

فهرست مطالب

۲	۱.۰ مقدمه
۳	۱ آشنایی با مفاهیم اولیه
۳	۱.۱ کیوبیت
۵	۲.۱ کیوبیت‌های چندتایی
۶	۳.۱ اندازه‌گیری در فضای هیلبرت
۶	۴.۱ vector bloch
۹	۵.۱ گیت‌های کوانتومی
۹	۱.۵.۱ انواع گیت کوانتومی
۱۳	۲.۵.۱ gate Swap
۱۳	۶.۱ مدارهای کوانتومی
۱۵	۱.۶.۱ نحوه‌ی نمایش مدارهای کوانتومی
۱۷	۲ برنامه‌نویسی کوانتومی
۱۷	۱.۲ تفاوت کامپیوتر کلاسیک و کوانتومی
۱۸	۲.۲ simulation vs comp
۱۹	۱.۲.۲ تفاوت کامپیوترهای کوانتومی و شبیه‌سازهای کلاسیک
۲۱	۳.۲ Qiskit and computer Quantum IBM
۲۳	۳ الگوریتم‌های کوانتومی
۲۳	۱.۳ موازی سازی کوانتومی
۲۷	۱.۱.۳ مدل محاسباتی استاندارد
۲۷	۲.۳ مدل کوثری

۳.۳	معرفی و پیاده سازی الگوریتم دوچ	۲۸
۱.۳.۳	مسئله‌ی دوچ	۲۸
۲.۳.۳	الگوریتم دوچ	۲۹
۴.۳	الگوریتم دوچ - جوزا	۳۲
۵.۳	ساخت یک اوراکل کوانتومی	۳۷
۴	شبیه سازی پدیده های کوانتومی	۳۹
۱.۴	states Bell	۳۹
۲.۴	entanglement	۴۱
۳.۴	رمزگذاری متراکم کوانتومی	۴۲
۴.۴	دوربری	۴۵

۱.۰ مقدمه

در عصر حاضر بواسطه‌ی رشد و توسعه‌ی نظریه‌ی اطلاعات کوانتومی و سرمایه گذاری 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

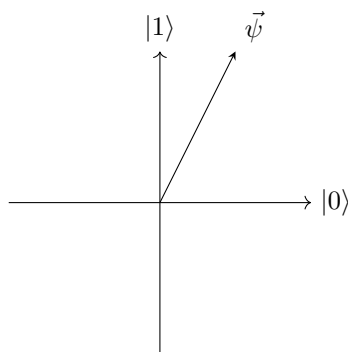
یک کیوبیت^۱، معادل یک واحد اطلاعات کوانتومی می‌باشد. این مفهوم معادل مفهوم کلاسیک بیت^۲ می‌باشد. به طور کلی هر کیوبیت حاوی دو بیت اطلاعات است. برای تبیین یک کیوبیت از خصوصیات سامانه های کوانتومی، بهره می‌بریم. کیوبیت یک سیستم کوانتومی با فضای دوبعدی است. برای تعیین این دوبعد می‌توان از یکی از خصوصیات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

برخلاف بیت ها که مقادیر ثابت ۰ یا ۱ را به خود می‌گیرند؛ یک کیوبیت می‌تواند در یک حالت «برهمتهی 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 برهمتهی، به شرح زیر است:

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

Qubit^۱
Binary Bit^۲

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 $\vec{\psi}$ 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:

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad (۱.۱)$$

برای تعریف کیوبیت‌ها، راه‌های زیادی وجود دارد، حالات قطبش فوتون، اسپین الکترون، یا سطوح انرژی اتم، هر یک می‌توانند تعیین‌کننده‌ی بردارهای فضای کیوبیت باشند.

به طور کلی، حالت کیوبیت یک بردار واحد در فضای برداری دو بعدی پیچیده است. در بیشتر مدل‌های انتزاعی ما از جهان، یک ارتباط مستقیم بین عناصر انتزاع و دنیای واقعی وجود دارد، درست همانطور که طرح‌های یک معمار برای یک ساختمان با ساختمان نهایی مطابقت دارد. فقدان این ارتباط مستقیم در مکانیک کوانتوم باعث می‌شود که رفتار سیستم‌های کوانتومی دشوار باشد؛ با این حال، یک ارتباط غیرمستقیم وجود دارد، زیرا می‌توان حالت‌های کیوبیت را دستکاری و تبدیل کرد به روش‌هایی که منجر به نتایج اندازه‌گیری می‌شود که به طور متمایز به خواص مختلف حالت بستگی دارد. بنابراین، این حالت‌های 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 سکه‌های غیرایده‌آل، ممکن است حالت‌های واسطه‌ای مانند قرار گرفتن آن روی لبه وجود داشته باشد، اما در حالت ایده‌آل می‌توان آنها را نادیده گرفت. در مقابل، یک کیوبیت می‌تواند در یک طیف پیوسته از حالت‌ها بین $|0\rangle$ و $|1\rangle$ وجود داشته باشد

^۳Computational Basis Vectors

- تا زمانی که مشاهده شود. بار دیگر تاکید می‌کنیم که وقتی یک کیوبیت اندازه‌گیری می‌شود، فقط «۰» یا «۱» را به عنوان نتیجه اندازه‌گیری می‌دهد - به صورت تصادفی. به عنوان مثال، یک کیوبیت می‌تواند در حالت $|0\rangle + |1\rangle$ باشد، که به این معنی است که با احتمال $50/50$ می‌تواند به عنوان ۰ یا ۱ اندازه‌گیری شود.

