

# فهرست مطالب

۵	۱ آشنایی با مفاهیم اولیه
۵	۱.۱ کیوبیت
۵	۱.۱.۱ کیوبیت واحد
۸	۲.۱.۱ کیوبیت‌های چندتایی
۹	۲.۱ اندازه‌گیری در فضای هیلبرت
۹	۱.۲.۱ vector bloch
۱۱	۳.۱ گیت‌های کوانتومی
۱۱	۱.۳.۱ انواع گیت کوانتومی
۱۸	۲.۳.۱ gate Swap
۱۹	۴.۱ مدارهای کوانتومی
۲۲	۱.۴.۱ نحوه‌ی نمایش مدارهای کوانتومی
۲۳	۲ برنامه‌نویسی کوانتومی
۲۳	۱.۲ تفاوت کامپیوتر کلاسیک و کوانتومی
۲۴	۲.۲ simulation vs comp
۲۵	۱.۲.۲ تفاوت کامپیوترهای کوانتومی و شبیه‌سازهای کلاسیک
۲۷	۳.۲ Qiskit and computer Quantum IBM
۲۹	۳ الگوریتم‌های کوانتومی
۲۹	۱.۳ موازی سازی کوانتومی
۳۳	۱.۱.۳ مدل محاسباتی استاندارد
۳۳	۲.۳ مدل کوثری

۳۴	معرفی و پیاده سازی الگوریتم دوچ	۳.۳
۳۴	مسئله‌ی دوچ	۱.۳.۳
۳۵	الگوریتم دوچ	۲.۳.۳
۳۸	الگوریتم دوچ - جوزا	۴.۳
۴۳	ساخت یک اوراکل کوانتومی	۵.۳
۴۵	شبیه‌سازی پدیده‌های کوانتومی	۴
۴۵	states Bell	۱.۴
۴۷	entanglement	۲.۴
۴۹	رمزگذاری متراکم کوانتومی	۳.۴
۵۲	دوربری	۴.۴

## مقدمه

در عصر حاضر بواسطه‌ی رشد و توسعه‌ی نظریه‌ی اطلاعات کوانتومی و سرمایه‌گذاری‌های 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<sup>۱</sup>، معادل یک واحد اطلاعات کوانتومی می‌باشد. این مفهوم معادل مفهوم کلاسیک بیت<sup>۲</sup> 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 از یکی از خصوصیات 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»<sup>۳</sup> 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.

---

<sup>۱</sup> Qubit

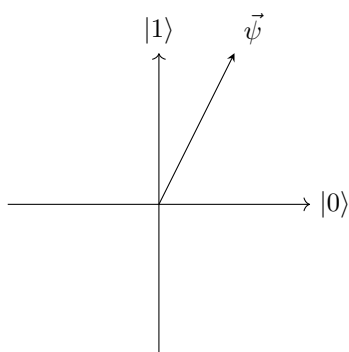
<sup>۲</sup> Binary Bit

<sup>۳</sup> Quantum Superposition

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

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

کت‌های  $|0\rangle$  و  $|1\rangle$  بیانگر پایه‌های فضای محاسباتی<sup>۴</sup> هستند؛ و مقادیر  $\alpha^2$  و  $\beta^2$  بیانگر احتمال وقوع هر یک از این حالات، در صورت مشاهده، می‌باشند. نمایش بردار  $\psi$  به شکل زیر است:



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

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

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.

---

<sup>۴</sup>Computational Basis Vectors

در بیشتر مدل های انتزاعی ما از جهان، یک ارتباط مستقیم بین عناصر انتزاع و دنیای واقعی وجود دارد، درست همانطور که طرح های یک معمار برای یک ساختمان با ساختمان نهایی مطابقت دارد. فقدان این ارتباط مستقیم در مکانیک کوانتوم باعث می شود که درک رفتار سیستم های کوانتومی دشوار باشد؛ با این حال، یک ارتباط غیرمستقیم وجود دارد، زیرا می توان حالت های کیوبیت را دستکاری و تبدیل کرد به وضعیتی هایی که منجر به نتایج اندازه گیری می شود. نتایج حاصل از اندازه گیری 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 غیرایده آل، ممکن است حالت های واسطه ای مانند قرار گرفتن آن روی لبه وجود داشته باشد، اما در حالت ایده آل می توان آنها را نادیده گرفت.

در مقابل، یک کیوبیت می تواند در یک طیف پیوسته از حالت ها بین  $|0\rangle$  و  $|1\rangle$  وجود داشته باشد - تا زمانی که مشاهده شود. بار دیگر تاکید می کنیم که وقتی یک کیوبیت اندازه گیری می شود، فقط یکی از ازمقادیر «۰» یا «۱» را به عنوان نتیجه اندازه گیری می دهد. به عنوان مثال، یک کیوبیت می تواند در حالت  $|1\rangle + |0\rangle$  باشد، که به این معنی است که با احتمال  $50/50$  می تواند به عنوان ۰ یا ۱ اندازه گیری 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 می شود. این حالت، زمانی که اندازه گیری شود، نتیجه ۰ را ۵۰ درصد از زمان و نتیجه ۱ را ۵۰ درصد از زمان می دهد. این حالت را می توان به عنوان یک ترکیب خطی از دو حالت پایه  $|0\rangle$  و  $|1\rangle$  در نظر گرفت.

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

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

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

## ۲.۱.۱ کیوبیت‌های چندتایی

Hilbert space is a big place.

