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 الرحیم

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

شکل — # فهرست تصاویر — صفحه

فهرست جداول

جدول صفحه

فهرست نمادها

نماد	مفهوم
$\mathbb{R}^n$	فضای اقلیدسی با بعد n
$\mathbb{S}^n$	کره یکه n بعدی
M^m	خمینه m-بعدی M
$\mathfrak{X}(M)$	جبر میدان‌های برداری هموار روی M
$\mathfrak{X}^1(M)$	مجموعه میدان‌های برداری هموار یکه روی (M, g)
$\Omega^p(M)$	مجموعه p-فرمی‌های روی خمینه M
Q	اپراتور ریچی
$\mathcal{R}$	تانسور انحنای ریمان
ric	تانسور ریچی
L	مشتق لی
Φ	۲-فرم اساسی خمینه تماسی
∇	التصاق لوی-چویتای
Δ	لاپلاسین ناهموار
∇^*	عملگر خودالحاق صوری القا شده از التصاق لوی-چویتای
g_s	متر ساساکی
∇	التصاق لوی-چویتای وابسته به متر ساساکی
Δ	عملگر لاپلاس-بلترامی روی p-فرم‌ها

فصل اول

مقدمه

بر اساس قانون مور [1] قدرت پردازنده های کامپیوتر های کلاسیک هر دو سال، دو برابر میشود. اما این رویه تا حدی ادامه خواهد داشت که محدودیت های دنیای فیزیک کلاسیک به آن اجازه دهند. چرا که اندازه ی اعضای تشکیل دهنده ی پردازنده ها به حدی کوچک میشود که ناخودآگاه وارد فضای کوچک کوانتوم [2] میشوند. پیشبینی میشود این اتفاق در سال ۲۰۵۰ رخ دهد.
پیچیدگی محاسباتی [3] برخی الگوریتم ها در کامپیوتر های 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 الگوریتم ها را کاهش دهند. [۳] به طور کلی، محاسبات کوانتومی از کنش و واکنش مواد در جهان در سطح ذرات تشکیل دهنده ی آن بهره میگیرد و بر روی بستر پدیده ی نسبیت خاص [4] 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 [5] که مسائلی هستند که برای پیدا کردن حالت بهینه با توجه به متغیر های مختلف است، کامپیوتر های 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 خوزه ها وجود دارند و کامپیوتر های کوانتومی برای اجرای این الگوریتم ها بسیار مناسب هستند. [۴]

[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

کیوبیت ها [۱] در کامپیوتر های کوانتومی، معادل بیت ها [۲] در کامپیوتر های کلاسیک هستند. یک بیت یا در حالت صفر قرار دارد یا در حالت یک قرار دارد. تفاوت کیوبیت ها 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.

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

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

$$\alpha^2 + \beta^2 = 1 \quad (۲-۲)$$

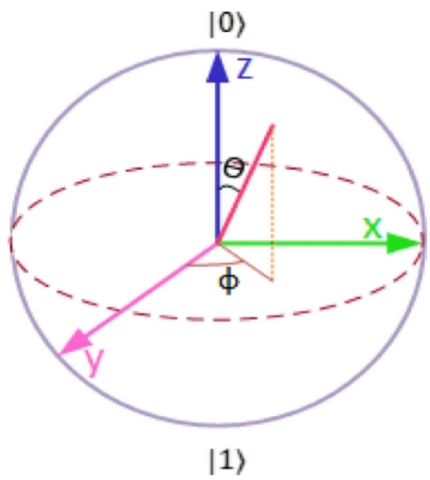
فضای حالتی که این دو متغیر تشکیل میدهند، یک فضای مختلط دو بعدی است. حالات خاص صفر و یک، یک فضای بردار پایه ای [۴] برای این فضای برداری تشکیل میدهند.

$$|0\rangle = (0,1) and\,|1\rangle = (1,0) \quad (۲-۳)$$

در شکل پایین، میتوانید کره ی 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 آن ها را جدا کرد. [۱] همچنان جمع مجذور همه ی مقادیر باید برابر با یک شود. نمایش انتزاعی دو کیوبیت به شکل زیر خواهد بود:

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

[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] :

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

۲-۲ ضرب تانسوری

ضرب تانسوری [۸] ، عملیاتی است که بین دو ماتریس میتوان انجام داد. این عملیات، یکی از بخش های اصلی محاسبات کوانتومی است. برای اینکه بتوان سیستم های 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. [۱] این ضرب را میتوان با یک گیت کوانتومی [۱۰] اعمال کرد.

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

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

$$M \oplus N = \begin{bmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{bmatrix} \tag{۲-۷}$$

برای ضرب تانسوری دو کیوبیت خواهیم داشت:

$$|0\rangle \oplus |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = |01\rangle \tag{۲-۸}$$

۲-۳ اصل برهم‌نهی

در دنیای روزمره، همه ی 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 ی 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 چالش های محاسبات کوانتومی، مشاهده نکردن کیوبیت ها در طول فرآیند است. کیوبیت ها تنها در آخرین مرحله ی الگوریتم باید مشاهده شوند. [۲]

۲-۴ اصل درهم‌تنیدگی

کیوبیت ها 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 ی 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 خواهندماند. نمایش ریاضی درهم‌تنیدگی زمانی است که نتوان حالت شامل چند کیوبیت را به ضرب تانسوری آن کیوبیت ها تبدیل کرد. در واقع ضربی وجود نخواهد داشت که آن حالت نهایی را درست کند. درهم‌تنیدگی را میتوان با استفاده از گیت های کوانتومی انجام داد. درهم‌تنیدگی در حوزه رمزنگاری و انتقال داده استفاده بخصوص دارد. [۲]

[11] spin
[12] entanglement

۲-۵ برگشت‌پذیری و گیت های 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 مدار های کوانتومی هستند. گیت‌های پایه و لازم کوانتومی شامل H, X, Y, Z, T, I و گیت فاز [۱۴] میباشد. همچنین گیت های 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. [۱]

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 گیت های کوانتومی

[13] reversible calculation
[14] phase gate

کتاب‌نامه

[1] Bhat, Hilal Ahmad, Khanday, Farooq Ahmad, Kaushik, Brajesh Kumar, Bashir, Faisal, and Shah, Khurshed Ahmad. Quantum computing: Fundamentals, implementations and applications. IEEE Open Journal of Nanotechnology, 3:61–77, 2022.

[2] Bhat, Hilal Ahmad, Khanday, Farooq Ahmad, Kaushik, Brajesh Kumar, Bashir, Faisal, and Shah, Khurshed Ahmad. Quantum Computing: Fundamentals, Implementations and Applications, vol. 3. 2022.

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

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