دانشگاه صنعتی امیرکبیر
(پلی‌تکنیک تهران)
دانشکده مهندسی کامپیوتر

درس روش پژوهش

گزارش نوشتاری

آشنایی مقدماتی با محاسبات کوانتومی از دید مهندسی کامپیوتر

نگارش

هلیا اکبری

استاد راهنما

دکتر حامد فربه

خرداد ۱۴۰۳


بسم الله الرحمن الرحيم

Amirkabir University of Technology
(Tehran Polytechnic)

Department of computer engineering

M. Sc. Thesis

An introdunction to quantum computing from computer engineering standpoint

By

Helia Akbari

Supervisor

Dr. Hamed Farbeh

June 2024

سپاس‌گزاری

از استاد گرامی جناب آقای دکتر حامد فربه که در انتخاب و پیشبرد این پروژه به عنوان استاد پروژه و به عنوان راهنما، در طول دوران تحصیلی این جانب، کمک های فراوانی داشته‌اند، کمال تشکر را دارم.

هلیا اکبری
خرداد ۱۴۰۳

چکیده

محاسبات کوانتوم عبارتی است که در همه فیلم های علمی‌تخیلی به گوش میخورد. عموم جامعه هیچ آگاهی در این زمینه ندارند و حتی تصوری از استفاده ی آن و پیشرفت های این زمینه ندارند. دانشجویان حوزه مهندسی کامپیوتر نیز به دنبال این زمینه نمیروند یا کمتر میروند چرا که تصور دارند این زمینه نیاز به دانش فیزیک پیشرفته و مکانیک پیشرفته دارد یا اساسا بدون کاربرد و برای آینده ی دور است. این مقاله قصد دارد محاسبات کوانتوم را برای دانشجویان کامپیوتری که به ساختار کامپیوتر، مسائل روز دنیای کامپیوتر و الگوریتم های رایج کامپیوتری آشنایی دارند، به صورت کاربردی و ملموس با آموخته‌هایشان توضیح دهد.
ابتدا با توضیح مفاهیم پایه همچون ریاضی کوانتومی، ویژگی های معادلات کوانتومی، ماهیت متغیر های کوانتومی، و قوانین حاکم بر دنیای کوانتوم شروع میکنیم. سپس، تعدادی از الگوریتم هایی که با محاسبات کوانتومی میتوان به آنها رسید و دلیل اهمیتشان را شرح میدهیم. در همین راستا، از کابرد های مختلف محاسبات کوانتومی خواهیم گفت و در نهایت، خواننده را با محدودیت هایی که ما را از این دنیای جدید و ناشناخته دور میسازد، آشنا خواهیم ساخت.

واژه‌های کلیدی:

محاسبات کوانتوم، کوانتوم، آشنایی، مهندسی کامپیوتر، کامپیوتر کوانتومی

فهرست مطالب

فهرست تصاویر

شکل صفحه

فصل اول

مقدمه

بر اساس قانون مور [۱] قدرت پردازنده‌های کامپیوترهای کلاسیک هر دو سال، دو برابر میشود. اما این رویه تا حدی ادامه خواهد داشت که محدودیت‌های دنیای فیزیک کلاسیک به آن اجازه دهند. چرا که اندازه ی اعضای تشکیل دهنده ی پردازنده‌ها به حدی کوچک میشود که ناخودآگاه وارد فضای کوچک کوانتوم [۲] میشوند. پیشبینی میشود این اتفاق در سال ۲۰۵۰ رخ دهد.
پیچیدگی محاسباتی [۳] برخی الگوریتم‌ها در کامپیوترهای کلاسیک کمتر قابلیت کاهش ندارند. در حالی که کامپیوتر های کوانتومی، در تئوری میتوانند با مقدار بزرگی داده همانند یک واحد داده برخورد کنند و پیچیدگی محاسباتی الگوریتم‌ها را کاهش دهند. [۳] به طور کلی، محاسبات کوانتومی از کنش و واکنش مواد در جهان در سطح ذرات تشکیل‌دهنده آن بهره میگیرد و بر روی بستر پدیده نسبیت خاص [۴] پایه‌گذاری شده‌است.
برای مثال، کامپیوتر کلاسیک مشکلی در پیدا کردن نام فرد موردنظر در یک کتاب تلفن ندارند. اما برای مسائل ریاضی بهینه سازی پیچیده [۵] که مسائلی هستند که برای پیدا کردن حالت بهینه با توجه به متغیرهای مختلف است، کامپیوترهای کلاسیک پاسخگو نیستند. از جمله این مسائل میتوان به اختصاص دادن منابع در ساخت یک برج بزرگ برای بدست آوردن کمترین خرج ممکن اشاره کرد. چنین مسائلی در همه ی حوزه‌ها وجود دارند و کامپیوترهای کوانتومی برای اجرای این الگوریتم‌ها بسیار مناسب هستند. [۱]

[1] Moore's law
[2] Quantum
[3] Computational complexity
[4] Special relativity
[5] Complex mathematical optimizing

فصل دوم

خواص دنیای محاسبات کوانتومی

۲-۱ کیوبیت

کیوبیت‌ها [۱] در کامپیوترهای کوانتومی، معادل بیت ها [۲] در کامپیوترهای کلاسیک هستند. یک بیت یا در حالت صفر قرار دارد یا در حالت یک قرار دارد. تفاوت کیوبیت‌ها در این است که میتوانند حالی به جز صفر یا یک داشته باشند یا میتوان گفت برهم‌نهی [۳] حالات را شاهد هستیم. درنتیجه، کیوبیت میتواند حالات بیشتری از بیت داشته باشد. هر کیوبیت، به یک احتمالی میتواند یک باشد و به یک احتمالی میتواند صفر باشد.

