،۱ - ۲n to ۰ from x number a selects terdam، which result، the with replies and (x) f function some calculates Bob Boston. of one of is which f function a use to promised has Bob Now، .۱ or ۰ either is balanced، is (x) f else or x، of values all for constant is (x) f either kinds؛ two half. other the for ۰ and x، possible the all of half exactly for ۱ to equal is، that constant a chosen has Bob whether certainty with determine to is goal Alice's fast How possible. as little as him with corresponding function، balanced a or succeed؟ she can

الگوریتم دوچ توضیح ساده از یک الگوریتم کوانتومی عمومی‌تر است که به عنوان الگوریتم دوچ-جوزا شناخته می‌شود. کاربرد این الگوریتم، که به عنوان مشکل دوچ شناخته می‌شود، به شرح زیر است:

آلیس، در آمستردام، یک عدد x را از بازه $[0, 2^n - 1]$ انتخاب می‌کند و آن را در یک نامه به باب، در بوستون، می‌فرستد. باب یک تابع$f(x)$ را محاسبه می‌کند و نتیجه را که ۰ یا ۱ است، ارسال می‌کند. اکنون، باب قول داده است که از یک مدل تابع استفاده خواهد کرد؛ این تابع یا$f(x)$ که برای همه مقادیر x ثابت است، یا $f(x)$ متعادل است، یعنی حاصل آن برای دقیقاً نیمی از همه هایx ممکن برابر با ۱ است و برای نیمی دیگر برابر با ۰ است.

هدف آلیس این است که با اطمینان و بکار بستن کمترین گام‌های ممکن تعیین کند که باب یک تابع ثابت یا متعادل را انتخاب کرده است. او چگونه می‌تواند به سرعت موفق شود؟

در حالت کلاسیک، آلیس ممکن است فقط یک مقدار x را در هر نامه به باب ارسال کند. در بدترین حالت، الی باید حداقل $\frac{2^n}{2} + 1$ بار از باب سوال کند، زیرا ممکن است قبل از دریافت یک، $\frac{2^n}{2}$ مرتبه پاسخ 0 را دریافت کند. آلیس باید یک را دریافت کند؛تا بتواند به او بگوید که تابع باب متعادل است.

یعنی در بهترین الگوریتم کلاسیک که می تواند استفاده کند بنابراین به$\frac{2^n}{2} + 1$ پرسش نیاز دارد. توجه داشته باشید که در هر نامه، آلیس n بیت اطلاعات را به باب ارسال می کند. علاوه بر این، در این مثال، فاصله فیزیکی باب و آلیس و به تبع آن افزایش هزینه محاسبه $f(x)$ و دشواری‌های احتمالی اجرای تابع $f(x)$ درنظر گرفته نشده‌است.

اگر باب و آلیس بتوانند کوبیت ها را به جای بیت های کلاسیک مبادله کنند، و اگر باب موافقت کند $f(x)$ را با استفاده از تبدیل یکه‌ی U_f محاسبه کند، سپس آلیس می تواند هدف خود را در یک مکاتبه با باب و با استفاده از الگوریتم زیر به دست آورد.

با توجه به الگوریتم دوچ، آلیس یک رجیستر n کوبیتی را برای ذخیره پرس و جو خود آماده می کند و یک رجیستر کوبیت واحد را که به باب می دهد تا پاسخ را در آن ذخیره کند. او هر دو رجیستر پرس و جو و پاسخ خود را در یک حالت برهمنهی آماده می کند. باب f(x) را با استفاده از موازی سازی کوانتومی ارزیابی می کند و نتیجه را به آلیس برمی گرداند. آلیس سپس با استفاده از اعمال تبدیل هادامارد روی رجیستر پرس و جو(n-کیوبیتی)، حالات برهمنهی تداخل می‌دهد و با انجام یک اندازه گیری مناسب، تعیین می کند که آیا f ثابت یا متعادل است.

