

# فهرست مطالب

۶	آشنایی با مفاهیم اولیه
۶	کیوبیت
۶	کیوبیت واحد
۱۰	کیوبیت‌های چندتایی
۱۱	اندازه‌گیری در فضای هیلبرت
۱۳	گیت‌های کوانتومی
۱۳	انواع گیت کوانتومی
۲۲	گیت مبادله
۲۵	مدارهای کوانتومی
۲۸	نحوه‌ی نمایش مدارهای کوانتومی
۳۰	برنامه‌نویسی کوانتومی
۳۰	کامپیوترهای کوانتومی در مقابل کامپیوترهای کلاسیک
۳۲	شبیه‌سازی کلاسیک در مقابل کامپیوتر کوانتومی
۳۲	تفاوت کامپیوترهای کوانتومی و شبیه‌سازهای کلاسیک
۳۳	شبیه‌سازی کلاسیک
۳۴	کامپیوتر کوانتومی IBM و زبان برنامه‌نویسی QisKit
۳۴	معرفی QisKit
۳۴	کدنویسی به زبان QisKit

۳۴	قواعد نوشتاری و ساختار داده
۳۵	پیاده‌سازی گیت‌های کوانتومی
۳۶	تصویر سازی
۳۸	<b>الگوریتم‌های کوانتومی</b>
۳۸	موازی سازی کوانتومی
۴۳	مدل محاسباتی استاندارد
۴۳	مدل کوثری
۴۴	معرفی و پیاده‌سازی الگوریتم دوچ
۴۴	مسئله‌ی دوچ
۴۵	الگوریتم دوچ
۴۹	پیاده‌سازی الگوریتم دوچ در کیس کیت
۵۶	<b>شبیه‌سازی پدیده‌های کوانتومی</b>
۵۶	حالات بل
۵۸	درهمتنیدگی
۵۹	پیاده‌سازی درهمتنیدگی در کیس کیت
۶۰	رمزگذاری متراکم کوانتومی
۶۳	پیاده‌سازی رمزگذاری متراکم در کیس کیت
۷۵	دوربری
۷۹	پیاده‌سازی دوربری در کیس کیت

## مقدمه

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



# آشنایی با مفاهیم اولیه

## 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، بهره می‌بریم. کیوبیت یک سیستم کوانتومی با فضای دوبعدی است. برای تعیین این دوبعد می‌توان از یکی از خصوصیات سامانه های کوانتومی استفاده کرد.

## 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

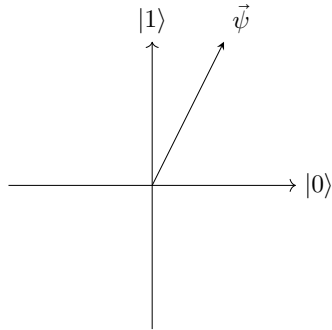
<sup>۲</sup> Binary Bit

<sup>۳</sup> Quantum Superposition

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

$$\begin{cases} |\psi\rangle = \alpha|0\rangle + \beta|1\rangle \\ \alpha^2 + \beta^2 = 1 \end{cases} \quad (۱)$$

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:

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad (۲)$$

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.

---

Computational Basis Vectors<sup>۴</sup>

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 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  $|0\rangle + |1\rangle$  باشد، که به این معنی است که با احتمال  $50/50$  می تواند به عنوان ۰ یا ۱ اندازه گیری شود.

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \quad (۳)$$

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.



## 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:

$$|\Psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \quad (۴)$$

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

به عنوان مثال، بردار حالت:

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

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

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

$$P(|00\rangle) = |a|^2 = \frac{1}{2} \quad (5)$$

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

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

$$|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}} \quad (6)$$

توجه داشته باشید که حالت پس از اندازه گیری با عامل  $\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}$  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.

## اندازه گیری در فضای هیلبرت

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

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

$$\begin{aligned} |+\rangle &\equiv (|0\rangle + |1\rangle)\sqrt{2} \\ |-\rangle &\equiv (|0\rangle - |1\rangle)\sqrt{2} \end{aligned} \quad (۷)$$

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

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle = \frac{(\alpha + \beta)}{2}|+\rangle + \frac{(\alpha - \beta)}{2}|-\rangle \quad (۸)$$

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 گونه ای که گویی آنها حالت های پایه محاسباتی هستند، در نظر بگیریم و با توجه به این پایه جدید اندازه‌گیری کنیم. طبیعی است که اندازه‌گیری با توجه به پایه  $|+\rangle$ ،  $|-\rangle$  منجر به نتیجه ”+” با احتمال  $\frac{|\alpha+\beta|^2}{2}$  و نتیجه ”-” با احتمال  $\frac{|\alpha-\beta|^2}{2}$  می‌شود.

در این بیان،  $|+\rangle$  و  $|-\rangle$  به عنوان ”پایه +” و ”پایه -” شناخته می‌شوند. اندازه‌گیری در پایه + یا پایه - یک کیوبیت را در حالت  $|+\rangle$  یا  $|-\rangle$  قرار می‌دهد.

به طور کلی تر، با توجه به هر دو پایه حالت  $|a\rangle$  و  $|b\rangle$  برای یک کیوبیت، می‌توان 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، می‌توان با توجه به پایه  $|a\rangle$ ،  $|b\rangle$  اندازه‌گیری کرد، که نتیجه a با احتمال  $|\alpha|^2$  و b با احتمال  $|\beta|^2$  قابل رخداد است.

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

اندازه‌گیری در پایه‌های دیگر یک ابزار قدرتمند در محاسبات کوانتومی است. این امکان را می‌دهد تا ما در حالت‌های کوانتومی که در پایگاه محاسباتی قابل اندازه‌گیری نیستند، اندازه‌گیری کنیم. این امکان را می‌دهد تا ما از روش‌های محاسباتی جدیدی استفاده کنیم که در محاسبات کلاسیک غیرممکن است.

دلایل زیادی برای استفاده از این مدل توسعه‌یافته برای اندازه‌گیری‌های 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 می‌دهد.

## 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 برهم‌نهی کوانتومی یا رمزگذاری داده در داخل یک یا چند کیوبیت شد.

## 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 برهم‌نهی کوانتومی گذار می‌کند. به عبارت دیگر هر یک از زیرحالات این حالت برهم‌نهی، با احتمال

Stern-Gerlach<sup>۵</sup>

Quantum Gates<sup>۶</sup>

Hadamard gate<sup>۷</sup>

یکسانی قابل رخ دادن هستند.

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad (۹)$$

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad (۱۰)$$

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

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (۱۱)$$

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad (۱۲)$$

$$H|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad (۱۳)$$

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

برای اعمال این گیت کوانتومی، فقط به یک کیوبیت نیاز داریم. به اصطلاح این گیت، یک گیت تک کیوبیت<sup>۸</sup> می‌باشد.

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

### گیت NOT

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

$$\begin{aligned} U_{NOT}|0\rangle &= |1\rangle \\ U_{NOT}|1\rangle &= |0\rangle \end{aligned} \quad (۱۴)$$

### نمایش ماتریسی گیت NOT

می‌بینید 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  $2 \times 2$

---

<sup>۸</sup> Single-Qubit Quantum gate

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

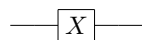
با اعمال گیت  $U_{NOT}$  به حالت  $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$  خواهیم داشت:

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

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 دوکیوبیتی NOT به یک سیستم دو کیوبیتی نظیر

خواهیم داشت:  $|\Psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$

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

## گیت CNOT

گیت کوانتومی CNOT<sup>۹</sup>، به عنوان گیت منطقی نیز یاد می‌شود. این گیت کوانتومی معادل گیت NOT کلاسیک می‌باشد. 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<sup>۱۰</sup>» دارای مقدار  $|1\rangle$  باشد، باعث تغییر وضعیت

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



«کیوبیت هدف<sup>۱۱</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 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.

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

$|ab\rangle$  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  $|a \oplus b\rangle$  می‌باشد. به‌طوری‌که:

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

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:

$$0 \oplus 0 = 0$$

$$0 \oplus 1 = 1$$

$$1 \oplus 0 = 1$$

$$1 \oplus 1 = 0$$

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

---

<sup>۱۱</sup>Qubit Target

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

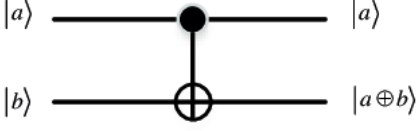
$$U_{CNOT}|10\rangle = |1, 1 \oplus 0\rangle = |1, 1\rangle = |11\rangle$$

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

خلاصه‌ای از عملکرد این عملگر به شرح زیر است:

$ A$	$B$		$ A$	$B \oplus A$
$ \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: نمایش ماتریسی و نمایش گیت کوانتومی CNOT

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

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

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

این فرآیند به صورت معکوس نیز قابل رخ دادن است:

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

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

### گیت تغییر فاز

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

$$U_{PS,\phi}|0\rangle = |0\rangle$$

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

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

### نمایش ماتریسی گیت تغییر فاز

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

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

با استفاده از روابط بالا می‌توان به راحتی اثبات کرد:

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

### گیت تغییر فاز در مدار و خصوصیات آن

در حالت کلی برای سیستم های تک کیوبیتی می‌توان نوشت:

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

در بردار اصلی،  $\alpha$  و  $\beta$  اعداد مختلط می‌باشند؛ به همین دلیل این اعداد را می‌توان به به عنوان یک ضرب فاز معرفی کرد:

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

که در آن  $\theta_1$  و  $\theta_2$  به ترتیب فازهای  $\alpha$  و  $\beta$  هستند.