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \begin{bmatrix}\alpha\\ \beta\end{bmatrix} \tag{۲-۱}$$

به طوری که α و β شدت احتمال هستند و هر دو اعداد مختلط هستند به طوری که

$$\alpha^2 + \beta^2 = 1 \tag{۲-۲}$$

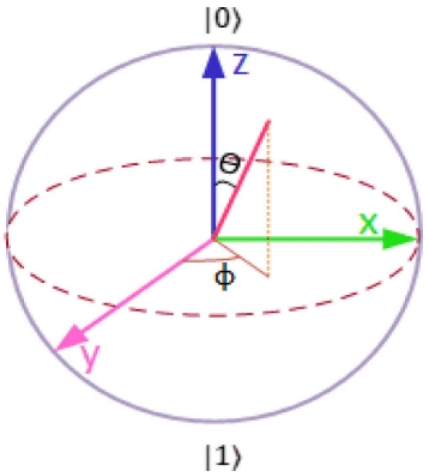
فضای حالتی که این دو متغیر تشکیل میدهند، یک فضای مختلط دو بعدی است. حالات خاص صفر و یک، یک فضای بردار پایه ای [۴] برای این فضای برداری تشکیل میدهند.

$$|0\rangle = (0,1) and\, |1\rangle = (1,0) \tag{۲-۳}$$

در شکل پایین، میتوانید کره بلاچ [۵] که نوعی بازنمایی هندسی از حالت یک کیوبیت است، را مشاهده کنید. این بازنمایی را میتوانید به تعداد نامحدودی کیوبیت هم انطباق دهید. به طوری که با داشتن n کیوبیت نیاز به نگهداری n^2 عدد خواهید داشت. این حالت زمانی رخ میدهد که n کیوبیت درهم‌تنیده [۶] شوند به طوری که باهم یک حالت را تشکیل دهند و نتوان آنها را جدا کرد. [۲] همچنان جمع مجذور همه مقادیر باید برابر با یک شود. نمایش انتزاعی دو کیوبیت به شکل زیر خواهد بود:

$$|\Psi\rangle = \alpha_0\,|00\rangle + \alpha_1\,|01\rangle + \alpha_2\,|10\rangle + \alpha_3\,|11\rangle = \begin{bmatrix}\alpha_0\\ \alpha_1\\ \alpha_2\\ \alpha_3\end{bmatrix} \tag{۲-۴}$$

[1] Qubits
[2] bits
[3] superposition
[4] orthonormal basis
[5] Bloch's sphere
[6] entangled



شکل ۲-۱: بازنمایی کیوبیت در کره بلاچ

نمایش دو کیوبیت در فرم ماتریسی و دیراک [۷] :

$$|00\rangle = \begin{bmatrix} \alpha_1 \\ \alpha_0 \\ \alpha_0 \\ \alpha_0 \end{bmatrix} ؛ |01\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_0 \\ \alpha_0 \end{bmatrix} ؛ |10\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_0 \\ \alpha_1 \\ \alpha_0 \end{bmatrix} ؛ |11\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_0 \\ \alpha_0 \\ \alpha_1 \end{bmatrix} \quad (۵-۲)$$

۲-۲ ضرب تانسوری

ضرب تانسوری [۸] ، عملیاتی است که بین دو ماتریس میتوان انجام داد. این عملیات، یکی از بخش‌های اصلی محاسبات کوانتومی است. برای اینکه بتوان سیستم‌های چند-کیوبیتی [۹] را به صورت ریاضی نمایش داد، از این عملیات استفاده میشود. به این صورت که اگر M یک ماتریس (p, q) باشد و N یک ماتریس (x, y) باشد، ماتریس ضرب تانسوری آنها یک ماتریس (px, qy) خواهد بود. [۲] این ضرب را میتوان با یک گیت کوانتومی [۱۰] اعمال کرد.

$$M = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} ؛ N = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \quad (۶-۲)$$

[7] Dirac
[8] Tensor product
[9] multiple-qubit systems
[10] quantum gate

$$M \otimes N = \begin{bmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{bmatrix} \quad (۷-۲)$$

برای ضرب تانسوری دو کیوبیت خواهیم داشت:

$$|0\rangle \otimes |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = |01\rangle \quad (۸-۲)$$