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

حالت $|+\rangle$ از کیوبیت است که با یک بردار ۲ بعدی واحد نشان داده می‌شود. این حالت، زمانی که اندازه‌گیری شود، نتیجه ۰ را ۵۰ درصد از زمان و نتیجه ۱ را ۵۰ درصد از زمان می‌دهد. این حالت را می‌توان 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. حالت‌های پایه $|0\rangle$ و $|1\rangle$ تنها حالاتی هستند که می‌توانند به طور مستقیم مشاهده شوند. حالت $|+\rangle$ ، با این حال، یک حالت ترکیبی است که به طور مستقیم قابل مشاهده نیست. تنها زمانی می‌توان آن را مشاهده کرد که اندازه‌گیری شود. با وجود غیرقابل مشاهده بودن، حالت $|+\rangle$ واقعی است. وجود آن توسط آزمایشات به طور گسترده‌ای تأیید شده است. همچنین می‌توان از آن برای انجام محاسبات کوانتومی استفاده کرد. در آینده، ممکن است حالت $|+\rangle$ برای اهداف مختلف دیگری نیز استفاده شود. به عنوان مثال، می‌تواند برای ذخیره اطلاعات یا برای ایجاد ارتباطات امن استفاده شود.

۲.۱ 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 می‌شود. یک جفت کیوبیت همچنین می‌تواند 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 می‌شود - به هر حالت محاسباتی، بیان می‌شود. بردار حالت توصیف کننده دو کیوبیت به شکل زیر است:

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

جایی که a, b, c و d دامنه‌های چهار حالت را نشان می‌دهند. دامنه‌ها می‌توانند هر عدد مختلطی باشند، اما معمولاً به گونه‌ای نرمال می‌شوند 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 $|x\rangle$. 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 $|a|^2 + |b|^2$ 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 می رود، 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.

۳.۱ اندازه گیری در فضای هیلبرت

۴.۱ 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:

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

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 $|+\rangle$ ، $|-\rangle$ ، $|+\rangle$ 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 $|\alpha|^2 + |\beta|^2 = 1$ 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.

۵.۱ 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.

۱.۵.۱ انواع گیت کوانتومی

گیت‌های کوانتومی، دارای انواع مختلف گوناگونی می‌باشند. به طور کلی گیت‌های کوانتومی، عملگرهایی یکه و بازگشت‌پذیر می‌باشند. به طور کلی گیت‌های کوانتومی متناسب با تعداد کیوبیت‌هایی که از آنها اثر می‌گیرند؛ 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 به یک حالت برهم‌نهی کوانتومی گذار می‌کند. به عبارت دیگر هر یک از زیرحالات این حالت برهم‌نهی، با احتمال یکسانی قابل رخ دادن هستند.

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

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

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

Quantum Gates^۴
Hadamard gate^۵

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

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

این گیت کوانتومی، یک گیت بازگشت پذیر است؛ یعنی اگر این گیت روی یک حالت کوانتومی اثر کند؛ می تواند آن را از حالت برهنه بیرون بیاورد.

برای اعمال این گیت کوانتومی، فقط به یک کیوبیت نیاز داریم. به اصطلاح این گیت، یک Single-Qubit Quantum gate می باشد.

نمایش این گیت کوانتومی در مدار با علامت زیر است:



گیت CNOT

گیت کوانتومی CNOT^۶، به عنوان گیت منطقی نیز یاد می شود. این گیت کوانتومی معادل گیت NOT کلاسیک می باشد. به طور 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 $|1\rangle$ باشد، باعث تغییر وضعیت «کیوبیت هدف^۸» می شود.

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 می ماند. 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 بی تغییر رها کند.

^۶gate controlled-X or gate controlled-NOT

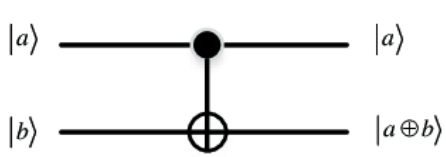
^۷Qubit Controlled

^۸Qubit Target

خلاصه‌ای از عملکرد این عملگر به شرح زیر است:
 ببین چرا از این نماد به جای تئسور پراداکت استفاده شده

$ A \rangle$ $ control\rangle$	$ B\rangle$ $ target\rangle$	Effect CNOT Gate	$ A \oplus B \rangle$ $ control\rangle$	$ B\rangle$ $ target\rangle$
$ 0\rangle$	$ 0\rangle$	\Rightarrow	$ 0\rangle$	$ 0\rangle$
$ 0\rangle$	$ 1\rangle$	\Rightarrow	$ 0\rangle$	$ 1\rangle$
$ 1\rangle$	$ 0\rangle$	\Rightarrow	$ 1\rangle$	$ 1\rangle$
$ 1\rangle$	$ 1\rangle$	\Rightarrow	$ 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:

$$CNOT |1\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = |1\rangle$$

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

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

گیت تغییر فاز

گیت تغییر فاز^۹، یکی از گیت‌های مهم کوانتومی می‌باشد. این گیت با ضرب کردن یک عدد ثابت در فاز یک کیوبیت، باعث تغییر فاز کیوبیت می‌شود. این گیت کوانتومی در بسیاری از الگوریتم‌های سرچ کوانتومی به کار می‌رود. این گیت بدین صورت تعریف می‌شود:

فرم ماتریسی این گیت به شرح زیر است:

این گیت کوانتومی در مدار کوانتومی به شکل زیر نشان داده می‌شود:

گیت دوران

گیت دوران^{۱۰}، باعث دوران حالت کیوبیت، در فضای هیلبرت می‌شود. پایه‌های فضای هیلبرت مذکور بردارهای هستند. نمایش این گیت کوانتومی به شرح زیر است:

فرم ماتریسی این گیت به شرح زیر است: نمایش این گیت در مدار کوانتومی به شرح زیر است:

gate shift Phase^۹
gate Rotation^{۱۰}

۲.۵.۱ gate Swap

۶.۱ مدارهای کوانتومی

مدارهای کوانتومی^{۱۱}، یک دسته از گیت های کوانتومی، که با یک توالی بخصوص قرار گرفته اند، می باشند. این کیوبیت ها، با توالی یاد شده، روی یک یا چند دسته کیوبیت، اثر داده می شوند. مدارهای کوانتومی، یکی از اولین مفهومی های بکاررفته برای تعریف کامپیوترهای کوانتومی می باشند. برای تعریف و شبیه سازی هریک از پدیده ها و الگوریتم های کوانتومی، نیاز به پیاده سازی یک مدار به خصوص 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.