بنابراین، اختلاف فاز آنها  $\theta_2 - \theta_1$  است. با توجه به رفتار گیت تغییر فاز، تغییر فاز  $\alpha$  صفر می‌باشد؛ اما فاز  $\beta$  به  $\theta_2 + \theta_1$  تغییر می‌کند. بنابراین، خویشاوندان آنها فاز با  $\theta_1$  تغییر می‌کند.

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

$$e^{-i\pi} = \cos \pi - i \sin \pi = -1 \quad \text{زیرا } e^{i\pi} = -1$$

این ماتریس پائولی  $\sigma_z$  می‌باشد؛ که به آن Z-gate نیز می‌گویند. گیت تغییر فاز، فاز نسبی  $|0\rangle$  و  $|1\rangle$  را با  $\pi$  تغییر می‌دهد. و به این ترتیب گیت Z فاز نسبی را با  $\pi$  تغییر می‌دهد.

## گیت مبادله

یک گیت مبادله<sup>۱۲</sup> اعداد را در حالت های پایه یک رجیستر ۲ کیوبیتی جابجا می‌کند. اگر فقط حالت های پایه را در نظر بگیریم، معادل مبادله حالات دو الکترون است. این گیت به صورت زیر تعریف می‌شود:

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

<sup>۱۲</sup> Swap gate

که در آن  $a$  و  $b$  فقط اعداد کیوبیت اول و دوم در پایه هستند.  $a$  و  $b$  می‌توانند مقادیر  $0$  و  $1$  را اتخاذ کنند. بنابراین می‌توان نوشت:

$$U_{SWAP}|00\rangle = |00\rangle$$

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

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

$$U_{SWAP}|11\rangle = |11\rangle$$

بنابراین، تنها  $|01\rangle$  و  $|10\rangle$  تحت مبادله (به یکدیگر) تغییر می‌کنند. اعمال این گیت برای حالات  $|00\rangle$  و  $|11\rangle$ ، بدون اثر است؛ زیرا  $0$  و  $0$  یا  $1$  و  $1$  تعویض می‌شوند؛ که پیامد خاصی در پی ندارد.

### نمایش ماتریسی گیت مبادله

نمایش ماتریسی  $U_{SWAP}$  به شکل زیر است:

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

از آنجایی که این یک گیت ۲ کیوبیتی برای عملیات است یک بردار در فضای چهار بعدی  $\mathbb{C}^4$ ، ماتریس (یا عملگر) باید  $4 \times 4$  باشد. علاوه بر این، فقط حالت پایه دوم و سوم را جابجا می‌کند. بنابراین، تنها ردیف دوم و سوم با ماتریس یک‌ه متفاوت هستند. به طور مثال:

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

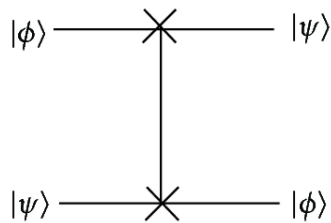
این رابطه بصورت معکوس نیز برقرار است.

### گیت مبادله در مدار و خصوصیات آن

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

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

$$= \alpha|00\rangle + \gamma|01\rangle + \beta|10\rangle + \delta|11\rangle$$



شکل ۲: نمایش گیت کوانتومی مبادله در مدار کوانتومی

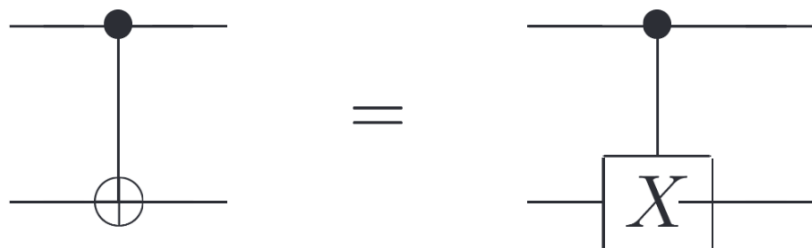
همانطور که انتظار می‌رود، ضرایب حالت‌های پایه دوم و سوم با هم مبادله می‌شوند.

## مدارهای کوانتومی

مدارهای کوانتومی<sup>۱۳</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 مفاهیم 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.



شکل ۳: نمایش های مختلف گیت CNOT در مدار کوانتومی

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

مدارهای کوانتومی مدلی بسیار سودمند برای شبیه سازی فرآیندهای کوانتومی است. این فرآیندها محدود به عملیات های محاسباتی نخواهد شد؛ بلکه در اغلب حوزه ها اعم از ارتباطات، اختلالات کوانتومی<sup>۱۴</sup> و ... بکارخواهدرفت.

<sup>۱۳</sup>circuit quantum

<sup>۱۴</sup>noise quantum





شکل ۴: نمایش‌های مختلف گیت CNOT در مدار کوانتومی

### شباهت‌ها و تفاوت‌های مدارهای کلاسیک و کوانتومی

مدارهای کوانتومی مشابه مدارهای کلاسیک هستند، اما از دروازه‌های کوانتومی به جای دروازه‌های منطقی کلاسیک استفاده می‌کنند. دروازه‌های کوانتومی عملیات قابل برگشت هستند که می‌توانند برای دستکاری حالت کوانتومی یک کیوبیت استفاده شوند.

### شباهت‌ها

- هر دو مدار کوانتومی و کلاسیک از یک دنباله عملیاتی تشکیل شده‌اند که به یک مجموعه داده اعمال می‌شوند.
- هر دو مدار را می‌توان به صورت گرافیکی با نماد مشابهی نشان داد.
- هر دو مدار می‌توانند برای پیاده‌سازی الگوریتم‌ها استفاده شوند.

### تفاوت‌ها

- مدارهای کوانتومی از کیوبیت‌ها، که معادل کوانتومی مفهوم بیت هستند، به عنوان واحد پایه داده خود استفاده می‌کنند.
- مدارهای کلاسیک از بیت‌ها، که بیت‌های کلاسیک هستند، به عنوان واحد پایه داده خود استفاده می‌کنند.
- مدارهای کوانتومی از دروازه‌های 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 برهمه و درهمتیدگی ، 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: شباهت ها و تفاوت های مدارهای کلاسیک و کوانتومی

### 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 برهمه کوانتومی از دو حالت ، ۰ و ۱ باشند. این بدان معنی است که یک کیوبیت می تواند هم ۰ و هم ۱ باشد ، که یک ویژگی به نام برهمه 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 برهمه ، انجام چرخش ها و درهم تنیدگی کیوبیت ها استفاده شوند. انواع مختلفی از دروازه ها وجود دارد ، اما برخی از رایج ترین آنها شامل گیت هادامارد ، گیت CNOT و گیت توفولی است.

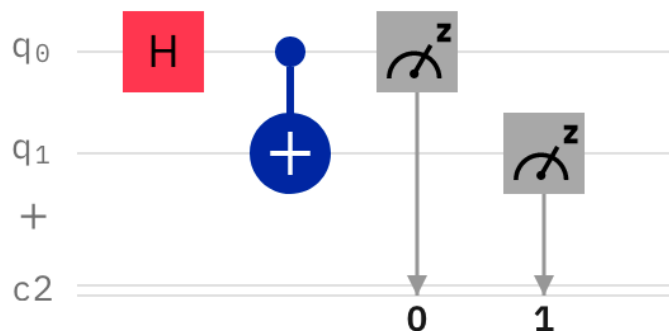
**عملیات** عملیات اقداماتی هستند که روی کیوبیت ها انجام می شوند. آنها می توانند اندازه گیری ها یا سایر اقدامات باشند. اندازه گیری ها برای رمبش حالت کوانتومی یک کیوبیت به یک مقدار قطعی ، ۰ یا ۱ استفاده می شود.

اجزای اساسی یک مدار کوانتومی کیوبیت ها ، دروازه ها و عملیات هستند. این اجزا برای ایجاد الگوریتم

های کوانتومی استفاده می شوند که الگوریتم هایی هستند که فقط می توانند روی یک رایانه کوانتومی اجرا شوند. مدارهای کوانتومی یک ابزار قدرتمند برای محاسبات کوانتومی هستند و پتانسیل انقلابی در بسیاری از زمینه های مختلف ، از جمله رمزنگاری ، شیمی و یادگیری ماشین را دارند.

### 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.



شکل ۵: مدار کوانتومی شبیه سازی شده برای آزمایش درهمتنیدگی



## برنامه‌نویسی کوانتومی

برنامه نویسی کوانتومی فرآیند طراحی و پیاده‌سازی دنباله‌هایی از دستورالعمل‌هایی موسوم مدارهای کوانتومی می‌باشد، با استفاده از گیت‌ها، سوئیچ‌ها و عملگرها برای دستکاری وضعیت کوانتومی یک کیوبیت به پردازش مسائل می‌پردازیم.

مدارهای کوانتومی یک نمایش گرافیکی از الگوریتم‌های کوانتومی هستند، این الگوریتم‌هایی 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 محبوب‌ترین زبان‌های برنامه نویسی کوانتومی عبارتند از Qiskit، Cirq و Quil.

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

### کامپیوترهای کوانتومی در مقابل کامپیوترهای کلاسیک

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

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

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

برخی از مثال‌های خاص از نحوه استفاده از کامپیوترهای کوانتومی:

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

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

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

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

## شبیه‌سازی کلاسیک در مقابل کامپیوتر کوانتومی

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 هر کدام از کامپیوترها می‌پردازیم و در ادامه به اهداف تعریف شده برای کامپیوترهای کوانتومی می‌پردازیم.