۲-۳ اصل برهم‌نهی

در دنیای روزمره، همه اشیا، حتی زمانی که به آنها نگاه نمیکنیم، در یک حالت مشخص قرار دارند. این موضوع برای اجسام کوچک همانند کیوبیت ها صدق نمیکند. یک جسم بسیار کوچک میتواند در یک زمان، در چند مکان باشد. در نتیجه، به جای اینکه بگوییم جسم در یک جا قرار دارد، میگوییم در برهم‌نهی قرار دارد. نه تنها مکانش میتواند در چند حالت باشد، بلکه سطح انرژی، شتاب، و خواص کوانتومی آن نظیر چرخش [۱۱] میتواند در چند حالت باشد.
ما نمیتوانیم این برهم‌نهی را مشاهده کنیم. به محض مشاهده کیوبیت، یا در واقع اندازه گیری آن، حالت آن به یک حالت واحد تبدیل میشود و همه ی مقادیرش ثابت میشوند. در نتیجه، یکی از چالش‌های محاسبات کوانتومی، مشاهده نکردن کیوبیت‌ها در طول فرآیند است. کیوبیت‌ها تنها در آخرین مرحله ی الگوریتم باید مشاهده شوند. [۶]

۲-۴ اصل درهم‌تنیدگی

کیوبیت‌ها خاصیت درهم‌تنیدگی [۱۲] دارند. به این صورت که با اندازه‌گیری برخی از آنها، مقدار برخی دیگر مشخص میشود و آنها هم مشاهده میشوند. این حالت به فاصله دو کیوبیت ربطی ندارد. درنتیجه میتوان دو کیوبیت را در هم تنید و از هم تا بینهایت دور کرد. سپس، اگر یکی از آنها مشاهده شود، حالت دیگری هم مشخص میشود و به یک حالت واحد تبدیل میشود. این حالت درهم‌تنیدگی همچنان باقی خواهند ماند. نمایش ریاضی درهم‌تنیدگی زمانی است که نتوان حالت شامل چند کیوبیت را به ضرب تانسوری آن کیوبیت‌ها تبدیل کرد. در واقع ضربی وجود نخواهد داشت که آن حالت نهایی را درست کند. درهم‌تنیدگی را میتوان با استفاده از گیت‌های کوانتومی انجام داد. درهم‌تنیدگی در حوزه رمزنگاری و انتقال داده استفاده بخصوص دارد. [۶]

[11] spin

[12] entanglement

۲-۵ برگشت‌پذیری و گیت‌های کوانتومی

محاسبات کوانتومی وابستگی حیاتی به محاسبات برگشت‌پذیر [۱۳] دارد. برگشت‌پذیری یعنی بتوان ورودی را با توجه به دانستن خروجی و تابع، بدست‌آورد. برای مثال در کامپیوتر کلاسیک گیت $NAND$ برگشت‌ناپذیر و گیت NOT برگشت‌پذیر است. در نتیجه این خاصیت، هیچ داده و انرژی‌ای از بین نمیرود.
همه گیت‌های کوانتومی باید خاصیت برگشت‌پذیری را داشته باشند. این برتری محاسبات کوامتومی به محاسبات کلاسیک است. گیت‌های کوانتومی بر روی مقدار کوچکی از کیوبیت ها عملیات انجام می‌دهند و بلوک‌های ساخت مدارهای کوانتومی هستند. گیت‌های پایه و لازم کوانتومی شامل H, X, Y, Z, T, I و گیت فاز [۱۴] میباشد. همچنین گیت‌های NOR, OR, AND, XOR را نیز میتوان پیاده‌سازی کرد. گیت هایی که ورودی n کیوبیت دارند، با یک ماتریس $2^n * 2^n$ نمایش داده میشوند. [۲]

Gate	Matrix Representation
H (Hadamard gate)	$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$
NOT (Pauli X gate)	$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$
Y (Pauli Y gate)	$\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}$
Z (Pauli Z gate)	$\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$
T ($\frac{\pi}{8}$ phase gate)	$\begin{bmatrix}1 & 0\\ 1 & e^{i\frac{\pi}{4}}\end{bmatrix}$
Identity Gate	$\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$
Phase Gate	$\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}$

شکل ۲-۲: بازنمایی ماتریسی برخی از گیت‌های کوانتومی

[13] reversible calculation
[14] phase gate

فصل سوم

الگوریتم‌های کوانتومی

در حال حاضر، چندین الگوریتم کوانتومی وجود دارد. این الگوریتم‌ها، کیوبیت‌ها را به صورتی تغییر میدهند که مسائل را حل کنند. به طور کلی، این الگوریتم‌ها کارایی بالاتری از الگوریتم‌های کلاسیک معادل خود دارند و باید هم چنین باشد زیرا در غیر این صورت، استفاده از کامپیوترهای کلاسیک و الگوریتم‌های کلاسیک، گزینه بهتری خواهد بود.
همه الگوریتم‌های کوانتومی ۴ مرحله ی یکسان را دنبال میکنند:

۱. هنگام شروع به کار سیستم، کیوبیت‌ها در یک حالت کلاسیک خاص قرار دارند(صفر یا یک)

۲. سیستم در حالت برهم‌نهی میرود

۳. سپس با اعمال گیت‌ها و عملیات مختلف، احتمالات برهم‌نهی تغییر پیدا میکند

۴. در نهایت، کیوبیت ها اندازه‌گیری میشوند [۶]

در الگوریتم‌های کوانتومی، از آنجایی که کیوبیت‌ها و حالات دارای احتمال هستند، همیشه با ورودی‌های یکسان، خروجی یکسان نخواهد بود. با انجام یک الگوریتم بر روی یک ورودی مشخص بارها و بارها، میتوان احتمال هر خروجی را بدست آورد. معمولا، جواب درست، از لحاظ احتمالاتی، فاصله زیادی با دیگر خروجی‌ها دارد.

۳-۱ الگوریتم دویچ

الگوریتم دویچ [1] ساده‌ترین الگوریتم کوانتومی است. فرض کنید تابعی داریم به نام f که فضای ورودی آن $\{0,1\}$ و فضای خروجی آن $\{0,1\}$ است. در این تابع، اگر $f(0)! = f(1)$ باشد، تابع متعادل است و اگر $f(0) = f(1)$ باشد، تابع ثابت است. فرض کنید نمیدانیم تابع از کدام نوع است و میخواهیم نوع تابع را مشخص کنیم. در الگوریتم کلاسیک، برای بدست آوردن جواب، دو بار فراخوانی تابع نیاز است. اما با استفاده از الگوریتم دویچ و محاسبات کوانتومی، با یک بار فراخوانی تابع به جواب میرسیم. ابتدا مسئله را مدل میکنیم. ۳-۱

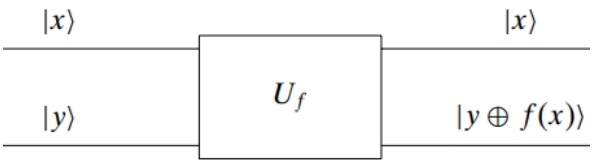
$$f(x) \oplus f(y) = \begin{cases} 1 & : \quad \texttt{f is balanced} \\ 0 & : \quad \texttt{f is constant} \end{cases} \tag{۳-۱}$$

تابع کوانتومی معادل با f را میتوان با یک ماتریس نشان داد. این تابع برگشت‌پذیر است و دو کیوبیت دریافت میکند و حاصل آن نیز دو کیوبیت با احتمالا متفاوت است. در نمایش ماتریسی، ردیف بالا خروجی ها و ستون چپ، ورودی ها را نشان میدهد. ۳-۱ ۳-۲

حال، باید مداری طراحی کنیم که ابتدا دو کیوبیت جامد(در حالت ساده فیزیک) را به حالت برهم‌نهی ببرد، تابع ارزیابی را روی آنها اعمال کند و درنهایت، با تبدیل دوباره کیوبیت‌ها به حالت جامد، آنها را اندازه‌گیری کند. دویچ، مدار شکل ۳-۳ را درنظر میگیرد. [2] برای راحتی دنبال کردن چرایی کارایی این الگوریتم و آشنایی با معادلات کوانتومی، حالت کیوبیت‌ها در هر مرحله زمانی از الگوریتم به نمایش گذاشته‌شده است. ۳-۴

[1] Deutsch's algorithm

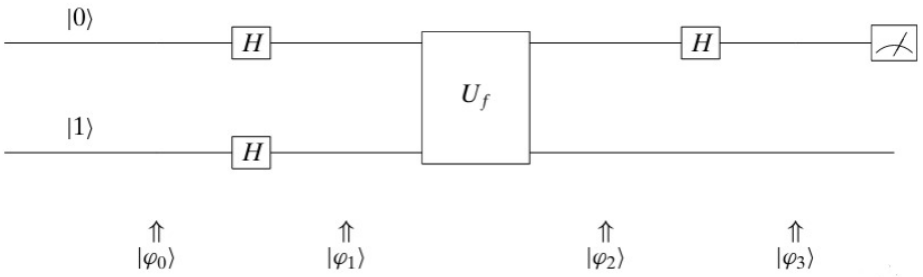
[2] solid-state qubit



شکل ۳-۱: تابع کوانتومی ارزیابی f

$$\begin{array}{c} \\ \mathbf{00} \\ \mathbf{01} \\ \mathbf{10} \\ \mathbf{11} \end{array} \begin{array}{c} \begin{array}{cccc} \mathbf{00} & \mathbf{01} & \mathbf{10} & \mathbf{11} \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \end{array}.$$

شکل ۳-۲: بازنمایی ماتریسی تابع کوانتومی ارزیابی f



شکل ۳-۳: مدار نهایی الگوریتم دویچ

۰. ورودی بالا را کیوبیت جامد با مقدار صفر و ورودی پایین را با مقدار یک قرار میدهیم.

۱. با اعمال گیت هادامار [۳] ، کیوبیت ها را به حالت برهم‌نهی میبریم.