گام‌های خاص الگوریتم در شکل ۲۰.۱ نشان داده شده است. بیایید با دنبال کردن این مدار، به بررسی حالات ایجاد شده بپردازیم. حالت ورودی ⍰۰⍰| = ⍰۱|n⍰⍰۰| (۴۶.۱)؛ شبیه حالت معادله (۴۱.۱) است، اما در اینجا رجیستر پرس و جو وضعیت n کوبیت را توصیف می‌کند که همه در حالت ⍰۰| آماده شده‌اند. پس از اعمال تبدیل هامادارد روی رجیستر پرس و جو و روی رجیستر پاسخ، می‌توان نوشت:

[۲√□۱| - □۰| ∑x□۰،۱n|x□√۲n[= |□۱□

reg- answer the and values، all of superposition a now is register query The is f function the Next، .۱ and ۰ of superposition weighted evenly an in is ister now Alice (۴۸.۱) giving (x)□، f □ y |x، □ y□ |x، : Uf using Bob) (by evaluated stored is evaluation function Bob’s of result the which in qubits of set a has terms interferes now She state. superposition qubit the of amplitude the in To register. query the on transform Hadamard a using position super- the in the calculate first to helps it transform Hadamard the of result the determine ۰ = x cases the checking By |x□. state a on transform Hadamard the of effect |z□/√۲. (-۱)xz z ∑ = H|x□ qubit single a for that see we separately ۱ = x and equa- useful very the in succinctly more summarized be can This (۴۹.۱) Thus Using .۲ modulo z، and x of product inner bitwise the is z · x where tion(۱.۵۰) observes now Alice |□۳□،(۱.۵۱) evaluate now can we (۴۸.۱) and equation this x(-۱)f ∑ is |۰□□n state the for amplitude the that Note register. query the (x)/۲n.

رجیستر پرس و جو اکنون یک برهمنهی از همه مقادیر ممکن به‌شمار می‌آید؛ درحالی که رجیستر پاسخ در یک برهمنهی به طور مساوی وزن شده از ۰ و ۱ محسوب می‌شود[۸].

در مرحله بعد، تابع f توسط باب و به شکل Uf : |x، □ y□ |x، □ y □ f□(x) ارزیابی می شود ، که (۴۸.۱) را می دهد.

آلیس اکنون یک مجموعه کوبیت دارد که در آن نتیجه اعمال تابع باب در دامنه کوبیت حالت برهمنهی ذخیره می شود. او اکنون با استفاده از تبدیل هادامارد روی رجیستر پرس و جو، عبارات را در حالت برهمنهی کوانتومی تداخل می کند.

برای تعیین نتیجه تبدیل هادامارد، بهترست ابتدا اثر تبدیل هادامارد را روی یک حالت |x□ محاسبه کنیم. با بررسی موارد x = ۰ و x = ۱ به صورت جداگانه می بینیم که برای یک کوبیت واحد H|x□ = ∑z (-۱)xz |z□/√۲ می‌باشد. بنابراین (۴۹.۱)

این را می توان به طور خلاصه در معادله بسیار مفید زیر خلاصه کرد:

(۵۰.۱)

جایی که z · x bitwise inner product x و z است، به modulo ۲.

با استفاده از این معادله و (۴۸.۱) اکنون می توانیم □۳□| را ارزیابی کنیم:

[۸] یعنی احتمال رخ‌دادن صفر و یک یکسان است.

(۵۱.۱)

آلیس اکنون رجیستر پرس و جو را مشاهده می کند. توجه داشته باشید که دامنه برای حالت n⟩۰| است $\sum f(-۱)x. n/۲(x)$

از استاد بپرس اشکاااااللل

discern to – balanced f and constant f – cases possible two the at look Let's or ۱+ is |۰⟩⟩n for amplitude the constant is f where case the In happens. what length unit of is |⟩۳⟩ Because takes. (x) f value constant the on depending ،۱- will observation an and zero، be must amplitudes other the all that follows it and positive the then balanced is f If register. query the in qubits all for ۰s yield amplitude an leaving cancel، |۰⟩⟩n for amplitude the to contributions negative one least at on ۰ than other result a yield must measurement a and zero، of the then ۰s all measures Alice if Summarizing، register. query the in qubit Deutsch–Jozsa The balanced. is function the otherwise constant؛ is function below. summarized is algorithm

بیایید به دو مورد ممکن - f ثابت و f متعادل - نگاه کنیم تا ببینیم چه اتفاقی می افتد.

