وضعیت فعلی فناوری در رایانش کوانتومی

سلمان ابوالفتح بیگی

۳ خرداد ۱۴۰۵

چکیده

رایانش کوانتومی یکی از حوزه‌های نوین در علوم محاسباتی به‌شمار می‌رود. با این‌حال، بسیاری از مطالبی که در این زمینه به زبان فارسی در دسترس هستند، از دقت کافی برخوردار نیستند. این بی‌دقتی‌ها عمدتاً ناشی از ترجمه‌های ناقص یا غیردقیق متون انگلیسی هستند که خود نیز لزوماً منابع معتبری به حساب نمی‌آیند. متأسفانه، به‌نظر می‌رسد که استراتژی توسعه‌ی فناوری کوانتومی در کشور نیز متأثر از این اطلاعات نادقیق است. این نوشتار تلاشی است در راستای ارائه‌ی تصویری روشن‌تر و دقیق‌تر از رایانش کوانتومی در عصر حاضر.

در این نوشتار، نخست جایگاه محاسبات کوانتومی را در قیاس با رایانش کلاسیک توصیف می‌کنیم. سپس به مسائلی می‌پردازیم که رایانه‌های کوانتومی احتمالاً در حل آنها نسبت به رایانه‌های کلاسیک برتری دارند. در ادامه، چالش‌های پیشِ روی ساخت رایانه‌های کوانتومی را بررسی می‌کنیم و در پایان، نکاتی را درباره‌ی استراتژی توسعه‌ی فناوری کوانتومی در کشور بیان می‌کنیم.

فهرست مطالب

۱ محاسبه و فیزیک

محاسبه فرآیندی گام به گام است برای حل مسأله‌ای مشخص براساس دنباله‌ای از عملیات‌های ریاضی یا منطقیِ ساده‌ی از پیش تعریف‌شده. به عنوان مثال برای جمع کردن دو عدد، ابتدا رقم یکان آنها را جمع و قانون «ده بر یک» را رعایت می‌کنیم و سپس این گام‌ها را به ترتیب روی ارقام دیگر مانند دهگان و صدگان اعمال می‌کنیم. در این فرآیند، مسأله‌ی پیدا کردن حاصل‌جمع دو عدد به دنباله‌ای از عملیات‌های ساده‌ی جمع اعداد تک‌رقمی کاهش پیدا می‌کند.

ماشین تورینگ[1] یک مدل ریاضیِ انتزاعی است که توصیف غیررسمی فوق از مفهوم محاسبه را به صورت صوری بیان می‌کند. ماشین تورینگ در سال ۱۹۳۶ توسط آلن تورینگ[2] معرفی شد و در حال حاضر به عنوان استانداردی از مفهوم محاسبه پذیرفته شده است، به این معنی که هر محاسبه‌ای را می‌توان با یک ماشین تورینگ مدل‌سازی کرد. بنا بر تز چرچ-تورینگ[3] هر آنچه که محاسبه‌پذیر است را می‌توان روی یک ماشین تورینگ پیاده‌سازی کرد. ماشین تورینگ نه تنها برای مطالعه‌ی مفهوم محاسبه‌پذیری، بلکه به عنوان ابزاری برای مطالعه‌ی پیچیده‌گی محاسباتی[4] و

[1] Turing machine
[2] Alan Turing
[3] Church–Turing thesis
[4] Computational complexity

کشف محدودیت‌های محاسبه مورد استفاده قرار می‌گیرد.

۱.۱ اجزای یک کوامپیوتر

کامپیوتر یا رایانه، دستگاهی است که محاسبه را به فرآیندی خودکار و ماشینی تبدیل می‌کند. به عبارت دیگر، رایانه مدل انتزاعیِ ماشین تورینگ را محقق کرده و در دسترس قرار می‌دهد. ماشین حساب پاسکال (پاسکالین) ساخته شده در سال ۱۶۴۲ یکی از اولین ماشین‌های محاسبه است که البته قدرت محاسباتی کامل یک ماشین تورینگ را ندارد، و در واقع یک ماشین حساب است که فقط قابلیت جمع و تفریق اعداد را دارد. با این حال به عنوان اولین دستگاهی که محاسبه را ماشینی می‌کند حائز اهمیت است. رایانه‌های امروزی قدرت محاسباتی کامل یک ماشین تورینگ را دارا هستند.