۲. در اینجا، مقدار های نامشخص f را در معادله قرار میدهیم. درنهایت، جواب بدست آمده، این مقادیر را مشخص میکنند. در نتیجه، با استفاده از خروجی میتوانیم نوع تابع را مشخص کنیم.

۳. تابع هادامار برگشت‌پذیر است و با اعمال دوباره آن، تاثیر اولیه‌اش را از بین میبریم.

و در نهایت، کیوبیت بالایی اندازه‌گیری میشود. اگر در حالت صفر قرار داشته باشد، تابع ثابت است و اگر در حالت یک باشد، تابع متعادل است. برتری الگوریتم کوانتومی این است که با یک بار ارزیابی، به جواب مسئله میرسیم که نصف قدم های الگوریتم کلاسیک است. هدف این الگوریتم این است که نشان دهد محاسبات کوانتومی میتوانند از محاسبات کلاسیک کارآمد تر باشند. [۶]

[3] Hadamar's gate

$$|\varphi_0\rangle = |0,1\rangle,$$

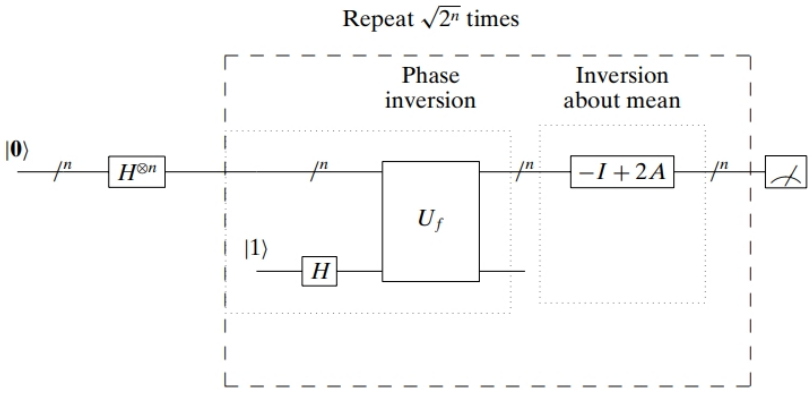
$$|\varphi_1\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] = \frac{+|0,0\rangle - |0,1\rangle + |1,0\rangle - |1,1\rangle}{2} = \begin{matrix}\mathbf{00}\\ \mathbf{01}\\ \mathbf{10}\\ \mathbf{11}\end{matrix}\begin{bmatrix}+\frac{1}{2}\\ -\frac{1}{2}\\ +\frac{1}{2}\\ -\frac{1}{2}\end{bmatrix}.$$

$$|\varphi_2\rangle = \left[\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right].$$

$$|\varphi_2\rangle = \begin{cases}(\pm 1)\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right], & \text{if } f \text{ is constant,}\\ (\pm 1)\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right], & \text{if } f \text{ is balanced.}\end{cases}$$

$$|\varphi_3\rangle = \begin{cases}(\pm 1)|0\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right], & \text{if } f \text{ is constant,}\\ (\pm 1)|1\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right], & \text{if } f \text{ is balanced.}\end{cases}$$

شکل ۳-۴: حالت کیوبیت‌ها در هر مرحله از مدار



شکل ۳-۵: مدار گراور

۳-۲ الگوریتم گراور

یکی از مسائل همیشگی کامپیوتر، پیدا کردن یک المان خاص در یک آرایه نامرتب با طول m است. در حالت کلاسیک، برای اینکار در بدترین حالت، m درخواست باید انجام دهیم و در حالت میانگین به $m/2$ درخواست نیاز است. الگوریتم گراور [۴] این زمان را به $\sqrt{m}$ درخواست تقلیل میدهد. البته چنین کاهش سرعتی در مقایسه با افزایش سرعت نمایی، چندان به چشم نمی‌آید.
جزئیات ریاضی این الگوریتم طولانی است درنتیجه در این بخش بیان نمیشود. اما کلیاتی از الگوریتم گراور را بیان میکنیم. ابتدا مسئله را مدل میکنیم. x_0 المان موردنظر است و آرایه هم طول 2^n دارد. ۳-۲

$$f(x) = \begin{cases} 1 & : if x = x_0 \\ 0 & : if x \neq x_0 \end{cases} \qquad (۳-۲)$$

مراحل الگوریتم گراور برای آرایه با طول 2^n: ۳-۵

۱. تعداد n کیوبیت با حالت صفر برمیداریم

۲. گیت هادامار n تایی به رویشان اعمال میکنیم و کیوبیت‌ها را به حالت برهم‌نهی میبریم.

۳. این مراحل را $\sqrt{2^n}$ بار تکرار میکنیم

(آ) عملیات معکوس کردن فاز را انجام میدهیم: $U_f(I \otimes H)$

(ب) عملیات معکوس میانگین را انجام میدهیم: $-I + 2A$

۴. کیوبیت‌ها را اندازه‌گیری میکنیم.