در صورتی که f ثابت باشد، دامنه برای حالت n⟩⟩۰| برابر است با +۱ یا -۱، بسته به مقدار ثابت f (x) که می‌گیرد.

از آنجایی که ⟩۳⟩| طول واحد است، نتیجه می‌گیریم که تمام دامنه‌های دیگر باید صفر باشند، و یک مشاهده ۰ را برای همه کوبیت‌ها در رجیستر پرس و جو به همراه خواهد داشت.

اگر f متعادل باشد، سهم مثبت و منفی دامنه برای n⟩⟩۰| خنثی می‌شود، و یک دامنه صفر باقی می‌ماند، و یک اندازه‌گیری باید نتیجه‌ای غیر از ۰ را در حداقل یک کوبیت در رجیستر پرس و جو به همراه داشته باشد.

به طور خلاصه، اگر الی همه ۰ را اندازه گیری کند، تابع ثابت است؛ در غیر این صورت تابع متعادل است.

الگوریتم Deutsch-Jozsa در زیر خلاصه شده است:

the performs which Uf box black A (۱) Inputs: Deutsch–Jozsa Algorithm: ،۰ ⟩ (x) f and ۱ - ۲n ، . . . . ،۰ ⟩ x for (x)⟩، f ⟩ |x⟩y ⟩ |x⟩y⟩ transformation (x) f else or x، of values all for constant either is (x) f that promised is It .۱ for ۰ and x، possible the all of half exactly for ۱ to equal is، that balanced، is evalu- One Runtime: constant. is f if only and if ۰ Outputs: half. other the ⟩ .۲ state initialize |۰⟩⟩n|۱⟩ .۱ Procedure: succeeds. Always . Uf of ation

Hadamard using superposition create [۲√ ⍰۱| - ⍰۰|] |x⍰ x=۰ ∑۱- ۲n √۲n ۱
⍰ .۴ Uf using f function calculate [۲√ ⍰۱| - ⍰۰|] (x)|x⍰ (-۱)f x ∑ ⍰ .۳ gates
.۵ transform Hadamard perform [۲√ ⍰۱| - ⍰۰|] √۲n (x)|z⍰ (-۱)x·z+f x ∑ z ∑
computer quantum a that shown We’ve z output final obtain to measure z ⍰
compared f function the of ation evalu- one with problem Deutsch’s solve can
impres- appears This evaluations. ۱ + ۲n/۲ for requirement classical the to
is lem prob- Deutsch’s First، caveats. important several are there but sive،
Second، applications. known no has it problem؛ important especially an not
an ways some in is algorithms quantum and classical between comparison the
is function the evaluating for method the as comparison، oranges and apples
probabilistic a use to allowed is Alice if Third، cases. two the in different quite
randomly few a for (x) f evaluate to Bob asking by then computer، classical
is f whether probability high with determine quickly very can she x chosen
than realistic more perhaps is scenario probabilistic This balanced. or constant
caveats، these Despite considering. been have we scenario deterministic the
quan- impressive more for seeds the contains algorithm Deutsch–Jozsa the
principles the understand to attempt to enlightening is it and algorithms، tum
operation. its behind الگوریتم: Deutsch–Jozsa ورودی‌ها: (۱) یک جعبه سیاه Uf که تبدیل
زیر را انجام می‌دهد ⍰|x⍰|y ⍰ |x⍰|y ⍰ f ،⍰(x) برای x ⍰ ۰، ...، ۲n - ۱ و f (x) ⍰ ۰، ۱. قول
داده شده است که f (x) برای همه مقادیر x ثابت است یا f (x) متعادل است، یعنی برای دقیقاً نیمی از
همه هایx ممکن برابر با ۱ و برای نیمی دیگر ۰ است. خروجی: ۰ اگر و فقط اگر f ثابت باشد. زمان
اجرا: یک ارزیابی .Uf همیشه موفق می شود. روش:

⍰۱|n⍰⍰۰| حالت را initialize کنید ⍰ ۱ ۲n √۲n ۱- ∑۰= x ⍰|x [|۰⍰ - |۱⍰ √۲] ایجاد
superposition با استفاده از دروازه‌های Hadamard ⍰ ∑ x f(۱-) ⍰|x(x) [|۰⍰ - |۱⍰ √۲]
تابع f را با استفاده از Uf محاسبه کنید ⍰ ∑ z ∑ x f+x·z(۱-) ⍰|z(x) ۲n√ [|۰⍰ - |۱⍰ √۲]
تبدیل Hadamard را انجام دهید ⍰ z اندازه گیری کنید تا خروجی نهایی z را بدست آورید ما نشان
داده‌ایم که یک کامپیوتر کوانتومی می‌تواند مشکل Deutsch را با یک ارزیابی حل کند – ارزشیابی
تابع f در مقایسه با نیاز کلاسیک برای ۲n/۲ + ۱ ارزیابی. این به نظر چشمگیر است، اما چند نکته مهم
وجود دارد. اول، مشکل Deutsch نیست یک مشکل مهم است؛ هیچ کاربرد شناخته شده ای ندارد.
دوم، مقایسه بین الگوریتم های کلاسیک و کوانتومی تا حدودی مقایسه سیب و پرتقال است، زیرا روش
برای ارزیابی تابع در دو مورد بسیار متفاوت است. سوم، اگر آلیس مجاز باشد از یک کامپیوتر کلاسیک

احتمالی استفاده کند، سپس با درخواست از باب برای ارزیابی f (x) برای چند x به صورت تصادفی می تواند بسیار سریع تعیین کند با احتمال بالا اینکه f ثابت یا متعادل است. این سناریو احتمالی است شاید واقع بینانه تر از سناریوی determinstic که ما در نظر گرفته ایم. علیرغم این ظرافت ها، الگوریتم Deutsch–Jozsa حاوی بذرهای الگوریتم های کوانتومی بیشتر و چشمگیرتر است، و درک اصول پشت آن روشنگر است. عملکرد آن.

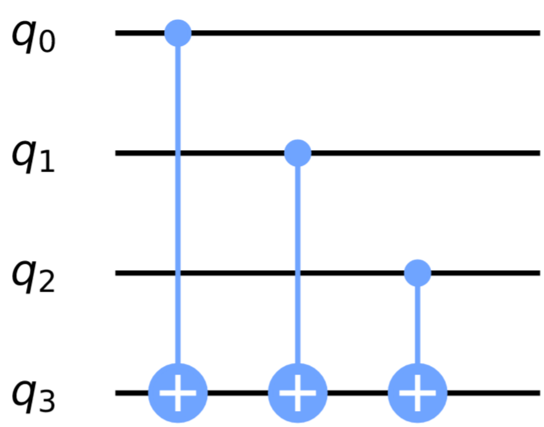
۵.۳ ساخت یک اوراکل کوانتومی

بیایید راه های مختلفی را ببینیم که می توانیم یک اوراکل کوانتومی ایجاد کنیم.

برای یک تابع ثابت، ساده است:

اگر f(x) = ۰، گیت را به کیوبیت در ثبات ۲ اعمال کنید. اگر f(x) = ۱، گیت را به کیوبیت در ثبات ۲ اعمال کنید.