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.

^{۱۱}circuit quantum

- 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 برهمه‌نی 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 table a with ۳ rows and ۳ columns.

اجزای مدارهای کوانتومی و سائز 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 su -perposition 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، 0 یا 1 استفاده می شود. راه اندازی ها برای تنظیم حالت یک کویت به یک مقدار خاص، 0 یا 1 استفاده می شوند.

اجزای اساسی یک مدار کوانتومی کویت 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.

۱.۶.۱ نحوه 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 کویت ها را نشان می دهد. دروازه ها توسط جعبه ها نشان داده می شوند و خطوط بین جعبه ها نشان دهنده ارتباطات بین کویت 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. بنابراین 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. در این 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 هر یک از عملگرهای 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 مسئله بستگی دارد. در محاسبات کلاسیک هرچه تعداد حالات بالاتر برود؛ پیچیدگی محاسبات بالاتر می‌رود و حتی اغلب با حالت نمایی رشد می‌کنند. این درحالیست که در محاسبات کوانتومی هر یک حالات مختلف مسئله 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. [۹] : درکودانس در محاسبات کوانتومی مهم است زیرا اصلی‌ترین منبع خطا در این سیستم‌ها است. کویت‌ها، واحد‌های اصلی اطلاعات در محاسبات کوانتومی، بسیار حساس به محیط خود هستند و می‌توانند به راحتی توسط interactions با فوتون‌ها، الکترون‌ها و سایر ذرات دکور شوند. این می‌تواند باعث شود که کویت‌ها خواص کوانتومی خود را مانند superposition و entanglement که برای انجام محاسبات کوانتومی ضروری هستند، از دست بدهند.

Decoherence می‌تواند توسط عوامل مختلفی ایجاد شود، از جمله:

* **دما: کویت‌ها در دماهای بالاتر مستعد دکوراسیون هستند. این به این دلیل است که هرچه دما بالاتر باشد، کویت‌ها انرژی بیشتری دارند و بیشتر احتمال دارد با محیط خود تعامل داشته باشند. * **تکان‌ها: کویت‌ها همچنین می‌توانند توسط ارتعاشات دکور شوند. این به این دلیل است که ارتعاشات می‌توانند باعث حرکت کویت‌ها شوند، که می‌تواند حالت‌های کوانتومی آنها را مختل کند. * **تابش الکترومغناطیسی: کویت‌ها می‌توانند توسط تابش الکترومغناطیسی، مانند نور و امواج رادیویی، دکور شوند. این به این دلیل است که تابش الکترومغناطیسی می‌تواند با الکترون‌های کویت‌ها تعامل داشته باشد و باعث از دست رفتن خواص کوانتومی آنها شود.

Decoherence یک مانع بزرگ برای توسعه ابررایانه‌های کوانتومی است. برای ساخت یک رایانه کوانتومی عملی، باید راه‌هایی برای کاهش دکوراسیون پیدا کرد. این یک مشکل دشوار است، اما تعدادی از مسیرهای تحقیقاتی امیدوارکننده وجود دارد، مانند:

* ** کویت ها را تا دماهای بسیار پایین سرد کنید: ** این می تواند انرژی کویت 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 شبیه سازی با کامپیوتر کلاسیک نمی توان میزان ناهمدوسی را شبیه سازی کرد. عکس از چنل یوتیوب بنادر و کدها رو باهم مقایسه کن.

Qiskit and computer Quantum IBM ۳.۲

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 کامپیوترهای کوانتومی 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

موازی سازی کوانتومی^۱، پایه و اساس 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:

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

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

^۱parallelism Quantum

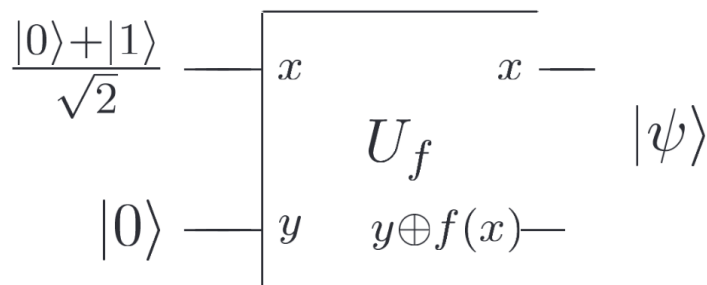
$|f(x) \oplus x, y\rangle$ تبدیل کرد که در آن \oplus بیانگر جمع مدوله با پایه ۲ می‌باشد.

۲

هریک از دسته‌های کیویت، رجیستر کوانتومی نامیده می‌شوند. اولین رجیستر، «رجیستر داده» و دومین رجیستر «رجیستر هدف» نامیده می‌شود.