### تفاوت کامپیوترهای کوانتومی و شبیه‌سازهای کلاسیک

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

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

هریک از حالات داخل رابطه‌ی بالا به صورت یک ماتریس قابل تعریف هستند. به طور مشابه هریک از 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 هریک 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. همدوسی در محاسبات کوانتومی اصلی ترین منبع خطا در این سیستم‌ها است. کیوبیت‌ها بسیار به محیط خود هستند و می‌توانند به راحتی توسط تعامل با فوتون‌ها، الکترون‌ها و سایر ذرات با آن‌ها دچار ناهمدوسی شوند. این می‌تواند باعث شود که کیوبیت‌ها خواص کوانتومی خود را مانند برهمه‌نی کوانتومی و درهم‌تنیدگی که برای انجام محاسبات کوانتومی ضروری هستند، از دست بدهند.

ناهمدوسی می‌تواند به دلایل مختلفی ایجاد شود:

**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.

**برخورد** 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.

ناهمدوسی یک مانع بزرگ برای توسعه ابررایانه‌های کوانتومی است. برای ساخت یک رایانه کوانتومی عملی، باید راه‌هایی برای کاهش ناهمدوسی پیدا کرد. این یک مشکل بزرگ ولی قابل حل است؛ اما تعدادی از مسیرهای تحقیقاتی امیدوارکننده وجود دارد، مانند:

**سردسازی کیوبیت‌ها** این می‌تواند انرژی کیوبیت‌ها را کاهش دهد و آنها را کمتر مستعد تعامل با محیط خود کند.

**استفاده از مواد با همدوسی بالا** برخی از مواد، مانند ابررساناها، زمان‌های همدوسی بسیار طولانی دارند که آنها را برای استفاده در رایانه‌های کوانتومی بسیار مناسب می‌کند.

**توسعه الگوریتم‌های جایگزین برای تصحیح خطای کوانتومی** الگوریتم‌های تصحیح خطای کوانتومی می‌توانند برای تشخیص و تصحیح خطاهایی که توسط ناهمدوسی ایجاد می‌شوند استفاده شوند.

## شبیه‌سازی کلاسیک

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

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



## کامپیوترکوانتومی IBM و زبان برنامه‌نویسی QisKit

### معرفی QisKit

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

۱. این زبان براساس زبان پایتون و برخی کتابخانه‌های آن ساخته شده است.
۲. جامعه دانشمندان کوانتوم و به‌طور کلی فیزیکدانان از سابق برای انجام شبیه‌سازی‌های خود از زبان پایتون استفاده می‌کنند و پایتون نیز کتابخانه‌های بسیار کارآمدی - نظیر نامپای<sup>۱۵</sup>، پانداس<sup>۱۶</sup>، سایپای<sup>۱۷</sup> و .. - ارائه کرده است.

### کدنویسی به زبان QisKit

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

```
import qiskit
```

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

### قواعد نوشتاری و ساختار داده

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

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

<sup>۱۵</sup>Numpy

<sup>۱۶</sup>Pandas

<sup>۱۷</sup>Scipy

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

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

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

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

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

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

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

## پیاده‌سازی گیت‌های کوانتومی

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

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

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

## تصویر سازی

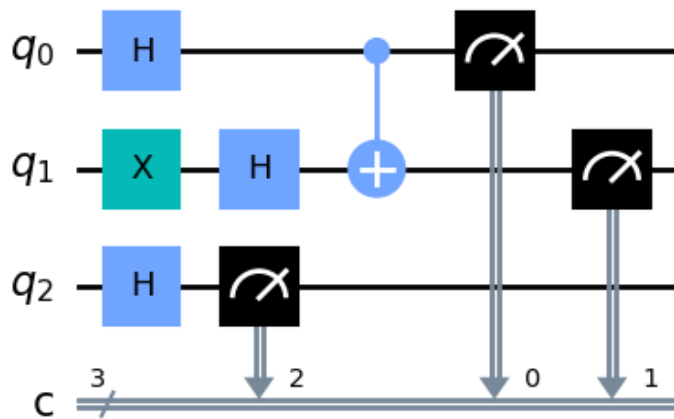
برای تصویر کردن وضعیت مدار کوانتومی می بایست از راه زیر استفاده کرد:

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

# draw circuit
circuit.draw()

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

در نهایت خروجی مشابه خروجی های زیر را می توان از این زبان برنامه نویسی دریافت کرد:



شکل ۶: نمونه ای از خروجی Qiskit



# 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.

## موازی سازی کوانتومی

موازی سازی کوانتومی<sup>۱۸</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

---

<sup>۱۸</sup> parallelism Quantum

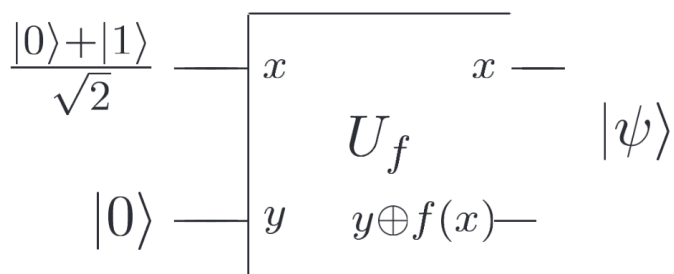
$|x, y\rangle$  شروع می‌شود. با یک توالی مناسب از گیت‌های منطقی می‌توان این حالت را به  $|f(x) \oplus x, y\rangle$  تبدیل کرد که در آن  $\oplus$  بیانگر جمع مدوله با پایه ۲ می‌باشد.

۱۹

هریک از دسته‌های کیوبیت، **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>۲۰</sup>

اگر  $y = 0$  آنگاه مقدار دومین کیوبیت بعد از اعمال تابع  $U_f$  برابر با مقدار  $f(x)$  خواهد بود.



شکل ۷: 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.

<sup>۱۹</sup>example. For  $\mathbb{Z}$  by division a of remainder the returns that operation mathematical a is  $\mathbb{Z} \text{ Modulo}$

$\mathbb{Z}$  of remainder a and  $\mathbb{Z}$  of quotient a has  $\mathbb{Z}$  by divided  $\mathbb{Z}$  because,  $\mathbb{Z}$  is  $\mathbb{Z} \bmod \mathbb{Z}$

be would "3 5" expression the So.  $\mathbb{Z}$  modulo addition indicate to used often is "5" symbol The

follows: as evaluated

remainder a and 4 of quotient a has  $\mathbb{Z}$  by divided 8 because is This  $\cdot = \mathbb{Z} \bmod 8 = \mathbb{Z} \bmod (3 + 5) = 3 \bmod 5$

$\cdot$  of

com- cryptography, including mathematics, of areas different many in operation useful a is  $\mathbb{Z} \text{ Modulo}$

whether checking when example, for life, everyday in used also is It theory, number and science, puter

odd, or even is number a

$\mathbb{Z}$  modulo of examples other some are Here

$1 = \mathbb{Z} \bmod 5$   $0 = \mathbb{Z} \bmod 4$   $1 = \mathbb{Z} \bmod 3$   $0 = \mathbb{Z} \bmod 2$   $1 = \mathbb{Z} \bmod 1$

<sup>۲۰</sup>اثبات این مطلب از حوصله‌ی بحث خارج است.

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  $|0\rangle$  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 نوبعی 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:

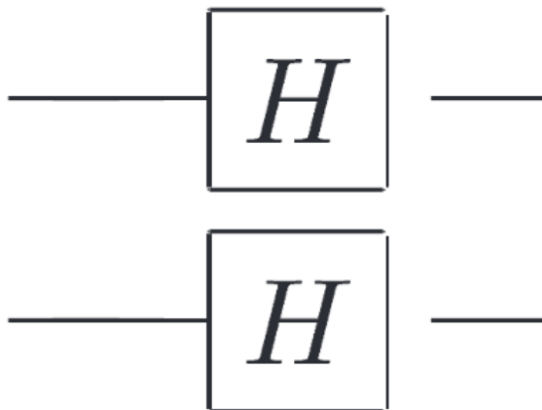
$$\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{\sqrt{2}}$$

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:

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

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 برهم‌نهی از  $2n$  حالت تولید می‌کند.



شکل ۸: اعمال تبدیل هادامارد  $H \otimes n$  روی دو کیوبیت

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،

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

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

در نهایت حالت زیر تولید می‌شود:

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

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

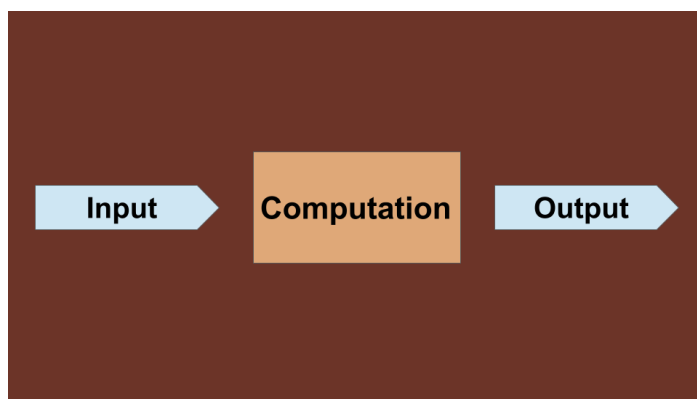
در مثال تک کیوبیتی ما، اندازه‌گیری حالت فقط  $|0, f(0)\rangle$  یا  $|1, f(1)\rangle$  را می‌دهد! به طور مشابه، در



حالت کلی، اندازه گیری حالت  $\sum_x |x, f(x)\rangle$  فقط  $f(x)$  را برای یک مقدار  $x$  خاص می دهد. البته یک کامپیوتر کلاسیک می تواند این کار را به راحتی انجام دهد! محاسبات کوانتومی برای مفید بودن به چیزی بیش از موازی سازی کوانتومی نیاز دارد؛ به توانایی استخراج اطلاعات مربوط به بیش از یک مقدار  $f(x)$  از حالت های درهم نهی مانند  $\sum_x |x, f(x)\rangle$  نیاز دارد. در بخش های بعدی به مثال های خواهیم پرداخت که این مسائل را حل کند.