– Carlton Caves

فرض کنید دو کیوبیت داریم. اگر این دو بیت کلاسیک بودند، چهار حالت ممکن وجود داشت: ۰۰، ۰۱، ۱۰ و ۱۱. به همین ترتیب، یک سیستم دو کیوبیتی دارای چهار حالت محاسباتی است که با  $|00\rangle, |01\rangle, |10\rangle, |11\rangle$  نشان داده می‌شود. یک جفت کیوبیت همچنین می‌تواند در برهمه‌ی 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  $a, b, c, d$  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 می‌دهد و کیوبیت‌ها به طور مساوی احتمال اندازه‌گیری در هر یک از چهار حالت محاسباتی را دارند. به عنوان مثال، بردار حالت:

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

یک سیستم دو کیوبیتی را نشان می‌دهد که در یک برهمه‌ی مساوی از حالت‌های ۰۰ و ۱۱ است. این بدان معناست که کیوبیت‌ها به طور مساوی احتمال اندازه‌گیری در حالت ۰۰ یا ۱۱ را دارند. بردار حالت یک سیستم دو کیوبیتی را می‌توان برای محاسبه احتمال اندازه‌گیری کیوبیت‌ها در هر یک از چهار حالت محاسباتی استفاده کرد. به عنوان مثال، احتمال اندازه‌گیری کیوبیت‌ها در حالت ۰۰ با فرمول زیر داده می‌شود:

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

احتمال اندازه‌گیری کیوبیت‌ها در هر حالت دیگر را می‌توان به روشی مشابه محاسبه کرد. نتیجه اندازه‌گیری  $x (= 00, 01, 10, 11)$  با احتمال  $|a_x|^2$  رخ می‌دهد، با حالت کیوبیت‌ها پس از اندازه‌گیری  $|x\rangle$ . این بدان معناست که اگر ما یک سیستم دو کیوبیتی را در حالت  $|\Psi\rangle = |00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$  داشته باشیم، و اگر ما اولین کیوبیت را اندازه‌گیری کنیم، احتمال اینکه ۰ را اندازه‌گیری کنیم برابر  $|a|^2 + |b|^2$  خواهد بود. در این حالت، حالت کیوبیت‌ها پس از اندازه‌گیری  $|0\rangle$  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 اندازه‌گیری با عامل  $\sqrt{|00|^2 + |01|^2}$  نرمال می‌شود 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 اندازه‌گیری به گونه‌ای تغییر می‌کند که احتمالات آن جمع شده و برابر ۱ شود.

## ۲.۱ اندازه‌گیری در فضای هیلبرت

### ۱.۲.۱ vector bloch

ما تاکنون اندازه‌گیری 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 می‌گذارد، با احتمالات  $|\alpha|^2$  و  $|\beta|^2$ . در حقیقت، مکانیک کوانتوم به اندازه کافی انعطاف پذیری در کلاس اندازه‌گیری هایی که می‌توان انجام داد، اگرچه مطمئناً به اندازه کافی نیست که  $\alpha$  و  $\beta$  را از یک اندازه‌گیری واحد بازبایی 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 می‌توان 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 می‌شوند. اندازه‌گیری در پایه + یا پایه - یک کیوبیت را در حالت  $|+\rangle$  یا  $|-\rangle$  قرار می‌دهد.

اندازه‌گیری در پایه های دیگر به غیر از پایه محاسباتی یک ابزار قدرتمند در محاسبات کوانتومی است. این امکان را می‌دهد تا ما در حالت های کوانتومی که در پایگاه محاسباتی قابل اندازه‌گیری نیستند، اندازه‌گیری کنیم. این امکان را می‌دهد 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 گونه‌ای که گویی آنها حالت های پایه محاسباتی هستند، در نظر بگیریم و با توجه به این پایه جدید اندازه‌گیری کنیم. طبیعی است که

اندازه گیری با توجه به پایه  $|+\rangle$ ،  $|-\rangle$  منجر به نتیجه “+” با احتمال  $\frac{|\alpha+\beta|^2}{2}$  و نتیجه “-” با احتمال  $\frac{|\alpha-\beta|^2}{2}$  می شود.

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

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

با توجه به بیان احتمالاتی مفهوم کیوبیت و نرمال بودن مقادیر احتمالات و متعامد بودن پایه ها، 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.

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 توسعه 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 نظیر نتایج آزمایش اشترن-گرلاخ<sup>۵</sup> را می دهد.

### ۳.۱ گیت‌های کوانتومی

گیت‌های کوانتومی<sup>۶</sup> 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 درهم‌نهی 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. 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<sup>۷</sup> است. با اعمال اثر این گیت روی یک کیوبیت، آن کیوبیت به یک حالت درهم نهی کوانتومی گذار می‌کند. به عبارت دیگر هر یک از زیرحالات این حالت درهم‌نهی، 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 دسته کت 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<sup>۶</sup>  
Hadamard gate<sup>۷</sup>

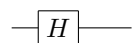
$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

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

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 بی خارج کند.

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 NOT

گیت کوانتومی  $U_{NOT}$  یک عملگر یکه و بازگشت پذیر است.

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

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

## نمایش ماتریسی گیت NOT

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

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

از آنجایی که یک حالت کیوبیت در فضای هیلبرت دو بعدی تعریف شده است. ابعاد ماتریس باید  $2 \times 2$  باشد. از این رو می‌توان نوشت:

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

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

### مدار NOT و خصوصیات آن

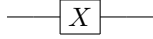
با اعمال گیت  $U_{NOT}$  به حالت  $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$  خواهیم داشت:

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

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

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

نمایش یک گیت NOT به صورت زیر است:



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

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

### گیت CNOT

گیت کوانتومی CNOT<sup>۸</sup>، 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»<sup>۹</sup> دارای مقدار  $|1\rangle$  باشد، باعث تغییر وضعیت «کیوبیت هدف»<sup>۱۰</sup> می‌شود.

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

<sup>۸</sup>gate controlled-X or gate controlled-NOT  
<sup>۹</sup>Qubit Controlled  
<sup>۱۰</sup>Qubit Target

برگردانده می‌شود.

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

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

$|ab\rangle$  چیست؟ این یک بردار در فضای  $\mathbb{C}^4$  و  $a$  و  $b$  دارای مقدار ۰ یا ۱ هستند.  $|ab\rangle$  می‌تواند هر یک از حالت‌های پایه (یعنی  $|11\rangle, |10\rangle, |01\rangle, |00\rangle$ ) باشد.