ازین پس در این بخش به عامل گذار $|x, y \oplus f(x)\rangle \rightarrow |x, y\rangle$ ، عنوان «تابع U_f » را اطلاق خواهیم کرد. لازم به ذکر است که این تبدیل، یک تبدیل یک به شمار می‌آید.^۳

اگر $y = 0$ آنگاه مقدار دومین کیویت 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. U_f مدار کوانتومی است که ورودی‌هایی مانند $|x, y\rangle$ را به $|x, y \oplus f(x)\rangle \rightarrow |x, y\rangle$ ، 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 $|0\rangle$

Modulo ۲ is a mathematical operation that returns the remainder of a division. For example, ۵ divided by ۲ has a remainder of ۱, so ۵ mod ۲ = ۱. This operation is useful in 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

Here are some other examples of modulo ۲:

$$۱ = ۱ \bmod ۲, ۲ = ۰ \bmod ۲, ۳ = ۱ \bmod ۲, ۴ = ۰ \bmod ۲, ۵ = ۱ \bmod ۲$$

^۳اثبات 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؛ به نحوی که انگار $f(x)$ را برای دو مقدار x به طور همزمان ارزیابی کرده ایم، این ویژگی به ”موازی سازی کوانتومی“ موسوم می‌باشد. برخلاف موازی سازی کلاسیک، که در آن هر یک مدارهای متعددی دارند ساخته شده برای محاسبه $f(x)$ به طور همزمان اجرا می‌شوند، در اینجا برای ارزیابی تابع برای چندین مقدار x به طور همزمان، یک مدار $f(x)$ (با قابلیت برهمه‌نی کوانتومی) استفاده می‌شود. این فرآیند را می‌توان 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 کیوبیت عمل می‌کنند.

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:

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

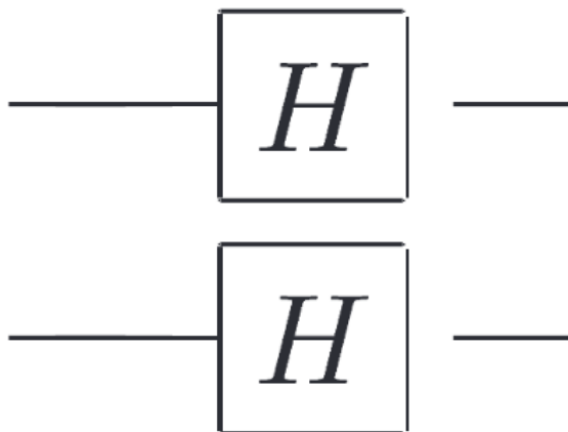
از نماد $H \otimes 2$ به عنوان نشانه‌ی عملکرد موازی دو گیت هادامارد استفاده می‌کنیم؛ از علامت \otimes به عنوان تانسور یاد می‌کنیم. به طور کلی نتایج اعمال موازی گیت هادامارد روی n کیوبیت روی حالت کوانتومی برابرست با:

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

در اینجا، \sum نشان دهنده جمع بر روی همه مقادیر ممکن x است، و $H \otimes n$ را برای نشان دادن این عمل می‌نویسیم. اعمال تبدیل هادامارد روی یک بهمنهی کوانتومی برابر از همه حالت‌های محاسباتی تولید می‌کند؛ و با استفاده از فقط n گیت، یک بهمنهی از $2n$ حالت تولید می‌کند.

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 برهمه‌نی قرار دارند.

در نهایت حالت زیر تولید می‌شود:

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

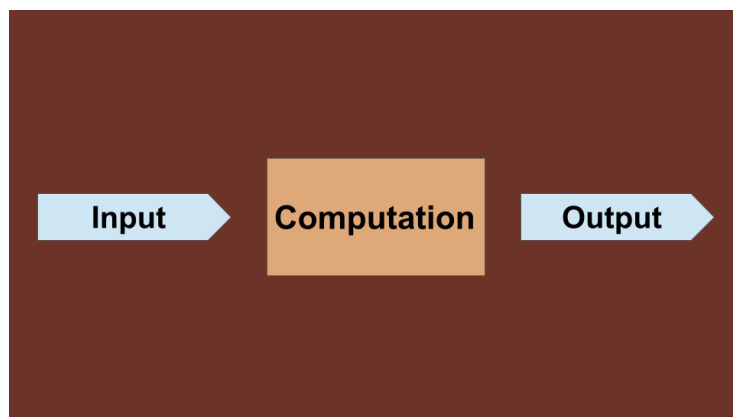
$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle$$

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 $\sum_x |x\rangle |f(x)\rangle$ 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 سوپروپوزیسیون مانند $\sum_x |x\rangle |f(x)\rangle$ نیاز دارد. در بخش‌های 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 کوثری، 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.

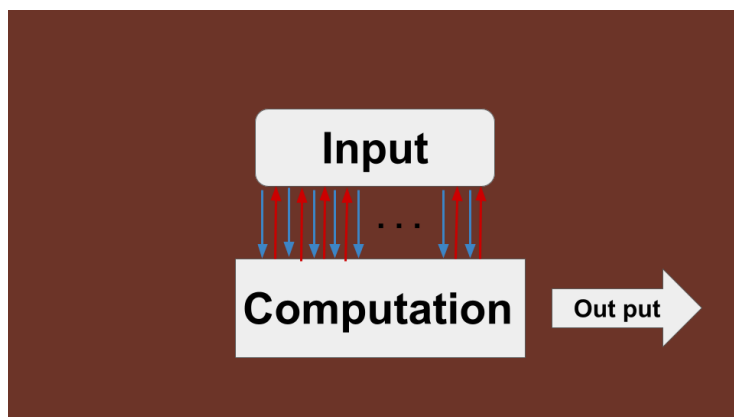
در تصویر بالا یک نمود ساده از کامپیوترهای امروزی ارائه شده است. در دنیای واقعی مقدار ورودی می‌تواند از هر منبعی تأمین شده باشد. با این وجود هدف ما بررسی منابع تولید ورودی نیست؛ بلکه هدف بررسی مقادیر ورودی (به صورت ایزوله) می‌باشد. می‌توان در نظر گرفت که ورودی داده شده و خروجی نهایی، هر دو در قالب یک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

در مدل کوثری، داده‌های ورودی توسط یک تابع تولید می‌شوند. واحد محاسباتی دسترسی به تابع تولید ورودی 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 در دسترس 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 محاسباتی کوثری 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 input می‌باشد.