## مدل محاسباتی استاندارد

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



شکل ۹: یک واحد محاسباتی که مقادیری را به عنوان ورودی گرفته، پردازش کرده و سپس مقدار/مقادیر خروجی را ارائه کرده است.

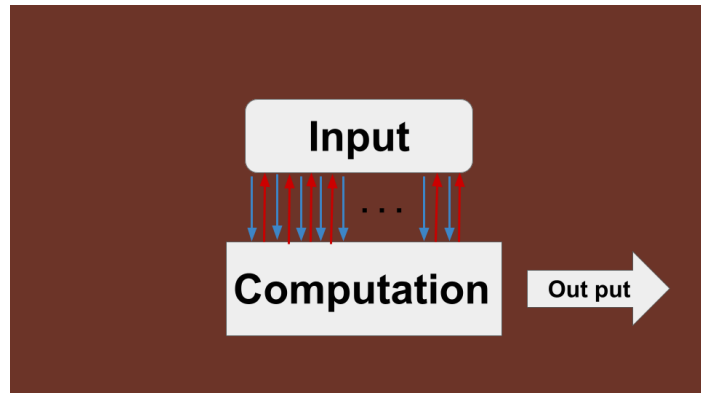
در تصویر بالا یک نمود ساده از کامپیوترهای امروزی ارائه شده است. در دنیای واقعی مقدار ورودی می‌تواند از هر منبعی تأمین شده باشد. با این وجود هدف ما بررسی منابع تولید ورودی نیست؛ بلکه هدف بررسی مقادیر ورودی (به صورت ایزوله) می‌باشد. می‌توان در نظر گرفت که ورودی داده شده و خروجی نهایی، هر دو در قالب یک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

## 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 تولید ورودی دریافت کند. در گاهی از مواقع به سیستم ورودی، Oracle یا جعبه‌ی سیاه می‌گویند. تابع Oracle یا جعبه‌ی سیاه یک سیستم است که ما به عنوان ناظر به سازوکار داخلی آن و تمامی اطلاعات



شکل ۱۰: 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.

آن دسترسی نداریم و فقط می‌توانیم مقادیر مجاز را به آن داده و مقادیر خروجی را 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.

## معرفی و پیاده سازی الگوریتم دوچ

### مسئله دوچ

الگوریتم دوچ<sup>۲۱</sup> اولین و ساده‌ترین الگوریتم کوانتومی است. این الگوریتم برای اولین بار در سال ۱۹۸۵ در مقاله‌ای مطرح شد؛ که توسط دیوید دوچ<sup>۲۲</sup> نوشته شده بود. این الگوریتم نقطه‌ی شروعی برای اثبات برتری

<sup>۲۱</sup>algorithm Deutsch

<sup>۲۲</sup>David Deutsch

کامپیوترهای کوانتومی نسبت به کامپیوترهای کلاسیک است.

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

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

هدف بررسی ثابت بودن یا متعادل<sup>۲۳</sup> بودن تابع  $f$  است. به‌طور کلی، در ساده‌ترین حالت، می‌توان 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 ۱۱: تمام حالات ممکن برای یک تابع ثابت و یک تابع متعادل

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

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

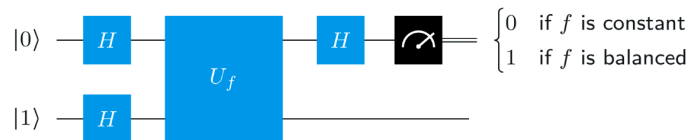
در الگوریتم‌های کلاسیک برای حل این مسئله، حداقل دو حالت باید بررسی شود.

## الگوریتم دوچ

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

مدار زیر نشان می‌دهد که چگونه مدارهای کوانتومی می‌توانند با پیاده‌سازی الگوریتم دوچ از مدارهای

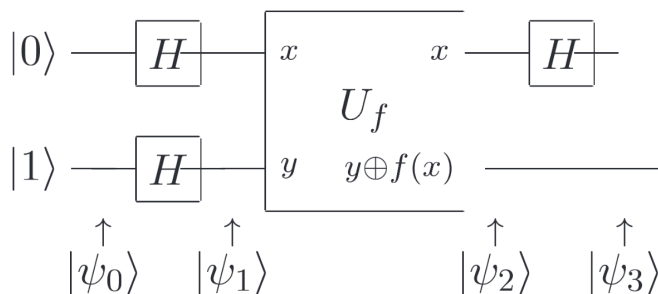
<sup>۲۳</sup> Constante or balance.



شکل ۱۲:

کلاسیک پیشی بگیرند<sup>۲۴</sup>. الگوریتم دوچ ترکیبی از موازی سازی کوانتومی با خاصیتی از مکانیک کوانتوم به نام تداخل<sup>۲۵</sup> است. مشابه قبل، ابتدا از گیت هادامارد برای آماده سازی اولین کیوبیت به عنوان برهمتهی  $\frac{(|0\rangle+|1\rangle)}{\sqrt{2}}$  استفاده کنیم، اما اکنون کیوبیت دوم  $y$  را با اعمال یک گیت هادامارد به حالت  $|1\rangle$  به عنوان برهمتهی  $\frac{(|0\rangle-|1\rangle)}{\sqrt{2}}$  آماده کنیم. به شکل زیر دقت کنید:

<sup>۲۴</sup> ما در واقع یک نسخه ساده شده و بهبود یافته از الگوریتم اصلی را ارائه می دهیم.  
<sup>۲۵</sup> how interference is used in deutsch algorithm : Interference to algorithm deutsch the in used is  
 always that function a is function constant A functions. balanced and constant between distinguish  
 half for • returns that function a is function balanced A input. its of regardless value. same the returns  
 half. other the for ۱ and inputs its of  
 qubit first The states. of superposition a in qubits two preparing first by works algorithm Deutsch The  
 prepared is qubit second The .  $|1\rangle$  and  $|0\rangle$  of superposition equal the is which,  $\frac{(|0\rangle+|1\rangle)}{\sqrt{2}}$  state the in prepared is  
 phases. opposite with  $|1\rangle$  and  $|0\rangle$  states the of superposition a is which  $\frac{(|0\rangle-|1\rangle)}{\sqrt{2}}$  state the in  
 CNOT a and gate Hadamard a includes that circuit quantum a through passed then are qubits two The  
 the copies gate CNOT the and,  $|1\rangle + |0\rangle$  superposition the into  $\frac{(|0\rangle+|1\rangle)}{\sqrt{2}}$  transforms gate Hadamard The gate.  
 qubit. second the to qubit first the of state  
 mea- is qubit first the If measured. are qubits two the executed. been has circuit quantum the After  
 state the to orthogonal is  $\frac{(|0\rangle-|1\rangle)}{\sqrt{2}}$  state the because is This constant. is f function the then,  $|0\rangle$  be to sured  
 interfere. destructively will states two the between interference the so,  $|0\rangle$   
 is  $\frac{(|0\rangle-|1\rangle)}{\sqrt{2}}$  state the because is This balanced. is f function the then,  $|1\rangle$  be to measured is qubit first the If  
 interfere. constructively will states two the between interference the so,  $|1\rangle$  state the to parallel  
 prob- a solve to used be can interference quantum how of example simple a is algorithm Deutsch The  
 between distinguish can algorithm Deutsch the case. this In classically. solve to difficult is that lem  
 ex- an take to need would computer classical a while step. single a in functions balanced and constant  
 steps. of number ponential



شکل ۱۳: پیاده‌سازی مدار کوانتومی الگوریتم دوچ

حالت ورودی:

$$|\psi_0\rangle = |01\rangle \quad (15)$$

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

$$|\psi_1\rangle = \left[ \frac{|0\rangle + |1\rangle}{\sqrt{2}} \right] \left[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \quad (16)$$

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

$$|\psi_2\rangle = \begin{cases} \pm \left[ \frac{|0\rangle+|1\rangle}{\sqrt{2}} \right] \left[ \frac{|0\rangle-|1\rangle}{\sqrt{2}} \right] & \text{if } f(0) = f(1) \\ \pm \left[ \frac{|0\rangle-|1\rangle}{\sqrt{2}} \right] \left[ \frac{|0\rangle-|1\rangle}{\sqrt{2}} \right] & \text{if } f(0) \neq f(1) \end{cases} \quad (۱۷)$$

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

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle \left[ \frac{|0\rangle-|1\rangle}{\sqrt{2}} \right] & \text{if } f(0) = f(1) \\ \pm|1\rangle \left[ \frac{|0\rangle-|1\rangle}{\sqrt{2}} \right] & \text{if } f(0) \neq f(1) \end{cases} \quad (۱۸)$$

با در نظر گرفتن شرایط زیر می توان  $|\psi_3\rangle$  را به شکل زیر بازنویسی کرد:

$$\begin{cases} f(0) = f(1) \Rightarrow & f(0) \oplus f(1) = 0 \\ f(0) \neq f(1) \Rightarrow & f(0) \oplus f(1) = 1 \end{cases} \quad (۱۹)$$

از این رو:

$$|\psi_3\rangle = \pm |f(0) \oplus f(1)\rangle \left[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \quad (۲۰)$$

بنابراین با اندازه گیری کیوبیت اول می توانیم  $f(0) \oplus f(1)$  را تعیین کنیم. واقعاً جالب است! مدار کوانتومی به ما توانایی تعیین یک ویژگی کلی 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 امکان پذیر است، یک دستگاه کلاسیک حداقل به دو ارزیابی نیاز دارد. این مثال تفاوت بین موازی سازی کوانتومی و الگوریتم های تصادفی کلاسیک

را برجسته می‌کند. به سادگی، ممکن است تصور شود که حالت  $|1\rangle|f(1)\rangle + |0\rangle|f(0)\rangle$  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.