برای عملکرد متعادل، مدارهای مختلفی وجود دارد که می توانیم ایجاد کنیم. یکی از راه‌هایی که می‌توانیم متوازن بودن مدار خود را تضمین کنیم، انجام یک CNOT برای هر کیوبیت در ثبات ۱، با کیوبیت موجود در ثبات ۲ به عنوان هدف است. مثلا:



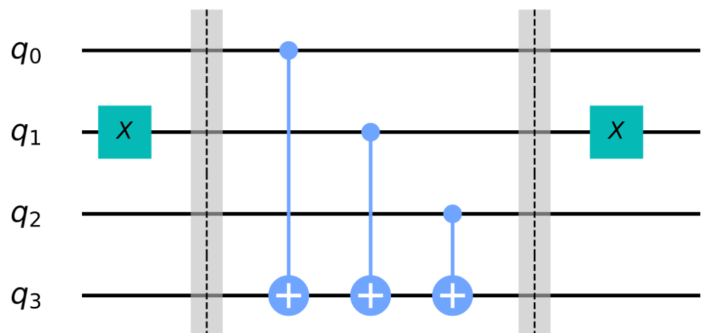
شکل ۸.۳:

در تصویر بالا، سه کیوبیت بالا، رجیستر ورودی را تشکیل می دهند و کیوبیت پایین، ثبات خروجی است. در جدول زیر می‌توانیم ببینیم کدام حالت‌های ورودی کدام خروجی را می‌دهند: ما می توانیم نتایج

حالاتی ورودی که به خروجی صفر منجر می‌شوند	حالاتی ورودی که به خروجی صفر منجر می‌شوند
۰۰۰	۰۰۱
۰۱۱	۱۰۰
۱۰۱	۰۱۰
۱۱۰	۱۱۱

جدول ۱.۳: This is a simple table.

را تغییر دهیم و در عین حال تعادل آنها را با قرار دادن کنترل های انتخاب شده در X-Gates حفظ کنیم. برای مثال، مدار و جدول نتایج آن را در زیر ببینید:



شکل ۹.۳:

حالاتی ورودی که به خروجی صفر منجر می‌شوند	حالاتی ورودی که به خروجی صفر منجر می‌شوند
۰۰۱	۰۰۰
۰۱۰	۰۱۱
۱۰۰	۱۰۱
۱۱۱	۱۱۰

جدول ۲.۳: This is a simple table.

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 states Bell

در اغلب موارد، سیستم از دو کیوبیت درهمتنیده تشکیل شده‌است. تابع حالت این سیستم‌ها به شکل زیر تعریف می‌شوند:

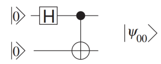
$$|\psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

برای آماده‌سازی این حالت کوانتومی، در حالت $|0\rangle$ داریم. با اعمال یک گیت هدامارد روی یکی از کیوبیت‌ها و سپس با کنترل آن با گیت CNOT، (به نحوی که کیوبیت دوم هدف قرارگیرد.) می‌توان به یک حالت درهمتنیده رسید. می‌توان این مراحل را به شکل زیر شرح داد:

$$|\psi_{00}\rangle = C_{10}H_1|00\rangle$$

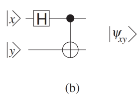
$$|\psi_{xy}\rangle = C_{10}H_1|xy\rangle$$

از آنجایی که چهار حالت $|xy\rangle$ یک مجموعه متعامد هستند و گیت‌های هادامارد و cNOT یکه هستند، چهار حالت درهم تنیده $|\psi_{xy}\rangle$ نیز یک مجموعه متعامد هستند، که به نام پایه Bell نامگذاری شده‌اند. می‌توان رابطه‌ی بالا را یک حالت کلی تعمیم داد:



(آ)
b

شکل ۱.۴: $y = x$



(آ)
b

شکل ۲.۴: $y = 3 \sin x$

شکل ۳.۴: (a) A circuit that creates the entangled state ⟨۰۰| = ۱√۲ (|۰۰⟩ + |۱۱⟩) from the unentangled computational-basis state |۰۰⟩. (b) A circuit that creates the four orthonormal entangled Bell states |ψxy⟩ from the unentangled computational-basis state |xy⟩

$$|\psi_{xy}\rangle = C10H1X_1^xX_0^y|00\rangle$$

درنظر داشته باشید که حالات بل قابل تبدیل به یکدیگرند؛ با کمک رابطه‌ی تعمیم یافته می‌توان از هر حالت بل به حالت $\langle 00|$ رسید. توضیحات درباره‌ی تبدیلات بنویس

این روابط به شکل‌های متعدد قابل بیان است که از حوصله‌ی بحث خارج است.