این معادله به ما می‌گوید؛ که پس از اعمال گیت CNOT به یکی از پایه‌ها، آن حالت به حالت پایه دیگری تبدیل خواهد شد. که این حالت برابر  $|a \ a \oplus b\rangle$  می‌باشد. به‌طوری‌که:

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

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

$$0 \oplus 0 = 0$$

$$0 \oplus 1 = 1$$

$$1 \oplus 0 = 1$$

$$1 \oplus 1 = 0$$

$$U_{CNOT}|00\rangle = |0, 0 \oplus 0\rangle = |0, 0\rangle = |00\rangle$$

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

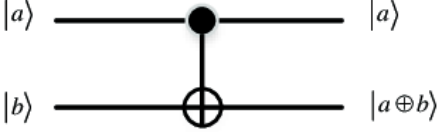
$$U_{CNOT}|10\rangle = |1, 1 \oplus 0\rangle = |1, 1\rangle = |11\rangle$$

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

خلاصه‌ای از عملکرد این عملگر به شرح زیر است:

$ A\rangle$	$ B\rangle$		$ A\rangle$	$ B \oplus A\rangle$
$ \text{control}\rangle$	$ \text{target}\rangle$	Effect CNOT Gate	$ \text{control}\rangle$	$ \text{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:

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

این فرآیند به صورت معکوس نیز قابل رخ دادن است:



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

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

### گیت تغییر فاز

گیت تغییر فاز که به آن گیت P یا گیت فاز نیز می‌گویند، یک کیوبیت است. دروازه‌ای که فاز نسبی را بین دو بردار پایه جابجا می‌کند. به عنوان زیر تعریف شده است:

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

که در آن  $i^{\frac{\pi}{2}}$  فاز و  $i^{\frac{\pi}{2}}$  فاکتور فاز است. زمانی که گیت شیف فاز باشد اعمال بر بردار پایه  $|0\rangle$ ، هیچ کاری انجام نمی‌دهد. اما زمانی که آن را به بردار پایه  $|1\rangle$ ، یک فاز اضافی به آن اضافه می‌کند. اضافه کردن یک فاز اضافی به معنای که بردار در  $i^{\frac{\pi}{2}}$  ضرب شود. چرا ما فقط فاز اضافی را اعمال می‌کنیم 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 می‌کند

### نمایش ماتریسی گیت تغییر فاز

۷.۱۶ شما می‌توانید آن را به راحتی بررسی کنید که معادله (۷.۱۶) معادله را برآورده می‌کند. (۶.۱۶).  
مثلاً ۸.۱۶

### گیت تغییر فاز در مدار و خصوصیات آن

۹.۱۶ در بردار اصلی،  $\alpha$  و  $i^{\frac{\pi}{2}}$  که به طور کلی اعداد مختلط هستند، می‌توانند باشند به عنوان حاصل ضرب ضریب فاز و بزرگی آنها نشان داده می‌شود. به عنوان مثال  $e = i^{\frac{\pi}{2}}$  و  $e = i^{\frac{\pi}{2}}$  که در آن

۱ و ۲ به ترتیب فازهای  $\alpha$  و  $\beta$  هستند. بنابراین، اختلاف فاز آنها  $\beta - \alpha$  است. با توجه به گیت شیف فاز، فاز از  $\alpha$  بدون تغییر است اما فاز  $\beta$  به  $\beta + \alpha$  تغییر می‌کند. بنابراین، خویشاوندان آنها فاز با  $\alpha$  تغییر می‌کند. این همچنین توضیح می‌دهد که چرا تغییر فاز فقط در مورد اعمال می‌شود حالت پایه دوم معنادار باشد. اگر برای هر دو اعمال شود، تغییری ایجاد نمی‌شود در اختلاف فاز  $\beta$  پارامتری از گیت تغییر فاز است. هنگامی که  $\pi = \pi$ ، دروازه تبدیل می‌شود  $(\pi e^{i\beta} - 1) = (1 - 0)$  زیرا  $1 - \pi \sin i + \pi \cos = i\pi e^{i\beta}$ . و این فقط ماتریس  $Z$ ، یکی از ماتریس‌های مهم پائولی. و به آن Z-gate نیز می‌گویند. گیت تغییر فاز فاز نسبی  $\beta$  و  $\alpha$  را با  $\beta$  تغییر می‌دهد. و به این ترتیب گیت Z فاز نسبی را با  $\pi$  تغییر می‌دهد. این باعث می‌شود Z-gate بسیار خاص باشد و بچرخد در مبنای  $|0\rangle / |1\rangle$ ، دروازه Z به عنوان یک دروازه NOT (دروازه X عمل می‌کند. این ممکن است صدای گیج‌کننده بیاید به یاد بیاوریم که معنای دروازه NOT چیست. وقتی NOT گیت به حالت پایه اعمال می‌شود، حالت پایه به حالت پایه دیگر تبدیل می‌شود. 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 می‌کند. به عنوان مثال، در فضای تشکیل شده توسط بردارهای پایه  $|0\rangle$  و  $|1\rangle$ ، دروازه NOT  $|0\rangle$  به  $|1\rangle$  و بالعکس تبدیل می‌کند. از این رو، انتظار می‌رود یک دروازه NOT در فضای  $|0\rangle / |1\rangle$  به  $|1\rangle / |0\rangle$  و بالعکس تبدیل شود. اجازه دهید بررسی کنیم که آیا دروازه Z در مبنای  $|0\rangle / |1\rangle$  به عنوان یک گیت NOT رفتار می‌کند. fig ۱۰.۱۶ ۲.۱۶

می‌بینیم که گیت Z  $|0\rangle / |1\rangle$  را به  $|1\rangle / |0\rangle$  تبدیل می‌کند. در اینجا من از ماتریس استفاده نمی‌کنم نمایندگی. من از درک خود از Z-gate استفاده می‌کنم که تغییر فاز را اضافه می‌کند از  $\pi$  به ضریب حالت پایه دوم (یعنی  $|1\rangle$ ). بنابراین، من فقط ضرب می‌کنم  $-1$  تا  $|1\rangle$ . 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 الگوریتم‌ها 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 شیف فاز و گیت Z را نشان می‌دهد