دریافت کنیم.

تابع oracle به صورت زیر تعریف می‌شود:

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

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

۳.۳ معرفی و پیاده‌سازی 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 شده بود. 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:

^۴Deutsch David

$$f: \Sigma \rightarrow \Sigma$$

هدف بررسی ثابت بودن یا متعادل^۵ بودن تابع f است. به طور کلی، در ساده ترین حالت، می توان چهار وضعیت را برای تابع $f: \Sigma \rightarrow \Sigma$ در نظر گرفت:

a	$f_1(a)$	a	$f_2(a)$	a	$f_3(a)$	a	$f_4(a)$
0	0	0	0	0	1	0	1
1	0	1	1	1	0	1	1

شکل ۵.۳:

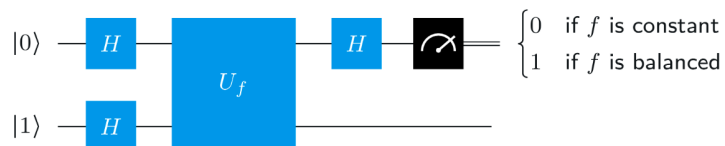
در شکل بالا توابع f_1 ، f_4 توابع ثابت و توابع f_2 و f_3 توابع متعادل هستند.

مسئله ی دوچ	
ورودی	$f: \Sigma \rightarrow \Sigma$
خروجی	صفر اگر تابع ثابت بود؛ یک اگر تابع متعادل بود.

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

۲.۳.۳ الگوریتم دوچ

حال به بررسی الگوریتم دوچ می پردازیم. الگوریتمی که مسئله ی دوچ را با یک مدار کوانتومی حل می کند:

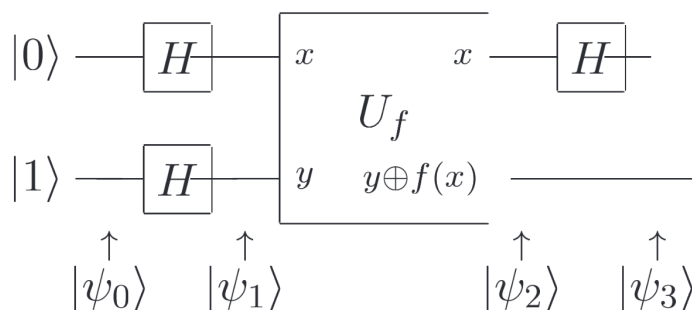


شکل ۶.۳:

^۵ balance. or Constante

یک تغییر ساده در مدار شکل ۳.۱ نشان می‌دهد که چگونه مدارهای کوانتومی می‌توانند 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 کویت به عنوان $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ استفاده کنیم، اما اکنون کویت دوم y را با اعمال یک گیت هادامارد به حالت $|1\rangle$ به عنوان $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ superposition آماده کنیم. به شکل زیر دقت کنید:

^۶ ما در واقع یک نسخه ساده شده و بهبود یافته از الگوریتم اصلی را ارائه می‌دهیم.
^۷ algorithm Deutsch the in used is Interference : algorithm deutsch in using is interference how
 that function a is function constant A functions. balanced and constant between distinguish to
 that function a is function balanced A input. its of regardless value, same the returns always
 half. other the for ۱ and inputs its of half for ۰ returns
 first The states. of superposition a in qubits two preparing first by works algorithm Deutsch The
 second The $|0\rangle$ and $|1\rangle$ of superposition equal the is which $|0\rangle$ state the in prepared is qubit
 opposite with $|0\rangle$ and $|1\rangle$ states the of superposition a is which $|0\rangle$ state the in prepared is qubit
 phases.
 and gate Hadamard a includes that circuit quantum a through passed then are qubits two The
 CNOT the and $|0\rangle + |1\rangle$ superposition the into $|0\rangle$ transforms gate Hadamard The gate. CNOT a
 qubit. second the to qubit first the of state the copies gate
 is qubit first the If measured. are qubits two the executed, been has circuit quantum the After
 to orthogonal is $|0\rangle$ state the because is This constant. is f function the then $|0\rangle$ be to measured
 interfere. destructively will states two the between interference the so $|0\rangle$ state the
 the because is This balanced. is f function the then $|0\rangle$ be to measured is qubit first the If
 constructively will states two the between interference the so $|0\rangle$ state the to parallel is $|0\rangle$ state
 interfere.
 solve to used be can interference quantum how of example simple a is algorithm Deutsch The
 distinguish can algorithm Deutsch the case, this In classically. solve to difficult is that problem a
 need would computer classical a while step, single a in functions balanced and constant between
 steps. of number exponential an take to



شکل ۷.۳: پیاده سازی مدار کوانتومی الگوریتم دوچ

حالت ورودی:

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

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

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

با کمی تأمل می توان دریافت که اگر U_f را به حالت $|x\rangle(|0\rangle - |1\rangle)$ اعمال کنیم، سپس به حالت $(-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)$ می رسیم. بنابراین اعمال U_f به $|x\rangle(|0\rangle - |1\rangle)$ 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 در نظر گرفتن شرایط زیر می توان $|\psi_3\rangle$ 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 اندازه‌گیری کیوبیت اول می‌توانیم $f(0) \oplus f(1)$ 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, $1 - 2^n$ to 0 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, 1 or 0 either is balanced, is (x) f else or x , of values all for constant is (x) f either kinds: two half. other the for 0 and x , possible the all of half exactly for 1 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 عمومی تر است که به عنوان الگوریتم دوچ-جوزا شناخته می شود. کاربرد این الگوریتم، که به عنوان مشکل دوچ شناخته می شود، به شرح زیر است: آلیس، در آمستردام، یک عدد x را از بازه $[0, 2^n - 1]$ انتخاب می کند و آن را در یک نامه به باب، در بوستون، می فرستد. باب یک تابع $f(x)$ را محاسبه می کند و نتیجه را که ۰ یا ۱ است، ارسال می کند. 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 های x ممکن برابر با ۱ است و برای نیمی دیگر برابر با ۰ است.