۲.۴ entanglement

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 کوبیت 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 کوبیت در حالت درهم‌تنیده زیر به اشتراک می‌گذارند:

$$|\text{?}\text{?}\rangle = |00\rangle + |11\rangle \sqrt{2} \quad (۱۳۳.۲)$$

=========

بیانات چی بیتی آلیس می‌تواند با استفاده از این جفت کوبیت‌های درهم‌تنیده، دو بیت کلاسیک را به باب منتقل کند. او این کار را با اعمال یک تبدیل واحد به کوبیت خود انجام می‌دهد، بسته به اینکه می‌خواهد کدام دو بیت کلاسیک را به باب ارسال کند. به عنوان مثال، اگر آلیس می‌خواهد بیت‌های ۰۰ را به باب ارسال کند، او تبدیل ۱ را به کوبیت خود اعمال می‌کند.

این تبدیل واحد باعث می‌شود که کوبیت آلیس و کوبیت باب در یکی از چهار حالت بل اورتوگونال قرار گیرند. اگر آلیس کوبیت خود را در حالت $|00\rangle$ قرار دهد، کوبیت باب به طور خودکار به حالت $|00\rangle$ تبدیل می‌شود. این بدان معناست که آلیس دو بیت اطلاعات (۰ و ۰) را به باب منتقل کرده است.

باب سپس کوبیت خود را اندازه‌گیری می‌کند و مقدار 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.

رمزگذاری متراکم یک پروتکل کوانتومی بسیار کارآمد است که می‌تواند دو بیت کلاسیک را با ارسال یک کوبیت منتقل کند. این پروتکل می‌تواند در کاربردهای مختلفی مانند رمزنگاری کوانتومی و ارتباطات کوانتومی استفاده شود.

==========

همانطور که در شکل ۳.۲ 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،

[۱] Quantum super dense coding

کوبیتی را به باب ارسال کند. در عوض، ممکن است یک طرف ثالث قبلاً حالت درهم‌تنیده را آماده کند، یکی از کوبیت‌ها را به آلیس و دیگری را به باب ارسال کند.

با ارسال تک کوبیت 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 X، NOT، را به کوبیت خود اعمال می‌کند.
- "11" را ارسال کند $\Longleftarrow$ تبدیل iY را به کوبیت خود اعمال می‌کند.

چهار حالت حاصل به راحتی قابل مشاهده هستند:

۰۰ : ▯▯| ▯ |۰۰▯ + |۱۱▯ ۲√ (۱۳۴.۲) ۰۱ : ▯▯| ▯ |۰۰▯ - |۱۱▯ ۲√ (۱۳۵.۲) ۱۰ : ▯▯|
▯ |۱۰▯ + |۰۱▯ ۲√ (۱۳۶.۲) ۱۱ : ▯▯| ▯ |۰۱▯ - |۱۰▯ ۲√ . (۱۳۷.۲)

همانطور که در بخش ۶.۳.۱ اشاره کردیم، این چهار حالت به عنوان پایه بل، حالت‌های بل، یا جفت‌های EPR شناخته می‌شوند، به احترام چندین تن از پیشگامان که اولین بار از نوآوری درهم‌تنیدگی قدردانی کردند. توجه داشته باشید که حالت‌های بل یک پایه متعامد هستند، و بنابراین می‌توانند با اندازه‌گیری کوانتومی مناسب از یکدیگر متمایز شوند. اگر آلیس کوبیت خود را به باب بفرستد، و باب هر دو کوبیت 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 کوبیت، قادر به انتقال دو بیت اطلاعات به باب است. البته دو کوبیت در پروتکل دخیل هستند، اما آلیس هرگز نیازی به تعامل با کوبیت 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.