### ۲.۳.۱ gate Swap

یک گیت SWAP همانطور که از نامش پیداست، اعداد را در حالت‌های پایه یک ۲ کیوبیتی مبادله می‌کند. ثبت نام. اگر فقط حالت‌های 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 ایالت‌ها به ترتیب. آنها می‌توانند ۰ یا ۱ باشند. ساده‌ترین راه برای به دست آوردن عمق بیشتر درک فقط برای وصل کردن همه حالت‌های

پایه است و ما دریافت می کنیم ۲.۱۶

بنابراین، تنها  $|0\rangle$  و  $|1\rangle$  تحت SWAP (به یکدیگر) تغییر می کنند. عمل. برای  $|00\rangle$  و  $|11\rangle$ ، آنها بدون تغییر هستند زیرا  $|0\rangle$  و  $|0\rangle$  تعویض می شوند. یا  $|1\rangle$  و  $|1\rangle$  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،  $C4$  ماتریس (اپراتور) باید  $4 \times 4$  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 برقرار است.

### گیت swap در مدار و خصوصیات آن

به طور کلی، برای یک بردار ۲ کیوبیتی،  $\alpha = |0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|$  داریم

fig ۱۶.۱ ۵.۱۶

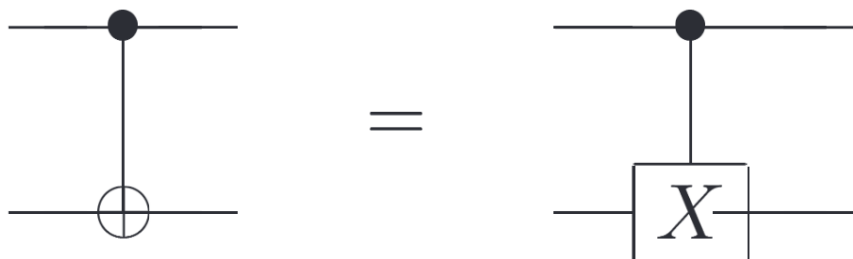
همانطور که انتظار می رود، ضرایب حالت های پایه دوم و سوم با هم مبادله می شوند. شکل ۱.۱۶ مدار یک عملیات SWAP را نشان می دهد. توجه داشته باشید که دوباره کیوبیت پایین MSB است. همانطور که تاکید کردیم، یک مدار کوانتومی یک جریان را نشان می دهد زمان نه یک جریان سیگنال بنابراین، برخلاف عملیات مبادله کلاسیک، اجرای 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<sup>۱۱</sup>، 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 مفهوم 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.

<sup>۱۱</sup>circuit quantum

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 شور برای رمزگشایی اعداد صحیح و الگوریتم گروور برای جستجوی پایگاه داده های بدون ترتیب استفاده شوند.



شکل ۲.۱: نمایش های 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  $\frac{1}{\sqrt{2}}|0\rangle + \alpha|1\rangle = \frac{1}{\sqrt{2}}|0\rangle$  state qubit single a with  $\cdot$  is which wire), double-line a as it drawing by qubit a from tinguished .  $\frac{1}{\sqrt{2}}$  probability with ۱ or ,  $\alpha$  probability

book chuang L fig ۱۰.۱

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.

### شباهت ها و تفاوت های مدارهای کلاسیک و کوانتومی

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

#### شباهت ها

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

- هر دو مدار می توانند برای پیاده سازی الگوریتم ها استفاده شوند.

### تفاوت ها

- مدارهای کوانتومی از کیوبیت ها، که معادل کوانتومی مفهوم بیت هستند، به عنوان واحد پایه داده خود استفاده می کنند.
- مدارهای کلاسیک از بیت ها، که بیت های کلاسیک هستند، به عنوان واحد پایه داده خود استفاده می کنند.
- مدارهای کوانتومی از دروازه های کوانتومی، که عملیات قابل برگشت هستند، به عنوان عملیات پایه خود استفاده می کنند.
- مدارهای کلاسیک از دروازه های منطقی، که عملیات برگشت ناپذیر هستند، به عنوان عملیات پایه خود استفاده می کنند.
- مدارهای کوانتومی می توانند خواص مکانیک کوانتوم را، مانند 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 table has 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.

**کیوبیت** کیوبیت 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 کیوبیت می تواند هم ۰ و هم ۱ باشد، که یک ویژگی به نام superposition کوانتومی است. کیوبیت ها همچنین می توانند به هم متصل شوند، که به این معنی است که حالت یک کیوبیت به حالت کیوبیت دیگر وابسته است.

**دروازه** دروازه ها عملیاتی هستند که روی کیوبیت ها اعمال می شوند. آنها می توانند برای ایجاد superpositions، انجام چرخش ها و درهم تنیدگی کیوبیت 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 کیوبیت 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 کیوبیت به یک مقدار قطعی، ۰ یا ۱ استفاده می شود. راه اندازی ها برای تنظیم حالت یک کیوبیت به یک مقدار خاص، ۰ یا ۱ استفاده می شوند.

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

### ۱.۴.۱ 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 کیوبیت ها را نشان می دهد. دروازه ها توسط جعبه ها نشان داده می شوند و خطوط بین جعبه ها نشان دهنده ارتباطات بین کیوبیت ها است.

## 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 (کیوبیت‌ها) برای ذخیره اطلاعات استفاده می‌کنند، در حالی که کامپیوترهای کلاسیک از بیت‌ها استفاده می‌کنند. کیوبیت‌ها می‌توانند در حالت برهم‌نهی دو حالت، ۰ و ۱، به‌طور همزمان باشند، در حالی که بیت‌ها فقط می‌توانند در یک حالت به‌طور همزمان باشند. این تفاوت در

نحوه ذخیره اطلاعات امکان محاسباتی را برای کامپیوترهای کوانتومی فراهم می‌کند که برای کامپیوترهای کلاسیک غیرممکن است.