هدف آلیس این است که با اطمینان و بکار بستن کمترین گام های ممکن تعیین کند که باب یک تابع ثابت یا متعادل را انتخاب کرده است. او چگونه می تواند به سرعت موفق شود؟ در حالت کلاسیک، آلیس ممکن است فقط یک مقدار x را در هر نامه به باب ارسال کند. بدترین حالت، الی باید حداقل $1 + \frac{2^n}{2}$ بار از باب سوال کند، زیرا ممکن است قبل از دریافت یک، $\frac{2^n}{2}$ مرتبه پاسخ ۰ 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 $1 + \frac{2^n}{2}$ 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 دشواری های احتمالی اجرای تابع $f(x)$ در نظر گرفته نشده است.

اگر باب و آلیس بتوانند کویت ها را به جای بیت های کلاسیک مبادله کنند، و اگر باب موافقت کند $f(x)$ را با استفاده از تبدیل یک به 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 کویتی را برای ذخیره پرس و جو خود آماده می کند و یک رجیستر کویت 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 می دهد و با انجام یک اندازه گیری مناسب، تعیین می کند که آیا f ثابت یا متعادل است.

گام های خاص الگوریتم در شکل ۲۰.۱ نشان داده شده است. بیایید با دنبال کردن این مدار، به بررسی حالات ایجاد شده بپردازیم. حالت ورودی $|0\rangle^{\otimes n} |1\rangle = |0\rangle^{\otimes n} |0\rangle$ ؛ شبیه حالت معادله (۴۱.۱) است، اما در اینجا رجیستر پرس و جو وضعیت n کویت را توصیف می کند که همه در حالت $|0\rangle$ آماده شده اند. پس از اعمال تبدیل هادامارد روی رجیستر پرس و جو و روی رجیستر پاسخ، می توان نوشت:

$$[2\sqrt{\frac{1}{n}} - \frac{1}{n} \sum_{x \in \{0,1\}^n} |x\rangle\langle x| \sqrt{2n}] = \frac{1}{n}$$

reg- answer the and values: all of superposition a now is register query The
is f function the Next, $|x\rangle$ and $|y\rangle$ of superposition weighted evenly an in is ister
now Alice (۴۸.۱) giving $(x) \otimes f(y) \otimes |x\rangle$: U_f 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
 $|x\rangle = x$ cases the checking By $|x\rangle$. state a on transform Hadamard the of effect
 $|z\rangle/\sqrt{2}$. $(-1)^{xz} \sum_z = H|x\rangle$ qubit single a for that see we separately $|x\rangle = x$ and
equa- useful very the in succinctly more summarized be can This (۴۹.۱) Thus
Using z modulo ۲ and x of product inner bitwise the is $z \cdot x$ where tion (۱.۵۰)
observes now Alice $|x\rangle \otimes f(y) \otimes |x\rangle$ (۱.۵۱) evaluate now can we (۴۸.۱) and equation this
 $x(-1)^f \sum_z$ is $|x\rangle \otimes f(y) \otimes |x\rangle$ state the for amplitude the that Note register. query the
 $(x)/2n$.

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

در مرحله بعد، تابع f توسط باب و به شکل $U_f : |x\rangle \otimes |y\rangle \otimes |x\rangle \rightarrow |x\rangle \otimes f(y) \otimes |x\rangle$ ارزیابی می‌شود، که
(۴۸.۱) را می‌دهد.

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

برای تعیین نتیجه تبدیل هادامارد، بهترست ابتدا اثر تبدیل هادامارد را روی یک حالت $|x\rangle$ محاسبه
کنیم. با بررسی موارد $|x\rangle = 0$ و $|x\rangle = 1$ به‌صورت جداگانه می‌بینیم که برای یک کویت واحد $H|x\rangle =$
 $\sum_z (-1)^{xz} |z\rangle/\sqrt{2}$ می‌باشد. بنابراین (۴۹.۱)

این را می‌توان به‌طور خلاصه در معادله بسیار مفید زیر خلاصه کرد:

$$(۵۰.۱)$$

جایی که $z \cdot x$ product inner bitwise x و z است، به modulo ۲.

با استفاده از این معادله و (۴۸.۱) اکنون می‌توانیم $|x\rangle \otimes f(y) \otimes |x\rangle$ را ارزیابی کنیم:

^۸ یعنی احتمال رخ دادن صفر و یک یکسان است.

آلیس اکنون رجیستر پرس و جو را مشاهده می کند. توجه داشته باشید که دامنه برای حالت $1 \leq n \leq 10^5$ است

discern to – balanced f and constant f – cases possible two the at look Let's
or \neg is $\frac{1}{\sqrt{2^n}}$ for amplitude the constant is f where case the In happens. what
length unit of is $\frac{1}{\sqrt{2^n}}$ Because takes. (x) f value constant the on depending, \neg –
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 s 's yield
amplitude an leaving cancel. $\frac{1}{\sqrt{2^n}}$ for amplitude the to contributions negative
one least at on \neg than other result a yield must measurement a and zero. of
the then \neg 's 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

از آنجایی که $3 \leq \ell \leq 5$ طول واحد است، نتیجه می‌گیریم که تمام دامنه‌های دیگر باید صفر باشند، و یک مشاهده ۰ را برای همه کوبت‌ها در رجیستر پرس و جو به همراه خواهد داشت.