بیانات چی پی تی: پروتکل سوپردنس کدینگ یک پروتکل کوانتومی است که آلیس می‌تواند از آن برای انتقال دو بیت کلاسیک به باب با ارسال یک کوبیت استفاده کند. پروتکل به شرح زیر است:

---

[۲] flip phase

آلیس و باب یک جفت کوبیت 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 کوبیت خود اعمال می‌کند که بسته به بیت‌هایی که می‌خواهد به باب ارسال کند متفاوت است. آلیس کوبیت خود را به باب می‌فرستد. باب کوبیت را اندازه‌گیری می‌کند و دو بیت کلاسیکی که آلیس به او ارسال کرده است را دریافت می‌کند. اگر آلیس یک عمل واحد بر روی کوبیت خود اعمال نکند، باب فقط می‌تواند یک بیت کلاسیک را دریافت کند. با این حال، اگر آلیس عمل واحد مناسب را اعمال کند، می‌تواند دو بیت کلاسیک را با ارسال یک کوبیت انتقال دهد.

پروتکل سوپردنس کدینگ 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.

۴.۴ دوربری

book isac فرض کنید آلیس یک کیوبیت در حالت زیر دارد:

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

کارول ممکن است با اعمال یک عملگر یکه به یک کیوبیت در حالت استاندارد، کیوبیت را از حالت $|0\rangle$ به حالت $|\psi\rangle$ تبدیل کرده باشد. کارول بدون اعلام نوع عملگر یکه به آلیس، کیوبیت را برای او ارسال می‌کند. حال آلیس می‌خواهد بدون دسترسی داشتن به کیوبیت باب، تغییراتی را در کیوبیت او ایجاد کند؛ این تنها درصورتی ممکن است که کیوبیت باب و آلیس درهمتنیده باشند. هرچند آلیس و باب می‌توانند از طریق راه‌های کلاسیک(نظیر تلفنی صحبت کردن و ...) با یکدیگر ارتباط برقرار کنند؛ ولی نمی‌توانند دسترسی مستقیم به کیوبیت یکدیگر داشته باشند.

کیوبیت باب را می‌توان به حالت زیر تعریف کرد: $|\phi\rangle = 1/\sqrt{2}(|0\rangle|0\rangle + |1\rangle|1\rangle)$

Alice's of state unknown the duplicating prohibits theorem no-cloning he possible be to out turns it But nearby. or her from away far either Qbit، first to |⍰⍰ state the assigning in telephone the over cooperate to Bob and Alice for violated not is theorem no-cloning The pair. entangled the of member Bob's of either from |⍰⍰ state the of traces all obliterates Alice so doing in because – Bob to Alice from state the teleporting called – process The Qbits. own her each For shared. formerly Bob and Alice tanglement en- the eliminates also term The state. ۱-Qbit single a just teleport can they pair، entangled shared Qbit Bob's by acquired assignment state the that emphasizes tion" "teleporta-Here his. to Qbit her from transported been has it Alice's؛ to applies longer no shares she pair entangled the and Qbit first Alice's works. teleportation how is ،(|۱⍰b |۱⍰a + |۰⍰b (|۰⍰a ۲√۱ (state ۳-Qbit the by characterized are Bob with Bob's and Alice's in Qbits the for symbols state the given have I where (۲۱.۶) to Qbit her of state unknown the teleport To . b and a subscripts possession her using gate، cNOT a applies first Alice pair، entangled the of member Bob's entangled shared the of member her and control the as |⍰⍰ state the in Qbit first + |۰⍰b (|۰⍰a ۲√۱ α|۰⍰a state ۳-Qbit the produces This target. the as pair a applies she Next (۲۲.۶) .(|۱⍰b |۰⍰a + |۰⍰b (|۱⍰a ۲√۱ ⍰|۱⍰a + (|۱⍰b |۱⍰a α state the Qbits three all giving Qbit، first her to H transformation Hadamard