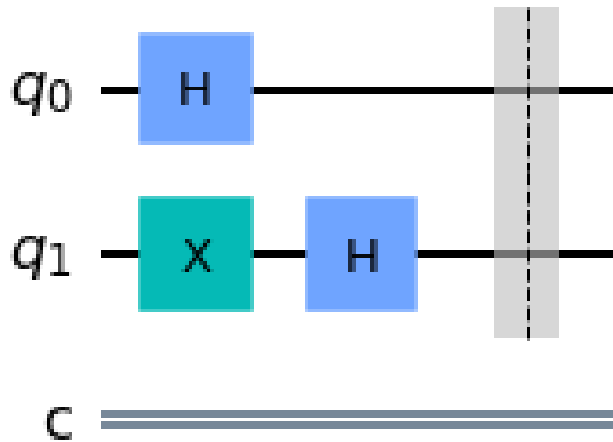
### پیاده‌سازی الگوریتم دوچ در کیس کیت

```
from qiskit import *
from qiskit.tools.visualization import plot_histogram
%matplotlib inline
```

```
circuit = QuantumCircuit(2,1)
```

```
circuit.h(0)
circuit.x(1)
circuit.h(1)
circuit.barrier()
circuit.draw(output='mpl')
```



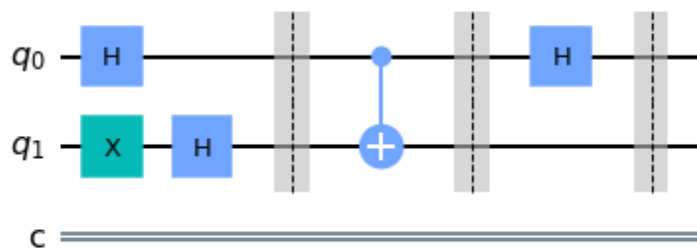


شکل ۱۴: This is an image.

```
circuit.cx(0,1)
circuit.barrier()
circuit.h(0)
circuit.barrier()
circuit.draw(output='mpl')
```

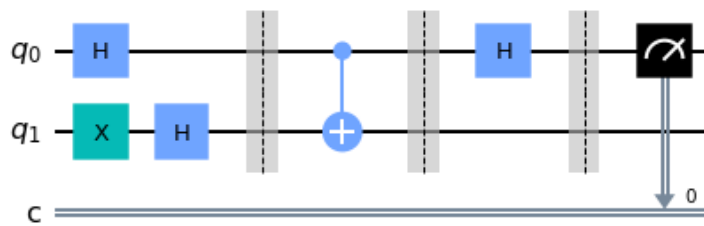
```
circuit.measure(0,0)
```

```
<qiskit.circuit.instructionset.InstructionSet at 0x7fb3a83c1c70>
```



شکل ۱۵: This is an image.

```
circuit.draw(output='mpl')
```



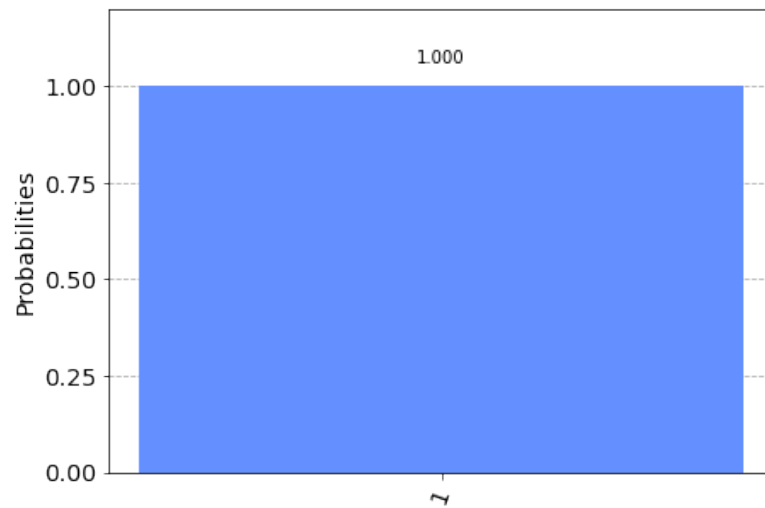
شکل ۱۶: This is an image.

```

backend = Aer.get_backend('qasm_simulator')
result = execute(circuit, backend=backend, shots=1024).result()
counts = result.get_counts(circuit)

plot_histogram([counts])

```



شکل ۱۷: This is an image.

*Computer Quantum #Real*

IBMQ.load\_account()

<AccountProvider for IBMQ(hub='ibm-q', group='open', project='main')>

```
provider = IBMQ.get_provider("ibm-q")
```

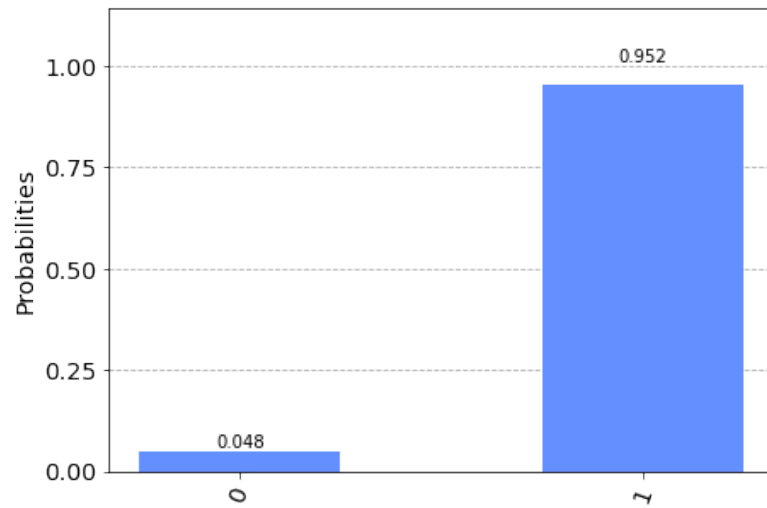
```
for backend in provider.backends():
    try:
        qubit_count = len(backend.properties().qubits)
    except:
        qubit_count = "simulated"
    print(f"{backend.name()} : {backend.status().pending_jobs} & {qubit_count}qubits")
```

```
ibmq_qasm_simulator : 3 & simulated qubits
ibmqx2 : 12 & 5 qubits
ibmq_16_melbourne : 411 & 15 qubits
ibmq_armonk : 48 & 1 qubits
ibmq_athens : 7 & 5 qubits
ibmq_santiago : 13 & 5 qubits
ibmq_lima : 12 & 5 qubits
ibmq_belem : 5 & 5 qubits
ibmq_quito : 4 & 5 qubits
simulator_statevector : 4 & simulated qubits
simulator_mps : 3 & simulated qubits
simulator_extended_stabilizer : 3 & simulated qubits
simulator_stabilizer : 3 & simulated qubits
ibmq_manila : 15 & 5 qubits
```

```
quantum_computer = provider.get_backend('ibmq_belem')
```

```
quantum_result = execute(circuit, backend=quantum_computer, shots=1024).result()
```

```
quantum_counts = quantum_result.get_counts(circuit)
plot_histogram([quantum_counts])
```



شکل ۱۸ : This is an image.





## 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.

### حالات بل

به مدار نمایش داده شده در شکل زیر دقت کنید:

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

بار دیگر مراحل را مرور می‌کنیم:

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

حالت خروجی را می‌توان به شکل زیر نمایش داد:

$$\begin{aligned}
 |\beta_{00}\rangle &= \frac{|00\rangle + |11\rangle}{\sqrt{2}} \\
 |\beta_{01}\rangle &= \frac{|01\rangle + |10\rangle}{\sqrt{2}} \\
 |\beta_{10}\rangle &= \frac{|00\rangle - |11\rangle}{\sqrt{2}} \\
 |\beta_{11}\rangle &= \frac{|01\rangle - |10\rangle}{\sqrt{2}}
 \end{aligned} \tag{۲۱}$$

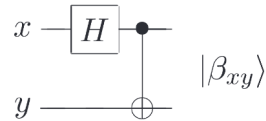
از حالت‌های بالا به عنوان حالات بل یا حالات EPR یاد می‌کنیم.

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

$$|\beta_{ay}\rangle = \frac{|0, y\rangle + (-1)^y |1, \bar{y}\rangle}{\sqrt{2}} \tag{۲۲}$$

منظور از این جمله چیه؟؟ where  $\bar{y}$  is the negation of  $y$ .

In	Out
$ 00\rangle$	$( 00\rangle +  11\rangle)/\sqrt{2} \equiv  \beta_{00}\rangle$
$ 01\rangle$	$( 01\rangle +  10\rangle)/\sqrt{2} \equiv  \beta_{01}\rangle$
$ 10\rangle$	$( 00\rangle -  11\rangle)/\sqrt{2} \equiv  \beta_{10}\rangle$
$ 11\rangle$	$( 01\rangle -  10\rangle)/\sqrt{2} \equiv  \beta_{11}\rangle$



شکل ۱۹: مدار کوانتومی بل به همراه ورودی و خروجی آن

پیاده‌سازی حالات بل در کیس کیت



## درهمنیدگی

در حوزه فیزیک کوانتومی، یکی از گیج کننده ترین پدیده هایی که همچنان توجه دانشمندان و فیلسوفان را به خود جذب می کند، «درهم تنیدگی» است. این مفهوم درک متعارف ما از واقعیت را به چالش می کشد و باعث بحث ها، آزمایش ها و تحقیقات فلسفی بی شماری شده است.