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

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

برخی از مثال‌های خاص از نحوه استفاده از کامپیوترهای کوانتومی:

\* رمزنگاری: کامپیوترهای کوانتومی می‌توانند برای رمزگشایی روش‌های رمزنگاری فعلی استفاده شوند، که تأثیر عمده‌ای بر امنیت آنلاین خواهد داشت. \* 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. <sup>[۹]</sup> : درکودانس در محاسبات کوانتومی مهم است زیرا اصلی‌ترین منبع خطا در این سیستم‌ها است. کیوبیت‌ها، واحد های 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 کیوبیت‌ها 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: کیوبیت‌ها در دماهای بالاتر مستعد دکوراسیون هستند. این به این دلیل است که هرچه دما بالاتر باشد، کیوبیت‌ها انرژی بیشتری دارند و بیشتر احتمال دارد با محیط خود تعامل داشته باشند. \* \*\*تکان‌ها: کیوبیت‌ها همچنین می‌توانند توسط ارتعاشات دکور شوند. این به این دلیل است که ارتعاشات می‌توانند باعث حرکت کیوبیت‌ها شوند، که می‌تواند حالت‌های کوانتومی آنها را مختل کند. \* \*\*تابش الکترومغناطیسی: کیوبیت‌ها می‌توانند توسط تابش الکترومغناطیسی، مانند نور و امواج رادیویی، دکور شوند. این به این دلیل است که تابش الکترومغناطیسی می‌تواند با الکترون‌های کیوبیت‌ها 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:

\* \*\* کیوبیت ها را تا دماهای بسیار پایین سرد کنید: \*\* این می تواند انرژی کیوبیت 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<sup>۱</sup>، 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

---

<sup>۱</sup>parallelism Quantum

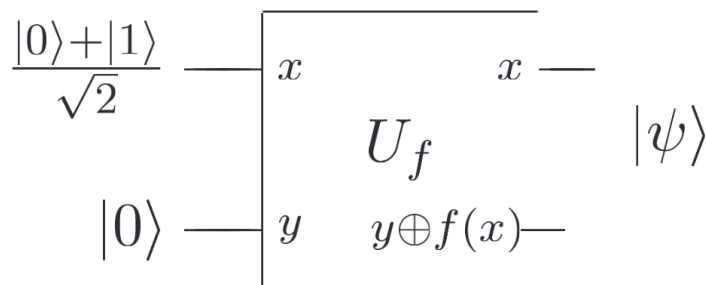
$|f(x) \oplus x, y\rangle$  تبدیل کرد که در آن  $\oplus$  بیانگر جمع مدوله با پایه ۲ می‌باشد.

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.<sup>۳</sup>

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 برهمه‌نی قرار دارد. این حالت برهمه‌نی را می‌توان با اعمال گیت هادامارد بر حالت کوانتومی  $|0\rangle$

<sup>۲</sup>Modulo a is ۲ by division a of remainder the returns that operation mathematical a is ۲. For ex- ۵ by divided ۲ because ۱ is ۲ mod ۵ ample. ۱ of remainder a and ۲ of quotient a has ۲ by divided ۵. The "mod" symbol often is used to indicate modulo addition. So, the expression "۵ mod ۳" would be evaluated as follows: ۵ divided by ۳ has a quotient of ۱ and a remainder of ۲. This is because  $۵ = ۳ \times ۱ + ۲$ . So,  $۵ \bmod ۳ = ۲$ .

Modulo a is ۲ by division a of remainder the returns that operation mathematical a is ۲. For ex- ۵ by divided ۲ because ۱ is ۲ mod ۵ ample. ۱ of remainder a and ۲ of quotient a has ۲ by divided ۵. The "mod" symbol often is used to indicate modulo addition. So, the expression "۵ mod ۳" would be evaluated as follows: ۵ divided by ۳ has a quotient of ۱ and a remainder of ۲. This is because  $۵ = ۳ \times ۱ + ۲$ . So,  $۵ \bmod ۳ = ۲$ .

Here are some other examples of modulo ۲:

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

<sup>۳</sup>اثبات این مطلب از حوصله‌ی بحث خارج است.

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

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

این یک حالت استثنایی است! جملات مختلف کسر بالا حاوی اطلاعاتی در مورد  $f(0)$  و  $f(1)$  می‌باشند؛ 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 برهمه‌نهی 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:

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

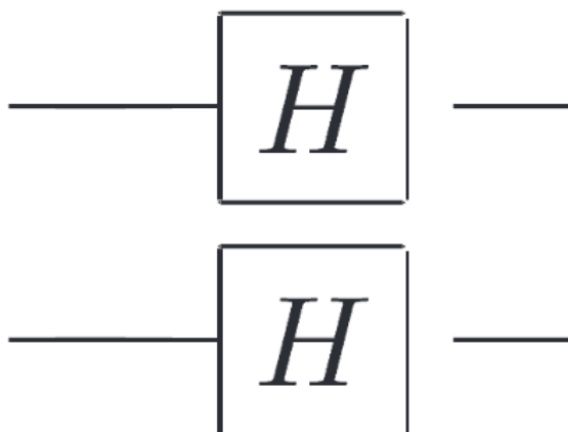
از نماد  $H \otimes 2$  به عنوان نشانه‌ی عملکرد موازی دو گیت هادامارد استفاده می‌کنیم؛ از علامت  $\otimes$  به عنوان تانسور یاد می‌کنیم. به طور کلی نتایج اعمال موازی گیت هادامارد روی  $n$  کیوبیت روی حالت کوانتومی برابرست با:

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

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:

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

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

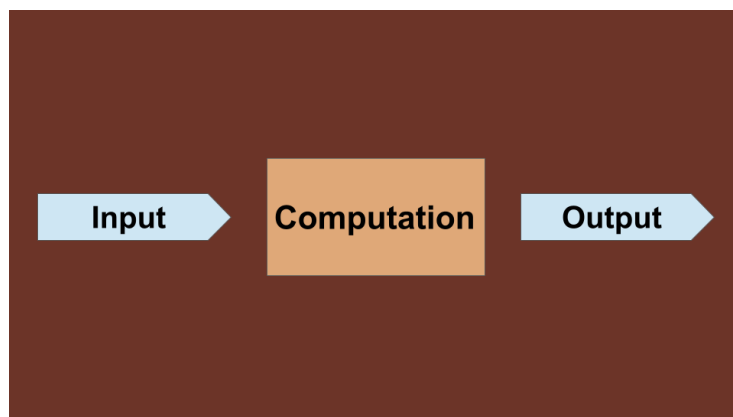
به طور کلی موازی‌سازی کوانتومی امکان ارزیابی همزمان همه مقادیر ممکن تابع  $f$  را فراهم می‌کند، حتی اگر ظاهراً فقط یک بار  $f$  را ارزیابی کرده باشیم. با این حال، این موازی‌سازی بلافاصله مفید نیست. در مثال تک کیوبیتی ما، اندازه‌گیری حالت فقط  $|0, f(0)\rangle$  یا  $|1, f(1)\rangle$  را می‌دهد! به طور 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.

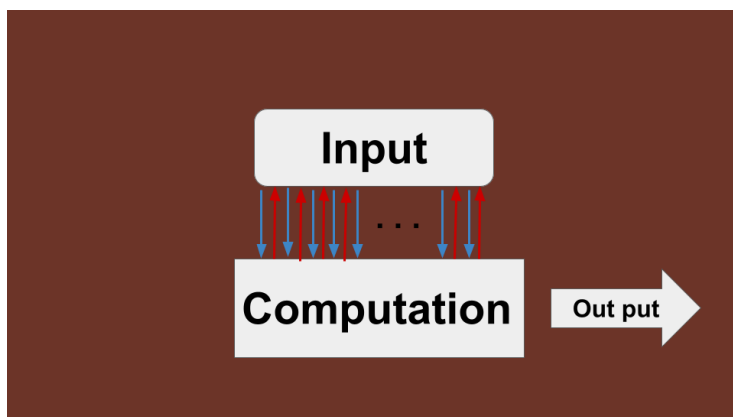
در تصویر بالا یک نمود ساده از کامپیوترهای امروزی ارائه شده است. در دنیای واقعی مقدار ورودی می‌تواند از هر منبعی تأمین شده باشد. با این وجود هدف ما بررسی منابع تولید ورودی نیست؛ بلکه هدف بررسی مقادیر ورودی (به صورت ایزوله) می‌باشد. می‌توان در نظر گرفت که ورودی داده شده و خروجی نهایی، هر دو در قالب یک 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<sup>۴</sup> 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:

<sup>۴</sup>Deutsch David

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

هدف بررسی ثابت بودن یا متعادل<sup>۵</sup> 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:

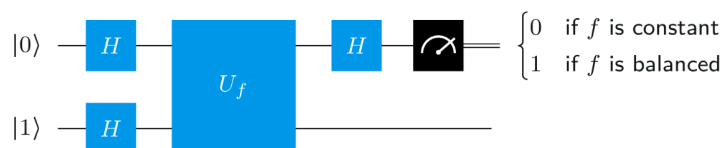
در شکل بالا توابع  $f_1$ ،  $f_4$  توابع ثابت و توابع  $f_2$  و  $f_3$  توابع متعادل هستند.

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:

<sup>۵</sup>balance. or Constante

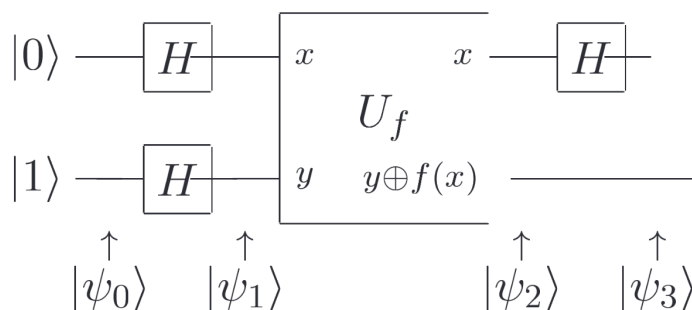
یک تغییر ساده در مدار شکل ۳.۱ نشان می‌دهد که چگونه مدارهای کوانتومی می‌توانند با پیاده سازی الگوریتم Deutsch از مدارهای کلاسیک پیشی بگیرند.<sup>۶</sup> الگوریتم Deutsch ترکیبی از موازی سازی کوانتومی با خاصیتی از مکانیک کوانتوم به نام تداخل<sup>۷</sup> است. مشابه قبل، ابتدا از گیت هادامارد برای آماده سازی اولین کیوبیت به عنوان superposition  $(|0\rangle + |1\rangle)/\sqrt{2}$  استفاده کنیم، اما اکنون کیوبیت دوم  $y$  را با اعمال یک گیت هادامارد به حالت  $|1\rangle$  به عنوان superposition  $(|0\rangle - |1\rangle)/\sqrt{2}$  آماده کنیم. به شکل زیر دقت کنید:

---

<sup>۶</sup> ما در واقع یک نسخه ساده شده و بهبود یافته از الگوریتم اصلی را ارائه می‌دهیم.