ماشین حساب پاسکال از تعداد زیادی چرخ‌دنده ساخته شده بود و رایانه‌های امروزی از ادوات الکترونیکی. بنیان فیزیکیِ ماشین حساب پاسکال، نظریه‌ی مکانیک کلاسیک است و رایانه‌های امروزی با استفاده از علوم الکترونیک و الکترومغناطیس کلاسیک ساخته شده‌اند. در اینجا تأکید می‌کنیم که گرچه ماشین حساب پاسکال و کامپیوترهای امروزی از لحاظ قدرت محاسباتی و سرعت کاملاً متفاوت هستند، هر دو براساس فیزیک کلاسیک (مکانیک یا الکترونیک) ساخته شده‌اند و از این نظر مشابهت دارند.

۲.۱ فیزیک کوانتومی، نظریه‌ای متفاوت

اوایل قرن گذشته شاهد ظهور ایده‌هایی کاملاً متفاوت در مطالعه‌ی پدیده‌های فیزیکی بودیم. مکانیک کلاسیک با فرمول‌بندی نیوتن، و قوانین الکترومغناطیس کلاسیک با فرمول‌بندی ماکسوِل تا اواخر قرن ۱۹ به بلوغ رسیده بودند. با این حال پدیده‌هایی وجود داشتند که فیزیک کلاسیک توصیف قابل قبولی برای آنها ارائه نمی‌داد. یکی از این پدیده‌ها مسأله تابش جسم سیاه[۵] بود. پلانک در سال ۱۹۰۰ با فرضی عجیب توصیفی از این پدیده ارائه داد که با نتایج آزمایشگاهی آن سازگار بود. فرض پلانک این بود که انرژی برخلاف شهود ما از طبیعت، کمیتی گسسته است و فقط می‌تواند مقادیر مشخصی را اتخاذ کند. اینشتین در آن زمان فیزیک‌دانی جوان بود و ایده‌ی پلانک را در حل مسأله‌ی اثر فوتوالکتریک به کار برد که یکی دیگر از مسائل چالش برانگیز آن دوران بود. اینشتین در سال ۱۹۰۵ فرض کرد که نور ماهیتی گسسته دارد و از ذراتی تشکیل شده است که آنها را فوتون نامید. فرض اینشتین برخلاف تلقی کلاسیک از نور بود که ماهیت آن را موج می‌دانست.

ایده‌های پلانک و اینشتین در دهه‌های بعد توسط فیزیک‌دانان مختلفی از جمله بور،[۶] هایزنبرگ[۷] و شرودینگر[۸] پیگیری و در دهه‌ی ۱۹۲۰ منجر به پدید آمدن نظریه‌ی فیزیک کوانتومی شد. لازم به ذکر است که فیزیک کوانتومی نظریه‌ای در عرض مکانیک نیوتونی یا الکترومغناطیس کلاسیک نیست. فیزیک کوانتومی توصیفی کاملاً متفاوت از طبیعت ارائه می‌دهد و با درک و شهود کلاسیک ما چندان سازگار نیست. با این حال پدیده‌های زیادی که توسط فیزیک کلاسیک قابل توصیف نیستند، توسط فیزیک کوانتومی به خوبی توضیح داده می‌شوند.

[5] Black body radiation
[6] Niels Bohr
[7] Werner Heisenberg
[8] Erwin Schrödinger

۳.۱ آزمایش دو-شکاف

آزمایش دو-شکاف[۹] برخی از ویژگی‌های فیزیک کوانتومی و تفاوت آن با فیزیک کلاسیک را به خوبی آشکار می‌کند. در این آزمایش مطابق شکل ۱ از یک منبع، ذراتی یکسان به سمت دیواری پرتاب می‌شوند. روی دیوار دو شکاف وجود دارد و پشت دیوار یک پرده‌ی آشکارساز که برخورد ذراتی که از شکاف‌ها عبور کرده و به پرده برخورد می‌کنند را نمایان می‌کند. البته که در اینجا برای سادگی و تمرکز بر اصل ماجرا از جزئیات و پیچیدگی‌های آزمایش دو-شکاف از جمله نوع منبع و ذرات مورد استفاده صرف نظر شده است.