[۶]

[4] Grover's algorithm

۳-۳ الگوریتم شور

در سال ۱۹۹۴، پیتر شور [۵] با الهام از الگوریتم سایمون [۶] یک الگوریتم فاکتورگیری کوانتومی با پیچیدگی زمانی چندجمله ای خلق کرد. از سال ۱۹۷۰، محققان به دنبال الگوریتم‌های فاکتورگیری سریع‌تر هستند. پیچیدگی زمانی یک فاکتور مهم در سیستم‌های رمزنگاری است. [۴]
بیشتر امنیت شبکه اینترنت بر مبنای پیچیدگی فاکتورگیری اعداد صحیح توسط کامپیوتر کلاسیک است. الگوریتم شور، به دلیل اهمیت و حساسیت زیاد باعث شد به حوزه محاسبات کوانتومی توجه بیشتری شود. [۶]
بهترین الگوریتم فاکتورگیری دارای پیچیدگی زمانی

$$O(e^{cn^{1/3}\log^{2/3} n}) \tag{۳-۳}$$

($n = log_2 N$ و N عددی است که میخواهیم فاکتورگیری کنیم) است. این درحالی است که پیچیدگی زمانی الگوریتم شور،

$$O(n^2 \log n \log\log n) \tag{۴-۳}$$

است. که نسبت به n چندجمله‌ای است. [۴]
الگوریتم شور بر اساس یک حقیقت خلق شده است: مسئله فاکتورگیری را به مسئله یافتن تناوب یک تابع تبدیل کرد. [۶] شور برای پیدا کردن تناوب یک تابع از تبدیل فوریر کوانتومی [۷] بهره‌گیری میکند. همچنین، از توازی کوانتومی [۸] برای ایجاد برهم‌نهی از تمام جواب‌های تناوب تابع استفاده میکند. در برخی از قدم‌های این الگوریتم، از محاسبات کلاسیک هم استفاده میشود. [۴]

[5] Peter Shor
[6] Simon's algorithm
[7] quantum Frourier transformation
[8] quantum parallelism

فصل چهارم

موارد استفاده محاسبات کوانتومی

کامپیوترهای کوانتومی، نه تنها از کامپیوترهای امروزی میتوانند سریع‌تر و کوچک‌تر باشند، بلکه یک نوع محاسبات بنیادین جدید ارائه میدهند. این کامپیوترها راه حل احتمالی پس از دوران قانون مور و جایگزین معماری فون-نیومن [1] هستند. [۲]
کامپیوترهای کوانتومی همه کارها را سریعتر از کامپیوترهای کلاسیک انجام میدهند چرا که تغییر ذرات در این کامپیوترها بسیار سریع‌تر از تغییر در ترانزیستورهای پردازنده کلاسیک است. زمانی که کیوبیت در حالت برهم‌نهی است، تعداد عملیاتی که در یک زمان واحد میتواند انجام دهد، به صورت نمایی از تعداد عملیات در کامپیوتر کلاسیک بیشتر است. دومین برتری کامپیوترهای کوانتومی در این است که در حل محاسبات کلاسیک و کوانتومی به یک اندازه قوی است.
با کامپیوتر کوانتومی میتوان تحقیقات پزشکی را تسریع بخشید و به دنبال آن صنعت شیمی پیشرفت میکند. آنها این توانایی را دارند که در زمینه پنهان شدن از رادار و رمزنگاری و پیشبینی آب و هوا باعث پیشرفت های چشمگیری شوند. در بازارهای بورسی و موتور جستجوی گوگل هم میتوانند استفاده شوند.
به طور کلی، کامپیوترهای کوانتومی در هر زمینه حرفی برای گفتن دارند. [۴] در این بخش، تعدادی از زمینه‌هایی که در آنها کامپیوترهای کوانتومی تاثیر زیادی میتوانند داشته باشند را بررسی میکنیم.

۴-۱ رمزنگاری کوانتومی

رمزنگاری‌های امروزی بر پایه مسائل ریاضی بنا شده اند. هنگامی که بتوان یک راه کارآمد و با سرعت برای حل کردن این مسائل بدست‌آورد، داده‌ها دیگر امن نخواهند بود.
مهمترین و پیشبینی‌شده ترین استفاده از کوانتوم در از بین بردن امنیت تمام کلیدهای عمومی [2] که امروزه استفاده میشود، است. این کار با الگوریتم شور امکان‌پذیر خواهد بود. میتوان یک روش تولید کلید کوانتومی تعریف کرد که به محض تلاش برای خرابکاری یا دسترسی به داده، حالت خود را تغییر دهد. در واقع این الگوریتم با استفاده از خاصیت درهم‌تنیدگی، یکی از امکانات جدیدی که رمزنگاری کوانتومی فراهم میکند، بهره‌گیری از موقعیت مکانی -با استفاده از درهم تنیدگی مکانی- برای احراز هویت است. [۲] [۵]