درهم تنیدگی به ارتباط فوق العاده ای اطلاق می شود که می تواند بین دو یا چند ذره، بدون توجه به فاصله ای که آنها را از هم، وجود داشته باشد. هنگامی که ذرات در هم می پیچند، ویژگی های آنها مانند اسپین، تکانه و قطبش به گونه ای به هم مرتبط می شوند که تغییر حالت یک ذره بدون توجه به فضای فیزیکی بین آنها، فوراً بر وضعیت ذره دیگر تأثیر می گذارد. به نظر می رسد این ارتباط آبی با مفاهیم کلاسیک علت و معلول مخالفت می کند.

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

درهم تنیدگی فقط یک مفهوم نظری نیست. به طور تجربی از طریق آزمایش های مختلف مشاهده و تأیید شده است. یکی از مهم ترین آزمایش هایی که درهم تنیدگی را به صورت تجربی نشان می دهد، آزمون بل است. این آزمایش نقض نابرابری های بل را آزمایش می کند. وقتی اندازه گیری های ذرات درهم تنیده این نابرابری ها را نقض می کند، نشان می دهد که رفتار آنها توسط فیزیک کلاسیک قابل توضیح نیست و در عوض به واقعیت درهم تنیدگی کوانتومی اشاره می کند.

پیامدهای درهم تنیدگی عمیق و پیچیده است و فراتر از محدوده آزمایشگاه های فیزیک است. محققان همواره در حال بررسی کاربردهای بالقوه درهم تنیدگی در زمینه هایی مانند محاسبات کوانتومی و رمزنگاری کوانتومی هستند. توانایی درهم تنیدگی برای فعال کردن کیوبیت ها (بیت های کوانتومی) برای وجود همزمان

در چندین حالت، این پتانسیل ایجاد تحولات شگرفی در رمزنگاری کوانتومی و محاسبات کوانتومی دارد و به راه‌حلی منجر شود که قبلاً غیرممکن تلقی می‌شدند.

locality Non

در نتیجه، از درهم تنیدگی به عنوان یکی از جذاب‌ترین و گیج‌کننده‌ترین پدیده‌ها در قلمرو فیزیک کوانتومی یاد می‌شود. ارتباط اسرارآمیز آن بین ذرات، شهود کلاسیک را به چالش می‌کشد و همچنان مرزهای درک ما از جهان را پیش می‌برد. همانطور که دانشمندان عمیق‌تر به پیچیدگی‌های درهم تنیدگی و کاربردهای بالقوه آن می‌پردازند.

### پیاده‌سازی درهم‌تنیدگی در کیس کیت

## رمزگذاری متراکم کوانتومی

رمزگذاری متراکم کوانتومی<sup>۲۶</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:

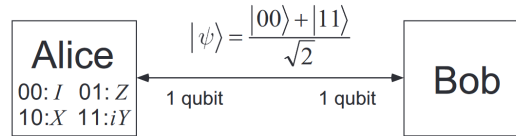
$$|\Psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \quad (۲۳)$$

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

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

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

<sup>۲۶</sup>Quantum super dense coding



شکل ۲۰: تنظیمات اولیه برای کدگذاری فوق متراکم، آلیس و باب که هر کدام یک کیوبیت، از جفت کیوبیت درهم‌تنیده را در اختیار دارند.

همانطور که در شکل بالا قابل ملاحظه است؛ آلیس و باب، هرکدام یک کیوبیت در اختیار دارند. توجه داشته باشید که  $\Psi$  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>۲۷</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:

---

<sup>۲۷</sup>flip phase

$$\begin{aligned}
 00 : |\psi\rangle &\rightarrow \frac{|00\rangle + |11\rangle}{\sqrt{2}} \\
 01 : |\psi\rangle &\rightarrow \frac{|00\rangle - |11\rangle}{\sqrt{2}} \\
 10 : |\psi\rangle &\rightarrow \frac{|10\rangle + |01\rangle}{\sqrt{2}} \\
 11 : |\psi\rangle &\rightarrow \frac{|01\rangle - |10\rangle}{\sqrt{2}}.
 \end{aligned}
 \tag{۲۴}$$

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

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

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

مراحل این پروتکل به اختصار به شرح زیر است:

- آلیس و باب یک جفت کیوبیت درهم‌تنیده را با هم به اشتراک می‌گذارند.
- آلیس می‌خواهد دو بیت کلاسیک، ۰۰ یا ۰۱ را به باب ارسال کند.
- آلیس یک عمل واحد بر روی کیوبیت خود اعمال می‌کند که بسته به بیت‌هایی که می‌خواهد به باب

ارسال کند متفاوت است.

- آلیس کیوبیت خود را به باب می‌فرستد.
- باب کیوبیت را اندازه‌گیری می‌کند و دو بیت کلاسیکی که آلیس به او ارسال کرده است را دریافت می‌کند.
- اگر آلیس یک عمل یکه بر روی کیوبیت خود اعمال نکند، باب فقط می‌تواند یک بیت کلاسیک را دریافت کند. با این حال، اگر آلیس عمل یکه مناسب را اعمال کند، می‌تواند دو بیت کلاسیک را با ارسال یک کیوبیت انتقال دهد.

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

### پیاده‌سازی رمزگذاری متراکم در کیس کیت

```
Coding Superdense #
```

```
%matplotlib inline
```

```
from qiskit import *
```

```
State Bell the Prepare 0: Step #
```

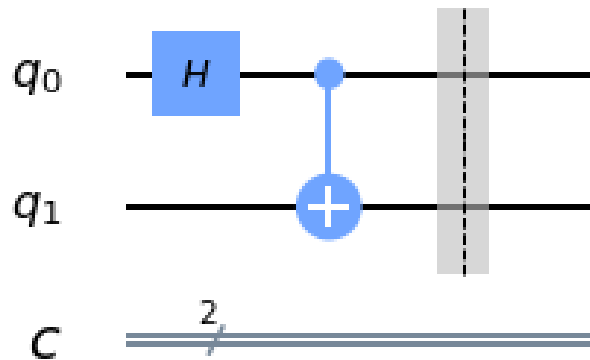
```
bell_circuit = QuantumCircuit(2, 2)
```

```
bell_circuit.h(0)
```

```
bell_circuit.cx(0, 1)
```

```
bell_circuit.barrier()
```

```
bell_circuit.draw(output="mpl")
```



شکل ۲۱: This is an image.

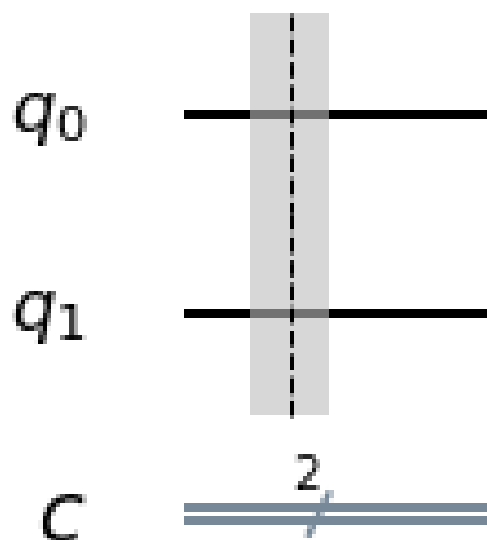
*b0b1 on depending circuits Alice Prepare 1: Step #*

*gates no has circuit the 00: Case #*

```
alice_00 = QuantumCircuit(2, 2)
```

```
alice_00.barrier()
```

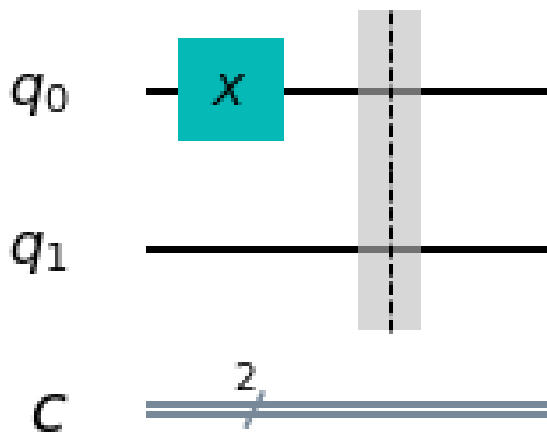
```
alice_00.draw(output="mpl")
```



شکل ۲۲: This is an image.