در آزمایش دو-شکاف ابتدا شکاف دوم را می‌پوشانیم به طوری که ذرات فقط بتوانند از شکاف اول عبور کنند، و در این حالت توزیع مکانی ذراتی که به پرده برخورد می‌کنند را ثبت می‌کنیم. انتظار داریم که چگالی ذرات روی پرده، روبروی شکاف اول بیشترین مقدار را داشته باشد و هرچه دور می‌شویم چگالی کمتر شود. این شهود با نتیجه آزمایش نیز سازگار است و همان‌طور که در شکل ۱(الف) دیده می‌شود نمودار چگالی فرمی زنگوله‌وار پیدا کرده و بیشترین مقدار را روبروی شکاف اول اخذ می‌کند.

می‌توانیم آزمایش را با پوشاندن شکاف اول و باز کردن شکاف دوم تکرار کنیم. در این صورت نتیجه آزمایش اول تکرار می‌شود با این تفاوت که مطابق شکل ۱(ب) چگالی ذرات روبروی شکاف دوم بیشتر خواهد بود.

برای آزمایش سوم هر دو شکاف را باز می‌گذاریم. در این حالت ذره‌ای که به پرده برخورد می‌کند یا از شکاف اول عبور می‌کند و یا از شکاف دوم. در نتیجه انتظار داریم که چگالی ذرات روبری این دو شکاف از جاهای دیگر بیشتر باشد. در واقع انتظار داریم که مطابق شکل ۱(د) نمودار چگالی برابر میانگین نمودار چگالی‌ها در آزمایش‌های اول و دوم باشد. با این حال نتیجه‌ی آزمایش کاملاً متفاوت از شهود ما و مطابق شکل ۱(ج) خواهد بود. شگفت‌آور است که در این حالت چگالی ذرات نه روبری شکاف‌ها، بلکه بین آنها بیشترین مقدار را دارد. به علاوه، نمودار چگالی حالتی سینوسی دارد که با شهود ما ناسازگار است.

بگذارید استدلال خود برای پیش‌بینی نتیجه‌ی آزمایش سوم را مرور کنیم. هر ذره‌ای که به پرده برخورد می‌کند یا از شکاف اول عبور کرده، یا از شکاف دوم. اگر از شکاف اول عبور کرده باشد، گویی برای آن ذره شکاف دوم پوشانده شده و در چینش آزمایش اول قرار داریم. در این صورت برای چنین ذراتی باید چگالی آزمایش اول را ببینیم. به همین ترتیب، برای ذراتی که از شکاف دوم عبور می‌کنند باید چگالی آزمایش دوم را ببینیم. حال از آنجایی که نمی‌دانیم هر ذره از کدام شکاف عبور کرده، انتظار داریم که میانگین نمودارهای آزمایش اول و دوم را مشاهده کنیم.