۴-۲ شبیه‌سازی فیزیک کوانتوم

هنگام شبیه‌سازی های کوانتومی بر روی یک کامپیوتر کلاسیک، دچار رشد نمایی داده و محاسبیات میشویم تا حدی که برخی شبیه‌سازی با قدرتمندترین کامپیوتر ها نیز نمیتوانند انجام شوند. ریچارد فاینمن [3] ، فیزیکدان شناخته شده، در راستای همین زمینه، توانایی کامپیوتر های کوانتومی برای محاسبات موازی را مورد پرسش قرارداد. فاینمن اولین نفری بود که برتری کامپیوترهای کوانتومی به کلاسیک را بیان کرد. او معتقد بود، تنها یک کامپیوتر کوانتومی میتواند فیزیک کوانتوم را به طور کارآمد، شبیه‌سازی کند.
ایده شبیه‌سازی کوانتومی بر این اساس است که از یک سیستم کوانتومی کنترل‌شده برای شبیه‌سازی یک سیستم کوانتومی دیگر استفاده کرد. کامپیوترهای کوانتومی مسیر پیشرفت طولانی‌ای را برای رسیدن

[1] von Neumann
[2] public key
[3] Richard Feynman

به حالتی که توانایی مسائل روز کوانتومی، در زمینه‌هایی نظیر ساخت دارو، شیمی و زیست و فیزیک، را شبیه‌سازی کنند دارند اما در حال پیشرفت روزافزون هستند. [۵]

۴-۳ ترابرد کوانتومی

ترابرد [۴] ایده‌ای است که در فیلم‌های علمی-تخیلی میتوان مشاهده کرد. اما این کار در دنیای فیزیک کوانتوم ممکن است. با استفاده از الگوریتم بل [۵] میتوان یک حالت کوانتومی را جابجا کرد بدون اینکه لازم باشد حالت تکان بخورد. اما مشکل این الگوریتم در این است که دو طرف باید باهم یک ارتباط دیگر خارج از کوانتوم هم داشته باشند، مثلا تلفن یا ایمیل. به طور کلی، این الگوریتم از دو بخش تشکیل شده که هر دو طرف باید انجام دهند:

۱. انجام عملیات کوانتومی محلی [۶] بر روی کیوبیت خودشان

۲. انتقال داده‌های اندازه‌گیری‌شده توسط روش‌های ارتباطی کلاسیک

[۴]