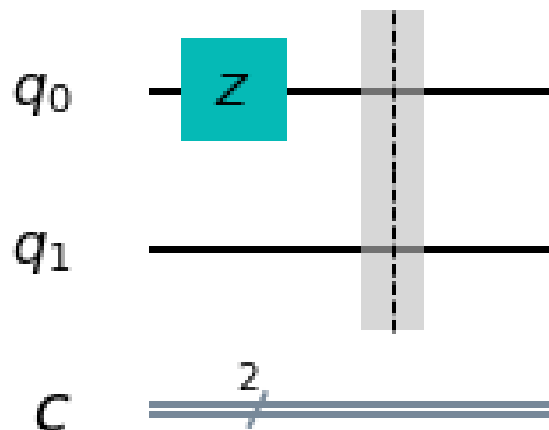


```
gate X the has circuit the 01: Case #
alice_01 = QuantumCircuit(2, 2)
alice_01.x(0)
alice_01.barrier()
alice_01.draw(output="mpl")
```



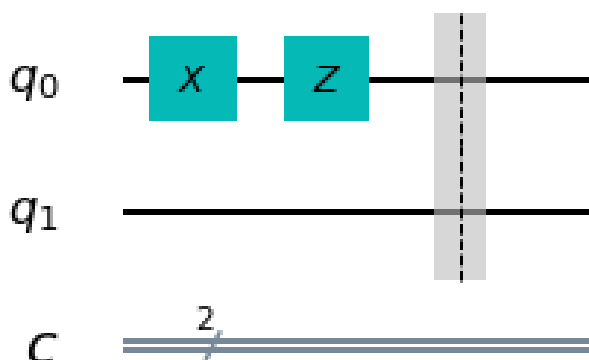
شکل ۲۳ : This is an image.

```
gate Z the has circuit the 10: Case #  
alice_10 = QuantumCircuit(2, 2)  
alice_10.z(0)  
alice_10.barrier()  
alice_10.draw(output="mpl")
```



شکل ۲۴: This is an image.

```
gate Z then and gate X the has circuit the 11: Case #
alice_11 = QuantumCircuit(2, 2)
alice_11.x(0)
alice_11.z(0)
alice_11.barrier()
alice_11.draw(output="mpl")
```

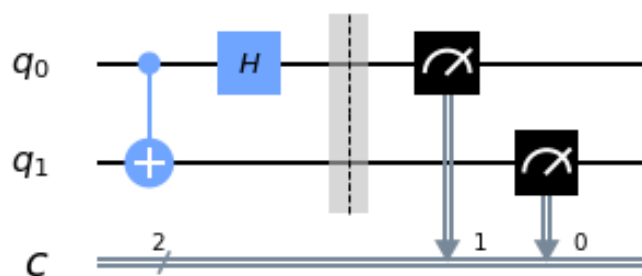


شکل ۲۵: This is an image.

```

measure then and ,circuit entanglement inverted the Apply 2: Step #
invert_circuit = QuantumCircuit(2, 2)
invert_circuit.cx(0, 1)
invert_circuit.h(0)
invert_circuit.barrier()
invert_circuit.measure([0, 1], [1, 0]) b0b1 not b1b0 ,reversed always are measur
invert_circuit.draw(output="mpl")

```

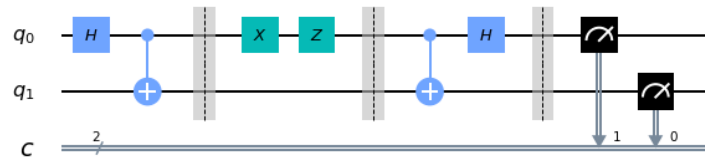


شکل ۲۶: This is an image.

```

like looks circuit whole the ,merged When #
(bell_circuit + alice_11 + invert_circuit).draw(output="mpl")

```



شکل ۲۷: This is an image.

it runs that function auxiliary an create we so do to ,outcome each si

```
def simulate_circuit(prepare, encoding, decoding):
```

*circuits""" three the of combination is that circuit the of counts*

```
    circuit = prepare + encoding + decoding
```

```
    simulator = Aer.get_backend("qasm_simulator")
```

```
    job = execute(circuit, simulator, shots = 2**16)
```

```
    result = job.result()
```

```
    count = result.get_counts()
```

```
    return count
```

*00 For #*

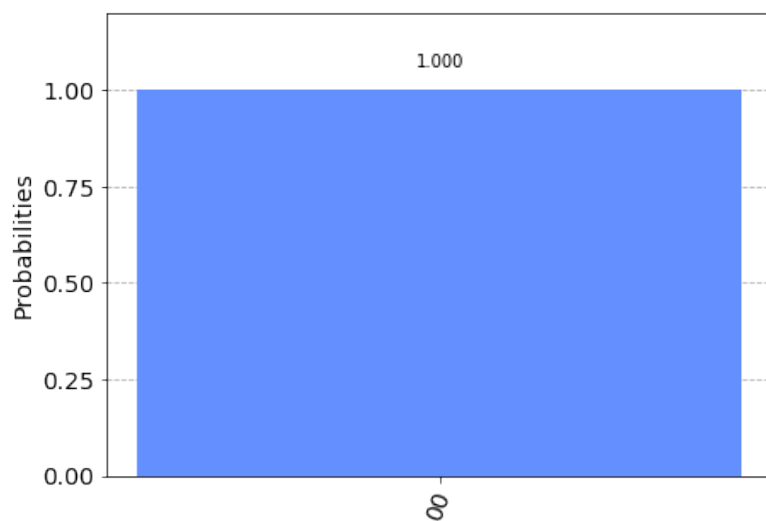
```
count_00 = simulate_circuit(bell_circuit, alice_00, invert_circuit)
```

```
visualization.plot_histogram(count_00)
```

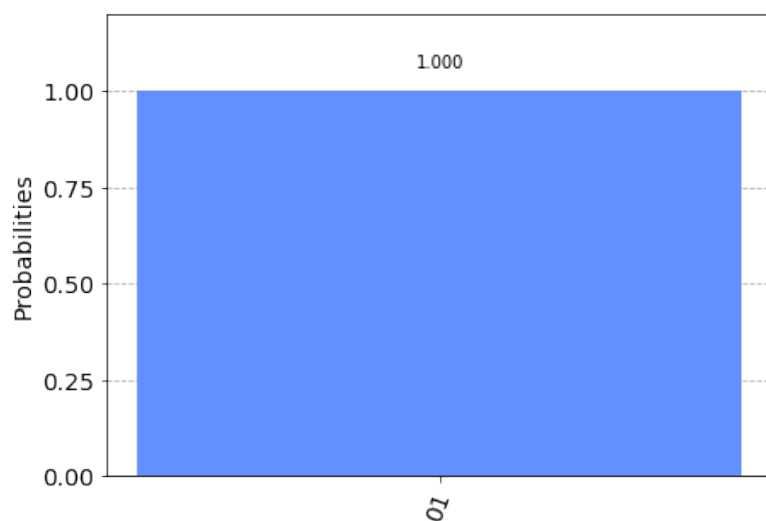
*01 For #*

```
count_01 = simulate_circuit(bell_circuit, alice_01, invert_circuit)
```

```
visualization.plot_histogram(count_01)
```



شکل ۲۸: This is an image.

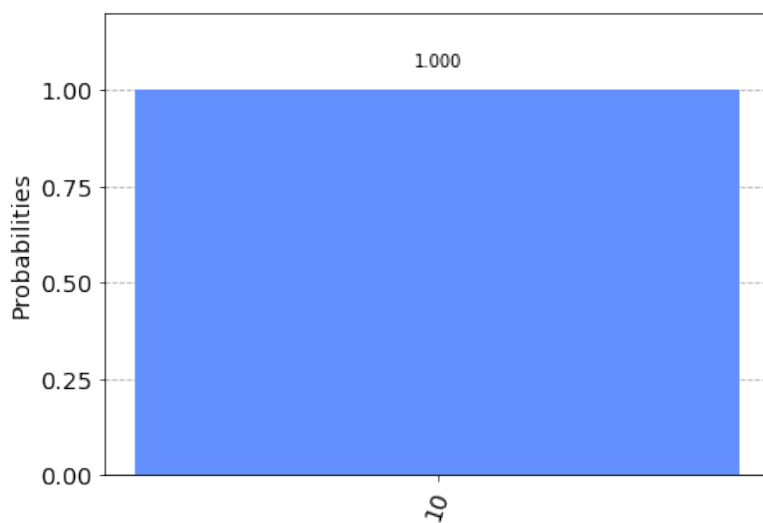


شکل ۲۹: This is an image.

```
10 For #
```

```
count_10 = simulate_circuit(bell_circuit, alice_10, invert_circuit)
```

```
visualization.plot_histogram(count_10)
```

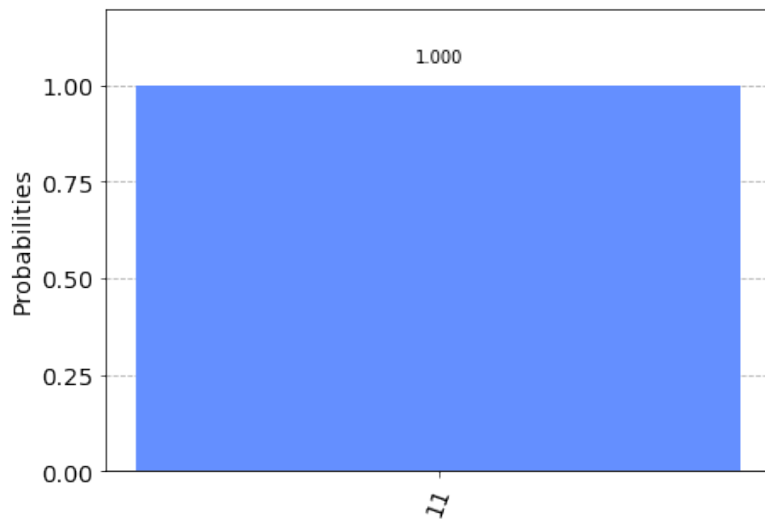


شکل ۳۰: This is an image.

```
11 For #
```

```
count_11 = simulate_circuit(bell_circuit, alice_11, invert_circuit)
```

```
visualization.plot_histogram(count_11)
```



شکل ۳۱: This is an image.