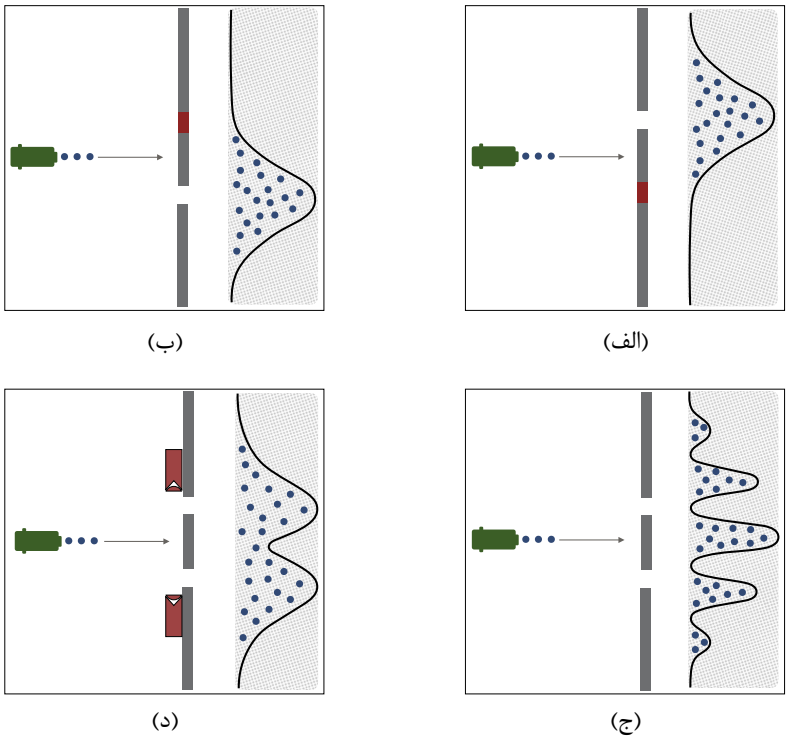
برای آزمودن استدلال فوق یک آشکارساز جدید به چینش آزمایش اضافه می‌کنیم. این آشکارساز را کنار شکاف‌ها قرار می‌دهیم تا مشخص کند که هر ذره از شکاف اول عبور می‌کند یا از شکاف دوم، و سپس آزمایش را تکرار می‌کنیم (همانند بالا از پیچیدگی‌های آزمایشگاهی اضافه کردن چنین آشکارسازی صرف نظر می‌کنیم). شگفت اینکه طبق شکل ۱(د) حاصل این آزمایش با آزمایش سوم متفاوت و منطبق با نتیجه استدلال فوق است.

واقعیت این است که فرض اولیه‌ی ما در استدلال فوق برای توصیف آزمایش سوم برقرار نیست. چنین نیست که ذره‌ای که به پرده برخورد می‌کند یا از شکاف اول عبور کرده یا از شکاف دوم. زیرا در آزمایش چهارم وقتی با اضافه کردن آشکارساز جدید این فرض را محقق کردیم، نتیجه آزمایش متفاوت شد. پس در آزمایش سوم حالت ذرات قبل از برخورد به پرده چیزی غیر از عبور از شکاف اول یا عبور از شکاف دوم است!

دو ویژگی بسیار مهم فیزیک کوانتومی براساس آزمایش دو-شکاف قابل توصیف است. ویژگی اول اصل برهم‌نهی[۱۰]

[9] Double-slit experiment

[10] Superposition principle



شکل ۱: آزمایش دو-شکاف: شکل (الف) نتیجه‌ی آزمایش وقتی فقط شکاف اول باز باشد را نمایش می‌دهد و شکل (ب) وقتی فقط شکاف دوم باز باشد. شکل (ج) حاصل آزمایش در حالتی است که هر دو شکاف باز باشند. با اضافه کردن آشکارسازهایی در کنار شکاف‌ها، نتیجه‌ی آزمایش مطابق شکل (د) است.

است که در رابطه با آزمایش فوق بیان می‌کند که حالت ذره می‌تواند عبور از شکاف اول، عبور از شکاف دوم یا برهم‌نهی آن دو باشد. عبور از شکاف اول یا دوم، دو حالت کلاسیک این سیستم فیزیکی هستند که با شهود ما نیز کاملاً سازگار هستند و در اینجا برهم‌نهی صرفاً به معنی حالتی غیر از دو این حالت کلاسیک است.

ویژگی دوم در رابطه با اندازه‌گیری است. در فیزیک کلاسیک اندازه‌گیری یک سیستم فیزیکی (حداقل به طور اصولی) حالت آن را تغییر نمی‌دهد، ولی در فیزیک کوانتومی چنین نیست. در آزمایش چهارم دیدیم که با اضافه کردن آشکارساز جدید که محل عبور ذرات را اندازه‌گیری می‌کرد، حاصل آزمایش و در واقع حالت ذرات عوض شد. قبل از اندازه‌گیری، ذرات در حالت برهم‌نهی بودند و بعد از اندازه‌گیری، آنها در یکی از دو حالت کلاسیک قرار گرفتند.