<sup>۷</sup> 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  
qubit second The  $|1\rangle$  and  $|0\rangle$  of superposition equal the is which  $(|0\rangle + |1\rangle)$  state the in prepared is qubit  
phases. opposite with  $|1\rangle$  and  $|0\rangle$  states the of superposition a is which  $(|0\rangle - |1\rangle)$  state the in prepared is  
and gate Hadamard a includes that circuit quantum a through passed then are qubits two The  
CNOT the and  $|1\rangle + |0\rangle$  superposition the into  $(|0\rangle + |1\rangle)$  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  $(|0\rangle - |1\rangle)$  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  $|1\rangle$  be to measured is qubit first the If  
constructively will states two the between interference the so  $|1\rangle$  state the to parallel is  $(|0\rangle - |1\rangle)$  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 کیوبیت 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  $n$  کیوبیتی را برای ذخیره پرس و جو خود آماده می کند و یک رجیستر کیوبیت 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 برهمه ای 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 برهمه ای 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  $|0\rangle^{\otimes n} |1\rangle = |0\rangle^{\otimes n} |1\rangle$ ؛ شبیه حالت معادله (۴۱.۱) است، اما در اینجا رجیستر پرس و جو وضعیت  $n$  کیوبیت 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:

$$[2\sqrt{\frac{1}{n}} - \frac{1}{n} \sum_{x \in \mathcal{X}} \langle x | \psi \rangle \langle \psi | x \rangle] = \frac{1}{n}$$

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

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  $0$  و  $1$  محسوب می‌شود.<sup>۸</sup>

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

آلیس اکنون یک مجموعه کیوبیت دارد که در آن نتیجه اعمال تابع باب در دامنه کیوبیت 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  $x = 0$  و  $x = 1$  به‌صورت جداگانه می‌بینیم که برای یک کیوبیت واحد  $H|x\rangle$   
 $z = \sum (-1)^{xz} |z\rangle/\sqrt{2}$  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  $2$ .

با استفاده از این معادله و (۴۸.۱) اکنون می‌توانیم  $\frac{1}{\sqrt{2}}$  را ارزیابی کنیم:

<sup>۸</sup> یعنی احتمال رخ دادن صفر و یک یکسان است.





Hadamard using superposition create  $\frac{1}{\sqrt{2n+1}} \sum_{x=0}^{2n} |x\rangle$ . ۱. ۲. ۳. gates. ۴. Uf using f function calculate  $\frac{1}{\sqrt{2n+1}} \sum_{x=0}^{2n} (-1)^{f(x)} |x\rangle$ . ۵. transform Hadamard perform  $\frac{1}{\sqrt{2n+1}} \sum_{x=0}^{2n} (-1)^{x \cdot z + f(x)} |x\rangle$ . 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.  $1 + 2n/2$  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  $x = 0, \dots, 2n-1$  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  $\frac{1}{\sqrt{2n+1}} \sum_{x=0}^{2n} |x\rangle$  حالت را با استفاده از دروازه‌های Hadamard  $\frac{1}{\sqrt{2n+1}} \sum_{x=0}^{2n} (-1)^{f(x)} |x\rangle$  تابع f را با استفاده از Uf محاسبه کنید  $\frac{1}{\sqrt{2n+1}} \sum_{x=0}^{2n} (-1)^{x \cdot z + f(x)} |x\rangle$  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 روشنتر است. عملکرد آن.

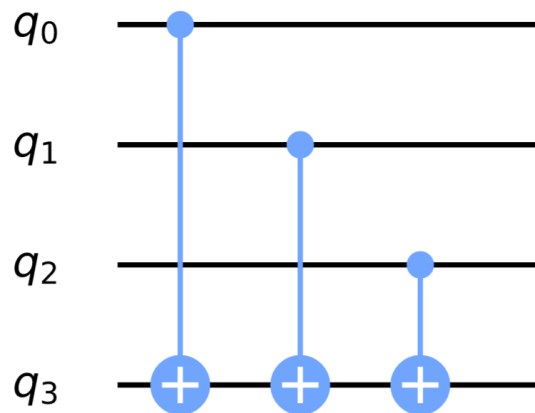
### ۵.۳ ساخت یک اوراکل کوانتومی

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:



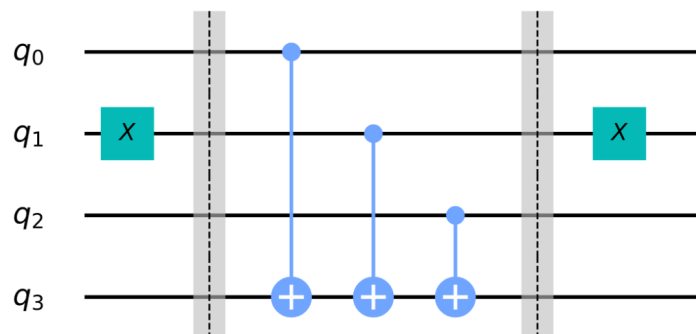
شکل ۵.۳:

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:

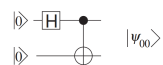
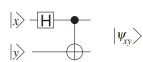
$$|\psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

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:

(a)  
bشکل ۱.۴:  $y = x$ 

(b)

(a)  
bشکل ۲.۴:  $y = 3 \sin x$ 

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

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

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

Physics Quantum in Connection Mysterious The Entanglement: that phenomena baffling most the of one physics. quantum of realm the In is alike philosophers and scientists of imagination the capture to continues of understanding conventional our challenges concept This "entanglement." philosophical and experiments. debates. countless to rise given has and reality inquiries.

can that connection extraordinary the to refers entanglement core. its At them. separating distance the of regardless particles. more or two between exist momentum. spin. as such properties. their entangled. become particles When particle one of state the that way a such in linked become polarization. and space physical the matter no other. the of state the influences instantaneously notions classical defy to seems connection instantaneous This them. between a at action "spooky it dub to Einstein Albert led has and effect and cause of distance."

is entanglement illustrating experiments thought famous most the of One entangled two scenario. this In paradox. (EPR) Einstein-Podolsky-Rosen the to sent and separated are "Bob." and "Alice" as to referred often particles. its particle. one on performed is measurement a When locations. different be to state particle's other the causing determined. instantaneously is state of violation apparent This apart. light-years are they if even well. as known information how of understanding our challenged has limit light's of speed the transmitted. be can

experimen- been has it concept: theoretical a just not is Entanglement most the of One experiments. of variety a through verified and observed tally which test. Bell the is entanglement demonstrating experiments groundbreaking entangled on measurements the When inequalities. Bell of violation the tests can- behavior their that suggests strongly it inequalities. these violate particles quan- of reality the to points instead and physics classical by explained be not entanglement. tum

con- the beyond extend and profound are entanglement of implications The potential the exploring actively are Researchers laboratories. physics of fines quantum and computing quantum like fields in entanglement of applications exist to bits) (quantum qubits enable to ability Entanglement's cryptography. computa- revolutionize to potential the has simultaneously states multiple in considered previously were that solutions to leading cryptography. and tion impossible.

concep- and philosophical with us presents also entanglement However, entan- between connection instantaneous the of nature The challenges. tual It causality. and time, space, of understanding our challenges particles gled human of role the and reality of nature true the about debates sparked has function. wave quantum the collapsing in observation per- and intriguing most the of one as stands entanglement conclusion, In connec- mysterious Its physics. quantum of realm the in phenomena plexing the push to continues and intuitions classical defies particles between tion deeper delve scientists As universe. the of understanding our of boundaries clear it's applications, potential its and entanglement of intricacies the into to generations inspire and captivate to continue will phenomenon this that come.