به طور خلاصه، اگر α_i همه α_i 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 (\) Inputs: Deutsch–Jozsa Algorithm:
 \bullet $\mathbb{F}_2^n(x)$ f and $\mathbb{F}_2^n(x)$ f for $(x) \in \mathbb{F}_2^n$ f $\mathbb{F}_2^n(x)$ f $\mathbb{F}_2^n(x)$ f transformation
 $(x) \in \mathbb{F}_2^n$ f else or x of values all for constant either is $(x) \in \mathbb{F}_2^n$ f that promised is It . \mathbb{F}_2^n
for \bullet and x possible the all of half exactly for \mathbb{F}_2^n to equal is that balanced. is
evalu- One Runtime: constant. is f if only and if \bullet Outputs: half. other the
 \mathbb{F}_2^n . \mathbb{F}_2^n state initialize \mathbb{F}_2^n \mathbb{F}_2^n \mathbb{F}_2^n . \mathbb{F}_2^n Procedure: succeeds. Always . Uf of ation

Hadamard using superposition create $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$. ۱. ۲. ۳. gates. ۴. Uf using f function calculate $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle$. ۵. transform Hadamard perform $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{x \cdot z + f(x)} |x\rangle$. 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 Deutsch-Jozsa ورودی‌ها: (۱) یک جعبه سیاه Uf که تبدیل زیر را انجام می‌دهد $|x\rangle \rightarrow (-1)^{f(x)} |x\rangle$ ، برای $x = 0, \dots, 2^n - 1$ و $f(x) \in \{0, 1\}$. قول داده شده است که f (x) برای همه مقادیر x ثابت است یا f (x) متعادل است، یعنی برای دقیقاً نیمی از همه‌های x 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 می‌شود. روش:

initialize کنید $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$ حالت را با استفاده از دروازه‌های Hadamard $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle$ تابع f را با استفاده از Uf محاسبه کنید $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{x \cdot z + f(x)} |x\rangle$ 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 - ارزیابی تابع f در مقایسه با نیاز کلاسیک برای $1 + 2n/2$ 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 الگوریتم‌های 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 deterministic که ما در نظر گرفته ایم. علیرغم این ظرافت ها، الگوریتم Deutsch-Jozsa حاوی بذره های الگوریتم های کوانتومی بیشتر و چشمگیرتر است، و درک اصول پشت آن روشنگر است. عملکرد آن.

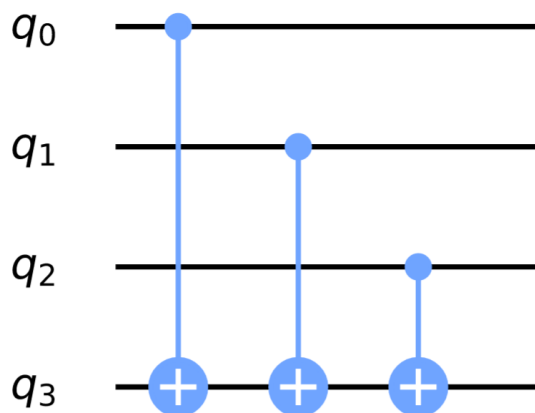
۵.۳ ساخت یک اوراکل کوانتومی

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

برای یک تابع ثابت، ساده است:

اگر $f(x) = 0$ ، گیت را به کیوبیت در ثبات ۲ اعمال کنید. اگر $f(x) = 1$ ، گیت را به کیوبیت در ثبات ۲ اعمال کنید.

برای عملکرد متعادل، مدارهای مختلفی وجود دارد که می توانیم ایجاد کنیم. یکی از راه هایی که می توانیم 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. مثلاً:



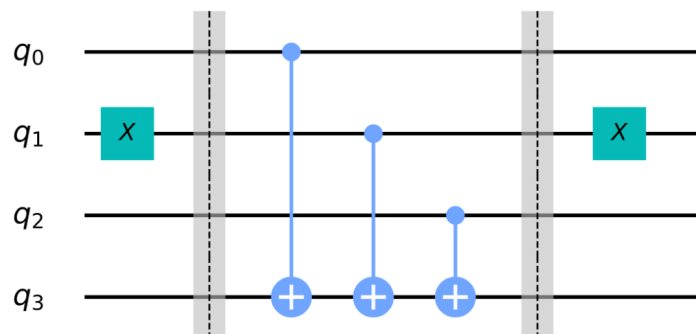
شکل ۵.۳:

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

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

جدول ۱.۳: This is a simple table.

را تغییر دهیم و در عین حال تعادل آنها را با قرار دادن کنترل‌های 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
۰۰۰	۰۰۱
۰۱۱	۰۱۰
۱۰۱	۱۰۰
۱۱۰	۱۱۱

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:

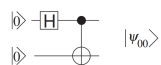
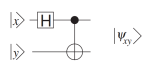
$$|\psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

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 هدامارد و cNOT یک هستند، چهار حالت درهم‌تنیده $|\psi_{xy}\rangle$ نیز یک مجموعه متعامد هستند، که به نام پایه Bell نامگذاری شده‌اند. می‌توان رابطه‌ی بالا را یک حالت کلی تعمیم داد:

(1)
bشکل ۱.۴: $y = x$ 

(b)

(1)
bشکل ۲.۴: $y = 3 \sin x$

شکل ۳.۴: (a) circuit A that creates the entangled state $|\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\rangle$ from the unentangled computational-basis states $|0\rangle$ and $|1\rangle$. (b) circuit A that creates the entangled state $|\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\rangle$ from the unentangled computational-basis states $|x\rangle$ and $|y\rangle$.