۴.۱ ناممکن بودن همانندسازی کوانتومی

از دیگر ویژگی‌ها و در واقع نتایج فیزیک کوانتومی، ناممکن بودن همانندسازی است. در دنیای کلاسیک حالت یک سیستم فیزیکی قابل کپی‌برداری است. برای مثال فایل‌های کامپیوتری را می‌توان کپی کرد. همچنین از هر سند کاغذی می‌توان کپی گرفت. فرآیندِ کپی کردن هم مستقل از محتوای فایل کامپیوتری یا محتوای سند است. ولی چنین کاری در فیزیک کوانتومی امکان‌پذیر نیست. هیچ فرآیندی نیست که بتواند حالت یک سیستم کوانتومی را،

بدون دانستن آن حالت، کپی کند. این ویژگی را «ناممکن بودن همانندسازی کوانتومی»[11] گویند.

۵.۱ فیزیک جدید، مدل محاسباتی جدید

دیدیم که محاسبه فرآیندی گام به گام براساس دنباله‌ای از عملیات‌های ساده است. حال سؤال این است که آیا می‌توان این عملیات ساده را براساس ویژگی‌های فیزیک کوانتومی تعریف کرد؟ آیا این تعریف جدید تأثیری در مفهوم محاسبه دارد؟

واقعیت این است که مفهوم محاسبه در حضور فیزیک کوانتومی تغییر نمی‌کند و ماشین تورینگ همچنان مدل محاسباتی جامعی است که محاسبات مبتنی بر فیزیک کوانتومی را نیز مدل‌سازی می‌کند. نکته در این است که فرضیات فیزیک کوانتومی، خود براساس مفاهیم ریاضی فرمول‌بندی می‌شوند و محاسبات ریاضی همگی قابل توصیف با ماشین تورینگ هستند. لذا فیزیک کوانتومی در مفهوم محاسبه و محاسبه‌پذیری تغییری ایجاد نمی‌کند. با این حال ممکن است فیزیک کوانتومی سرعت محاسبات، یا به طور دقیق‌تر، پیچیدگی محاسباتی را تحت تأثیر قرار دهد [۱۰].

در بخش بعدی ابتدا به طور اجمالی به توصیف رایانش کوانتومی می‌پردازیم و سپس مسائلی را معرفی می‌کنیم که پیچیدگی محاسباتی آنها در حضور کامپیوترهای کوانتومی کاهش می‌یابد.

۲ رایانش کوانتومی

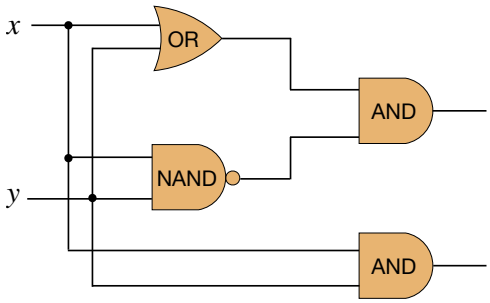
در این بخش ابتدا با توصیف اجزای یک کامپیوتر کوانتومی، نحوه‌ی عملکرد آن را شرح می‌دهیم. سپس کابردهای کامپیوترهای کوانتومی را توضیح می‌دهیم و به الگوریتم‌هایی کوانتومی اشاره می‌کنیم که پیچیدگی محاسباتی بعضی از مسائل را در مقایسه‌ی با کامپیوترهای کلاسیک کاهش می‌دهند.