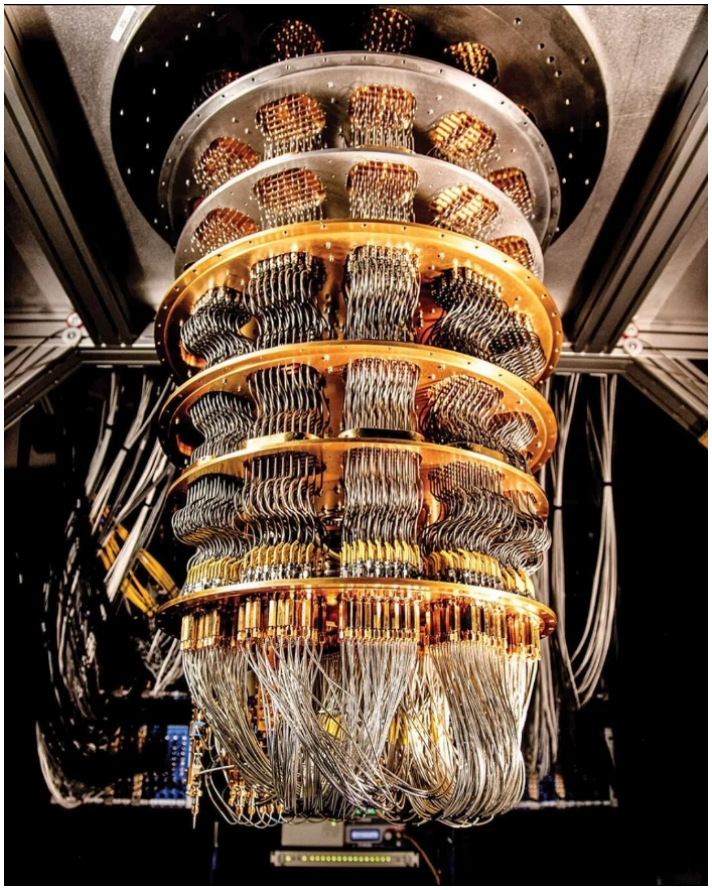
[4] Teleportation

[5] Bell's algorithm

[6] local

فصل پنجم

چالش‌ها و محدودیت‌های محاسبات کوانتومی



شکل ۵-۱: تصویر کامپیوتر کوانتومی شرکت گوگل با ظرفیت ۷۰ کیوبیت

بزرگترین نکته منفی کامپیوتر کوانتومی قیمت زیاد آن است. شرکت های کوچک توانایی پرداخت هزینه این ماشین را ندارند. همچنین، در حال حاضر زیرساخت‌های ساختن کامپیوتر کوانتومی بسیار کم هستند چرا که بخش مهمی از محاسبات کوانتومی، الکترون، به راحتی توسط محیطش آسیب میبیند.
تحقیقات جدید نشان داده اند که تمام کامپیوترهای کلاسیک، حتی کدهای اتمی نسبت به کامپیوترهای کوانتومی آسیب‌پذیر خواهدبود. در نتیجه باید مراقب بود که این فناوری به دست سودجویان نرسد.
برای اینکه این فناوری به حداکثر ظرفیت خود برسد، باید مجموعه ای از الگوریتم‌های بدیع و مخصوص آن را پشتیبانی کنند. بدون الگوریتم های کوانتومی، کامپیوترهای کوانتومی نسبت به کامپیوترهای کلاسیک برتری نخواهند داشت.
چند شرکت بزرگ ادعا دارند که کامپیوتر کوانتومی ساخته‌اند. IBM و Wave D در صدر این شرکت‌ها قراردارند. اما اگر حتی کامپیوترهای کوانتومی ساخته شوند، ما از دانش استفاده موثر از آنها برخوردار نیستیم.
بخش بزرگی از مسائل توسط کامپیوترهای کلاسیک میتوانند حل شوند و استفاده از کامپیوتر کوانتومی برای آنها، منطقی نیست. کامپیوترهای کوانتومی و دانش استفاده از آنها باید تا حدی پیشرفت کند که بتوان مسائل غیرقابل حل در کامپیوترهای کلاسیک را با آنها حل کرد.
کامپیوترهای کوانتومی باید در دمای بسیار پایین $460^{\circ}C$ نگهداری شوند که بسیار نزدیک به صفر مطلق است. در غیر این صورت، کارآیی نخواهند داشت. [۴]

فصل ششم

جمع‌بندی و نتیجه‌گیری

تا سی سال آینده، قانون مور به انتها میرسد و پردازنده‌های کلاسیک به پایان پیشرفت خود میرسند. همچنین، بسیاری از مسائل پیچیده را نمیتوان با کامپیوترهای کلاسیک حل کرد. این باعث رویکرد دانشمندان و صنعت به نوع جدید از کامپیوترها، کامپیوترهای کوانتومی شده‌است.
کامپیوترهای کوانتومی به‌وسیله تغییر حالت ذرات کوانتومی کار میکنند. آنها از خواص دنیای کوانتوم نظیر برهم‌نهی و درهم‌تنیدگی و توازی کوانتومی بهره میبرند. آنها نسبت به کامپیوترهای کلاسیک سرعت بیشتر و قابلیت ذخیره اطلاعات بیشتری دارند.
الگوریتم‌های قدرتمند کوانتومی سالهاست که طراحی شده‌اند و اگر بتوان آنها را به مرحله اجرا رساند، تمام ساختارهای امنیتی کنونی که بر اساس محاسبات کلاسیک است، فروپاشی میکند. اما با این حال تعداد این الگوریتم ها بسیار کم است و برای استفاده از تمام ظرفیت کامپیوترهای کوانتومی به الگوریتم‌های بیشتری نیاز است. این الگوریتم‌ها باید بتوانند مسائلی که با کامپیوترهای کلاسیک قابل حل نیستند، را حل کنند. ما در حال حاضر دانش کافی برای بکارگیری موثر از کامپیوتر کوانتومی برخوردار نیستیم.
بزرگترین کامپیوترهای کوانتومی که تاکنون ساخته‌شده‌اند بسیار گران بوده و همچنین ظرفیتشان آنقدر کم است که نمیتوان مسائل بزرگ را با آنها حل کرد. همچنین، تعداد این کامپیوتر ها کم است و شرایط نگهداری سختی دارند.
با تمام این نکات، بنظر میرسد کامپیوترهای کوانتومی یک نیاز حتمی برای حل مسائل ناشناخته بشر است و یک الزام برای دنیای آینده است. با اینکه به نظر در مراحل ابتدایی خود به سر میبرد، پیشرفت‌های حاصل در این زمینه چشمگیر بوده و به صورت روزافزون، توجه بیشتری جلب میکند.

کتاب‌نامه

[1] Arute, F. et al. Quantum supremacy using a programmable superconducting processor. Nature, 547(7779):505–510, 2019.

[2] Bhat, Hilal Ahmad, Khanday, Farooq Ahmad, and Kaushik. Quantum computing: Fundamentals, implementations and applications. IEEE Open Journal of Nanotechnology, 3:61–77, 2022.

[3] Devoret, M.H. and Schoelkopf, R.J. Superconducting circuits for quantum information: an outlook. Science, 339(6124):1169–1174, 2013.

[4] Kuldeep Singh Kaswan, Jagjit Singh Dhatterwal. Quantum Computing: A New Era of Computing. Wiley-IEEE Press, 2023.

[5] Swan, Melanie, Witte, Frank, and dos Santos, Renato P. Quantum information science. IEEE Internet Computing, 26(1):7–14, 2022.

[6] Yanofsky, Noson S. and Mannucci, Mirco A. Quantum Computing for Computer Scientists. Cambridge University Press, 2008.