*predictions! our match results The #*  
*is version Qiskit the ,reproducibility of purposes For #*  
 qiskit.\_\_qiskit\_version\_\_

```
{'qiskit-terra': '0.11.0',
 'qiskit-aer': '4.3.0',
 'qiskit-ignis': '0.2.0',
 'qiskit-ibmq-provider': '4.4.0',
 'qiskit-aqua': '1.6.0',
 'qiskit': '0.14.0'}
```





## دوربری

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

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

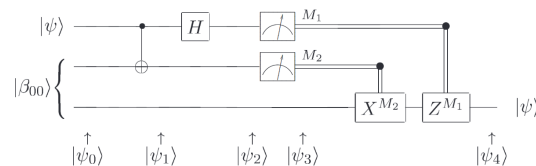
در ظاهر، تمام شرایط علیه آلیس است. او وضعیت  $|\Psi\rangle$  کیوبیتی را که باید برای باب بفرستد نمی‌داند، و طبق قوانین مکانیک کوانتومی، او حق تعیین وضعیت  $|\Psi\rangle$  را ندارد؛ زیرا فقط یک نسخه از جفت کیوبیت را در اختیار دارد. به علاوه، حتی اگر او حالت  $|\Psi\rangle$  را می‌دانست، توصیف دقیق آن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

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

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

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

$$|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle \quad (۲۵)$$



شکل ۳۲: مدار کوانتومی برای انتقال یک کیوبیت دو خط بالا نشان دهنده سیستم آلیس هستند، در حالی که خط پایین نشان دهنده سیستم آلیس است خط سیستم باب است. مترها اندازه گیری را نشان می دهند و خطوط دوتایی که از آنها بیرون می آیند دارای حالت کلاسیک هستند بیت ها (به یاد بیاورید که خطوط منفرد نشان دهنده کیوبیت هستند)

$$= \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)] \quad (۲۶)$$

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

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)] \quad (۲۷)$$

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

$$|\psi_2\rangle = \frac{1}{2}[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)] \quad (۲۸)$$

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

$$|\psi_2\rangle = \frac{1}{2} [ |00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle) ] \quad (29)$$

این عبارت به طور طبیعی به چهار اصطلاح تقسیم می‌شود. عبارت اول دارای کیوبیت های آلیس است در حالت  $|00\rangle$  و کیوبیت باب، که بیانگر حالت اصلی  $|\Psi\rangle$  است؛ در حالت  $\alpha|0\rangle + \beta|1\rangle$  قرار دارد.

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

$$\begin{aligned} 00 &\mapsto |\psi_3(00)\rangle \equiv [\alpha|0\rangle + \beta|1\rangle] \\ 01 &\mapsto |\psi_3(01)\rangle \equiv [\alpha|1\rangle + \beta|0\rangle] \\ 10 &\mapsto |\psi_3(10)\rangle \equiv [\alpha|0\rangle - \beta|1\rangle] \\ 11 &\mapsto |\psi_3(11)\rangle \equiv [\alpha|1\rangle - \beta|0\rangle] \end{aligned} \quad (30)$$

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

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

اگر نتیجه‌ی اندازه گیری ۱۰ باشد، باب می‌تواند حالت کیوبیت خود را با استفاده از گیت Z ثابت کند. اگر

اندازه‌گیری ۱۱ باشد، باب می‌تواند با اعمال ابتدا یک  $X$  و سپس یک گیت  $Z$  حالت کیوبیت خود را اصلاح کند. به طور خلاصه، باب باید تبدیل  $ZM1XM2$  را در کیوبیت خود اعمال کند<sup>۲۸</sup>؛ و بدین طریق او می‌تواند حالت  $|\Psi\rangle$  را بازیابی می‌کند.

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

### سوال اول

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

می‌توان نشان داد؛ که بدون این کانال ارتباطی کلاسیک، دوربری توان انتقال هیچ اطلاعاتی را ندارد.

کانال ارتباط کلاسیک با سرعت نور محدود می‌شود، بنابراین می‌توان نتیجه گرفت که تله پورت کوانتومی نمی‌تواند سریعتر از سرعت نور انجام شود و این تناقض ظاهری را حل می‌شود.

### سوال دوم

در فرآیند دوربری به نظر می‌رسد یک کپی از حالت کوانتومی در حال انتقال از راه دور ایجاد می‌شود؛ در حالی که آشکارا قضیه عدم شبیه سازی<sup>۲۹</sup> مورد بحث نقض می‌کند.

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

<sup>۲۸</sup> توجه داشته باشید که چگونگی زمان در نمودارهای مدار از چپ به راست می‌گذرد، اما در عملیات‌های ماتریسی سمت راست اول اتفاق

می‌افتد

<sup>۲۹</sup> No cloning theorem

## پیاده‌سازی دوربری در کیس کیت

```
from qiskit import *
```

```
circuit = QuantumCircuit(3,3)

circuit.x(0) example this in 1 state transfer to want we ,optional #

circuit.barrier()

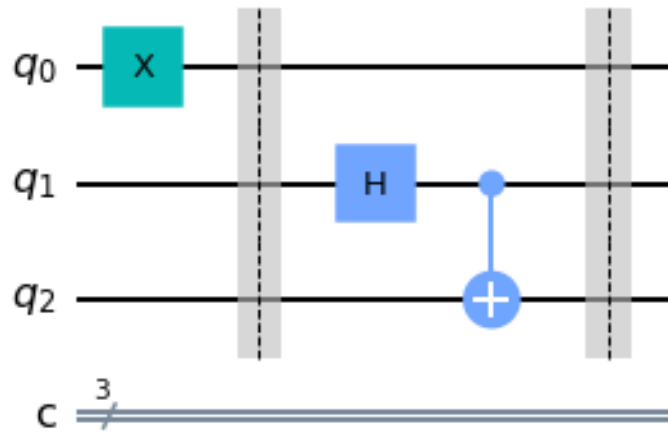
circuit.h(1)
circuit.cx(1,2)

circuit.barrier()
```

```
<qiskit.circuit.instructionset.InstructionSet at 0x7fc41902df70>
```

```
%matplotlib inline
```

```
circuit.draw(output='mpl')
```



شکل ۳۳: This is an image.

```

circuit.cx(0,1)
circuit.h(0)

circuit.barrier()
circuit.draw(output='mpl')

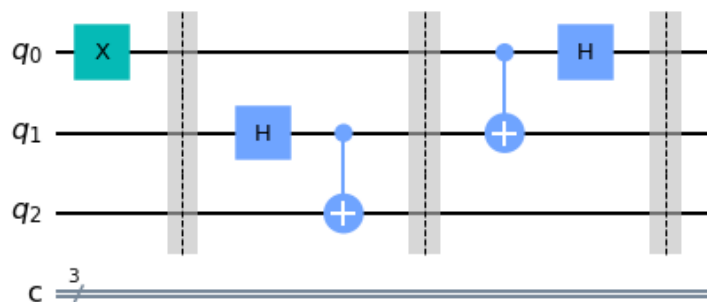
```

```

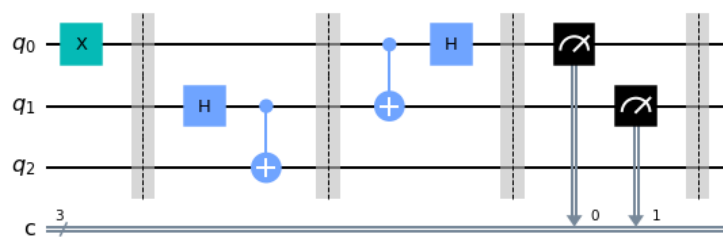
circuit.measure([0, 1], [0, 1])

circuit.barrier()
circuit.draw(output='mpl')

```



شکل ۳۴: This is an image.



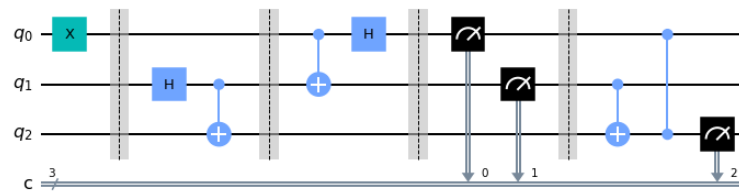
شکل ۳۵: This is an image.



```

circuit.cx(1, 2)
circuit.cz(0, 2)
circuit.measure([2], [2])
circuit.draw(output='mpl')

```

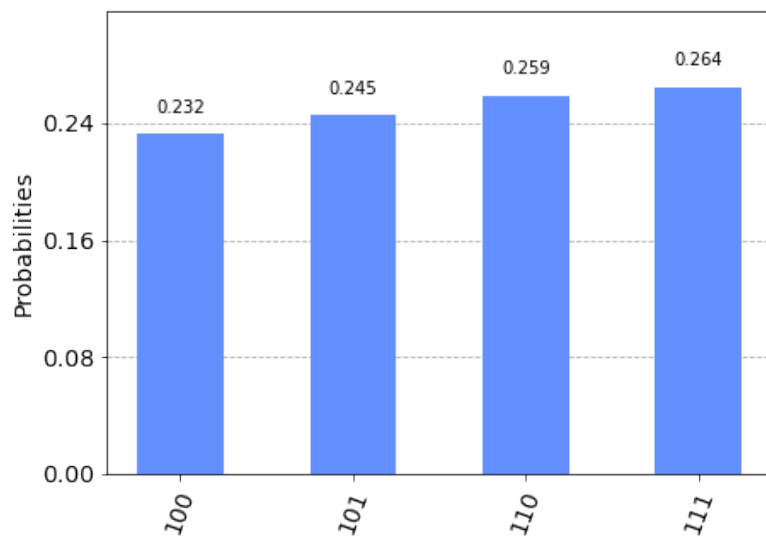


شکل ۳۶: This is an image.

```

simulator = Aer.get_backend('qasm_simulator')
result = execute(circuit, backend=simulator, shots=1024) result()
from qiskit.visualization import plot_histogram
plot_histogram(result.get_counts(circuit))

```



شکل ۳۷: This is an image.