$$|\psi_{xy}\rangle = C10H1X_1^x X_0^y |00\rangle$$

در نظر داشته باشید که حالات بل قابل تبدیل به یکدیگرند؛ با کمک رابطه‌ی تعمیم یافته می‌توان از هر حالت بل به حالت $|00\rangle$ رسید. توضیحات درباره‌ی تبدیلات بنویس این روابط به شکل‌های متعدد قابل بیان است که از حوصله‌ی بحث خارج است.

entanglement ۲.۴

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 غیرقابل توضیح 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 کویت 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 کویت در حالت درهم‌تنیده زیر به اشتراک می‌گذارند:

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (3.2)$$

=====

بیانات چپیتی آلیس می‌تواند با استفاده از این جفت کویت‌های درهم‌تنیده، دو بیت کلاسیک را به باب منتقل کند. او این کار را با اعمال یک تبدیل واحد به کویت 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 کویت خود اعمال می‌کند.

این تبدیل واحد باعث می‌شود که کویت آلیس و کویت باب در یکی از چهار حالت بل اورتوگونال قرار گیرند. اگر آلیس کویت خود را در حالت $|00\rangle$ قرار دهد، کویت 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 کویت 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 کویت 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 کویت در اختیار دارند. توجه داشته باشید که \otimes یک حالت ثابت است؛ نیازی نیست که آلیس برای آماده‌سازی این حالت،

^۱Quantum 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 رشته بیت:

• "00" را ارسال کند \Leftarrow هیچ کاری روی کوبیت خود انجام ندهد.

• "01" را ارسال کند \Leftarrow تبدیل دگرگونی فاز^۲ را روی کوبیت خود اثر می‌دهد.

• "10" را ارسال کند \Leftarrow گیت کوانتومی NOT، X را به کوبیت خود اعمال می‌کند.

• "11" را ارسال کند \Leftarrow تبدیل iY را به کوبیت خود اعمال می‌کند.

چهار حالت حاصل به راحتی قابل مشاهده هستند:

$$\begin{aligned} & 00 : |00\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ & 01 : |01\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ & 10 : |10\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\ & 11 : |11\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \end{aligned}$$

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 کویت 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 کویت خود اعمال می‌کند که بسته به بیت‌هایی که می‌خواهد به باب ارسال کند متفاوت است. آلیس کویت خود را به باب می‌فرستد. باب کویت را اندازه‌گیری می‌کند و دو بیت کلاسیکی که آلیس به او ارسال کرده است را دریافت می‌کند. اگر آلیس یک عمل واحد بر روی کویت 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 کویت 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 در صورتی 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.

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

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 $|\phi\rangle$ 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 $|\phi\rangle$ 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 , ($|\phi\rangle_b |\phi\rangle_a + |\phi\rangle_b (|\phi\rangle_a \sqrt{1/2})$) 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 $|\phi\rangle$ state the in Qbit first + $|\phi\rangle_b (|\phi\rangle_a \sqrt{1/2})$ state ۳-Qbit the produces This target. the as pair a applies she Next (۲۲.۶) . ($|\phi\rangle_b |\phi\rangle_a + |\phi\rangle_b (|\phi\rangle_a \sqrt{1/2})$) + ($|\phi\rangle_b |\phi\rangle_a$) α state the Qbits three all giving Qbit, first her to H transformation Hadamard

$$\begin{aligned} & \frac{1}{\sqrt{2}} (|1\rangle_a - |0\rangle_a) \frac{1}{\sqrt{2}} (|1\rangle_b + |0\rangle_b) = \frac{1}{2} (|1\rangle_a |1\rangle_b + |1\rangle_a |0\rangle_b - |0\rangle_a |1\rangle_b - |0\rangle_a |0\rangle_b) \\ & = \frac{1}{2} (|1\rangle_a |1\rangle_b + |1\rangle_a |0\rangle_b - |0\rangle_a |1\rangle_b - |0\rangle_a |0\rangle_b) \end{aligned}$$

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 $|0\rangle$ state the acquire indeed will Qbit Bob’s , . . is result the if But .($|0\rangle$ to reduced be then would state (whose Qbit first Alice’s by Qbit Bob’s of state the then $|1\rangle$ or , . . , $|1\rangle$ is measurement Alice’s of result of each In (۲۴.۶) . $|0\rangle$, $|1\rangle$ or $|0\rangle$, $|1\rangle$ becomes of state the stores re- that transformation unitary a is there cases three these (which Z apply can we case first the In $|0\rangle$. state original Alice’s to Qbit Bob’s (which X case, second the in ,($|0\rangle$ of sign the changes but alone $|0\rangle$ leaves I T A T R O P E L T E ۵ . ۶ ZX. case, third the in and ,($|0\rangle$ and $|1\rangle$ 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 (. . 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 $|0\rangle$ and state whose pair. entangled standard a of aid the with Yet, . $|1\rangle = |0\rangle + |\alpha\rangle$ that described Qbit a with Bob provide to able is Alice $|0\rangle$, 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 $|x\rangle$. and α in encoded be can that information than $|x\rangle$, state the assigned now Qbit, his manipulating from $|x\rangle$ 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 $|x\rangle$. 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, $-(21.6)$ in analysis the of any through going without diagram, circuit classical of $|x\rangle = |x\rangle$ state the exchanges that circuit a shows (a) 5.6 Figure $.(24.6)$. \cdot or $\cdot = x$ whether of regardless Cbit, Bob's of $|x\rangle$ 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 $|x\rangle = |x\rangle + \alpha|x\rangle = |x\rangle$ superpositions, with $.(a) 5.6$ 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 $.(a) 5.6$ Figure (which Qbits entangled of pair shared their produce to necessary interaction $|x\rangle$). state the in Qbit her acquired even has Alice before well place take can

oracle a determine to how