## ۳.۴ رمزگذاری متراکم کوانتومی

رمزگذاری متراکم کوانتومی<sup>۱</sup> 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 کیوبیت به باب ارسال کند. آیا می‌تواند به هدف خود برسد؟

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

$$| \Phi \rangle = \frac{1}{\sqrt{2}} (| 00 \rangle + | 11 \rangle) \quad (133.2)$$

=====

بیانات جی بیتی آلیس می‌تواند با استفاده از این جفت کیوبیت‌های درهم‌تنیده، دو بیت کلاسیک را به باب منتقل کند. او این کار را با اعمال یک تبدیل واحد به کیوبیت 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 کیوبیت خود اعمال می‌کند.

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

<sup>۱</sup> Quantum super dense coding

توجه داشته باشید که  $\Psi$  یک حالت ثابت است؛ نیازی نیست که آلیس برای آماده‌سازی این حالت، کیوبیتی را به باب ارسال کند. در عوض، ممکن است یک طرف ثالث قبلاً حالت درهم‌تنیده را آماده کند، یکی از کیوبیت‌ها را به آلیس و دیگری را به باب ارسال کند.

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

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

چهار حالت حاصل به راحتی قابل مشاهده هستند:

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

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 کیوبیت خود را به باب بفرستد، و باب هر دو کیوبیت را در اختیار داشته باشد، سپس با انجام اندازه‌گیری در پایه بل، باب می‌تواند تعیین کند که کدام یک از چهار رشته بیت ممکن را آلیس ارسال کرده است.

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

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

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 کیوبیت استفاده کند. پروتکل به شرح زیر است:

آلیس و باب یک جفت کیوبیت درهم‌تنیده را با هم به اشتراک می‌گذارند. آلیس می‌خواهد دو بیت کلاسیک، ۰۰ یا ۰۱ را به باب ارسال کند. آلیس یک عمل واحد بر روی کیوبیت خود اعمال می‌کند که بسته به بیت‌هایی که می‌خواهد به باب ارسال کند متفاوت است. آلیس کیوبیت خود را به باب می‌فرستد. باب کیوبیت را اندازه‌گیری می‌کند و دو بیت کلاسیکی که آلیس به او ارسال کرده است را دریافت می‌کند. اگر آلیس یک عمل واحد بر روی کیوبیت 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 کیوبیت 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 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 , (  $|1\rangle_b |1\rangle_a + |0\rangle_b (|0\rangle_a \sqrt{1/2})$  ) 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 state the in Qbit first +  $|0\rangle_b (|0\rangle_a \sqrt{1/2})$  state ۳-Qbit the produces This target. the as pair a applies she Next (۲۲.۶) . (  $|1\rangle_b |0\rangle_a + |0\rangle_b (|1\rangle_a \sqrt{1/2})$  ) + (  $|1\rangle_b |1\rangle_a \alpha$  state the Qbits three all giving Qbit, first her to H transformation Hadamard

$$\begin{aligned} & \frac{1}{\sqrt{2}} (|0\rangle_a - |1\rangle_a) \frac{1}{\sqrt{2}} (|0\rangle_b + |1\rangle_b) = \frac{1}{2} (|00\rangle - |01\rangle - |10\rangle + |11\rangle) \\ & = \frac{1}{2} (|00\rangle + |11\rangle) - \frac{1}{2} (|01\rangle + |10\rangle) \end{aligned}$$

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  $|\Phi\rangle$  state the acquire indeed will Qbit Bob’s , . . . is result the if But .( $|\Phi\rangle$  to reduced be then would state (whose Qbit first Alice’s by Qbit Bob’s of state the then  $|\Phi\rangle$  or  $|\Phi\rangle$  ,  $|\Phi\rangle$  is measurement Alice’s of result of each In (۲۴.۶) .  $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$  or  $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$  becomes of state the stores re- that transformation unitary a is there cases three these (which Z apply can we case first the In  $|\Phi\rangle$  state original Alice’s to Qbit Bob’s (which X case. second the in  $|\Phi\rangle$  of sign the changes but alone  $|\Phi\rangle$  leaves I T A T R O P E L T E ۵ . ۶ ZX. case. third the in and  $|\Phi\rangle$  and  $|\Phi\rangle$  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  $\alpha$  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  $|\Phi\rangle$  and state whose pair. entangled standard a of aid the with Yet.  $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$  that described Qbit a with Bob provide to able is Alice  $|\Phi\rangle$  and  $\alpha$  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  $|0\rangle$ . and  $\alpha$  in encoded be can that information than  $|0\rangle$ , state the assigned now Qbit, his manipulating from  $|0\rangle$  and  $\alpha$  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  $|0\rangle$ . 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  $|x\rangle = |0\rangle$  state the exchanges that circuit a shows (a)  $5.6$  Figure  $.(24.6)$ .  $\cdot$  or  $\cdot = x$  whether of regardless Cbit, Bob's of  $|0\rangle$  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  $|0\rangle|0\rangle + \alpha|1\rangle|0\rangle = |0\rangle$  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  $|0\rangle$ ). state the in Qbit her acquired even has Alice before well place take can

oracle a determine to how