۲√۱ (|۱�a - (|۰�a ۲√۱ � + (|۱�b |۱�a + |۰�b (|۰�a ۲√۱ (|۱�a + (|۰�a ۲√۱
(α|۰�b |۰�a |۱�a ۲ ۱ + (�|۱�b + (α|۰�b |۰�a |۰�a ۲ ۱ = (|۱�b |۰�a + |۰�b (|۱�a
.(�|۰�b - (α|۱�b |۱�a |۱�a ۲ ۱ + (�|۰�b + (α|۱�b |۱�a |۰�a ۲ ۱ + (�|۱�b -
in remarked (As possession. her in Qbits both measures Alice Now (۲۳.۶) immediately gates، Hadamard and cNOT of application an such ،۴.۶ Section the If basis.") Bell the in "measuring called is gates، measurement by followed possessed originally |�� state the acquire indeed will Qbit Bob's ،۰۰ is result the if But .(�۰| to reduced be then would state (whose Qbit first Alice's by Qbit Bob's of state the then ۱۱ or ،۰۱ ،۱۰ is measurement Alice's of result of each In (۲۴.۶) . �|۰�b - α|۱�b or ، �|۰�b + α|۱�b ، �|۱�b - α|۰�b becomes of state the stores re- that transformation unitary a is there cases three these (which Z apply can we case first the In |��. state original Alice's to Qbit Bob's (which X case، second the in ،(�۱| of sign the changes but alone �۰| leaves I T A T R O P E L TE ۵ . ۶ ZX. case، third the in and ،(�۱| and �۰| interchanges member Bob's to Qbit her of state the transfer to do need Alice all So ۱۵۱ N O of results the him to report and Bob telephone to is pair entangled their of been already has state the whether knows then He measurements. two her must he transformation unitary what or (۰۰ is result Alice's (if transferred transfer the plete com- to order in pair entangled the of member his to apply quantum to resemblance the Note three.) other the of one is result Alice's (if information the acquires Alice measurement a making by correction: error anybody without state، quantum ular partic- a reconstruct to Bob for needed be to appears This is. actually state the what about information any acquiring α numbers complex two by described is Qbit a of state general A remarkable. requirement the by only constrained values، of continuum a on take that � and state whose pair، entangled standard a of aid the with Yet، .۱ = |�|۲ + |α|۲ that described Qbit a with Bob provide to able is Alice �، and α on depend not does information classical of bits two only of price the at state، unknown the by entanglement the of loss the and measurements) two her of results the (giving pair. their of

the Bob to communicate not does process teleportation the course of But the learn to able more no is Bob ⍰. and α in encoded be can that information than |⍰⍰، state the assigned now Qbit، his manipulating from ⍰ and α of values state same the assigned was that Qbit her was it when do to able was Alice of stage crucial a at produced be could state Alice's hand other the On |⍰⍰. him enable could Bob to transfer its and computation، quantum elaborate an computer، quantum far-away own his on computation the with continue to dense Like teleportations. such by objective nontrivial a achieve can one s elementary an manipulating by constructed be also can teleportation coding، –(۲۱.۶) in analysis the of any through going without diagram، circuit classical of |x⍰ = |⍰⍰ state the exchanges that circuit a shows (a)۵.۶ Figure .(۲۴.۶) .۱ or ۰ = x whether of regardless Cbit، Bob's of ⍰۰| state the with Cbit Alice's As Cbits. two the between coupling physical direct by achieved is transfer The arbitrary for exchange this perform to continues it circuit quantum linear a be can protocol teleportation entire The ⍰|۱⍰. + α|۰⍰ = |⍰⍰ superpositions، with ،(a)۵.۶ Figure in gates two the expanding appropriately by constructed direct the eliminate to is expansion the of aim The Qbit. ancillary an of aid the in gates cNOT two the through Qbits Bob's and Alice's between interaction the and Bob، to Alice from message telephoned the of favor in ،(a)۵.۶ Figure (which Qbits entangled of pair shared their produce to necessary interaction |⍰⍰). state the in Qbit her acquired even has Alice before well place take can

۱

oracle a determine to how