۱.۲ مدل مداری کوانتومی

برای فهمیدن نحوه‌ی علمکرد یک کامپیوتر کوانتومی بهتر است ابتدا با مدل محاسباتی مداریِ کلاسیک آشنا شویم. فرض کنید می‌خواهیم حاصل‌جمع دو عدد را محاسبه کنیم. در این مسأله ورودی، دو عدد و خروجی، حاصل‌جمع آنها است. معمولاً در کامپیوترها برای ذخیره‌ی اعداد از نمایش دودویی استفاده می‌شود. لذا ورودی مسأله دو دنباله از ۰، ۱ است. به هر خانه‌ی حافظه در یک کامپیوتر که می‌تواند یکی از ارقام ۰ یا ۱ را ذخیره کند یک بیت[12] گفته می‌شود. بنابراین، اگر بخواهیم حاصل‌جمع دو عدد را بیابیم که نمایش دودویی هر یک از آنها شامل n بیت است، مسأله ما $2n$ بیت ورودی دارد، و برای خروجی به $n+1$ بیت نیاز داریم (زیرا ممکن است برای نمایش حاصل‌جمع به ارقام بیشتری احتیاج پیدا کنیم).

در اینجا برای معرفیِ مدل مداری، فرض می‌کنیم که می‌خواهیم مجموع دو عدد تک‌بیتی را محاسبه کنیم. برای این کار می‌توان از مدار شکل ۲ استفاده کرد. در این شکل دو عدد ورودیِ تک‌بیتی در سمت چپ مدار با x, y مشخص شده‌اند. این دو بیت از سمت چپ به راست وارد گِیت‌های منطقی[13] مختلفی می‌شوند. خروجی این گیت‌ها یا به عنوان

[11] Quantum no-cloning
[12] Bit
[13] Logical gates



شکل ۲: مداری کلاسیک که جمع دو بیت ورودی x, y را با استفاده از گیت‌های منطقی AND, OR, NAND محاسبه می‌کند.

خروجی مدار و یا به عنوان ورودی گیت‌های بعدی در نظر گرفته می‌شوند تا اینکه خروجی نهایی مدار مشخص شود.

در حالت کلی، یک مدار دارای بیت‌های ورودی و خروجی، و گیت‌های منطقی است. ورودی مسأله مقادیر بیت‌های ورودی را مشخص می‌کند. سپس با اعمال دنباله‌ای از گیت‌ها، خروجی مدار به عنوان حاصل محاسبات مشخص می‌شود.

مدل مداری، معادل با مدل محاسباتی ماشین تورینگ است. به این معنا که به ازای هر ماشین تورینگ و طول ورودی داده شده، مداری وجود دارد که عملکردی دقیقاً مشابه عملکرد ماشین تورینگ دارد.

حال می‌توانیم به توصیف مدل مداری کوانتومی بپردازیم. بیت‌های کوانتومی که برای اختصار کیوبیت[۱۴] نامیده می‌شوند، اولین اجزای چنین مداری هستند. براساس اصل برهم‌نهی که در بالا به آن اشاره شد، یک کیوبیت می‌تواند در حالت ۰، ۱ یا برهم‌نهی آنها قرار گیرد. لذا فضای حالات بیت‌های کوانتومی بزرگ‌تر از فضای حالات بیت‌های کلاسیک است. معمولاً کیوبیت‌ها در ابتدای محاسبه در حالات ۰ یا ۱ قرار می‌گیرند. ولی در حین محاسبه معمولاً حالت آنها به حالات برهم‌نهی تغییر می‌کند.

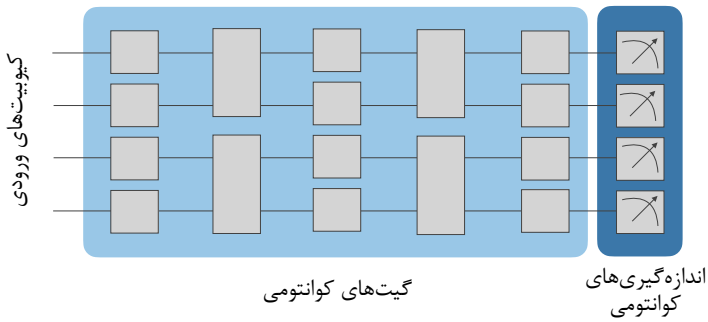
گیت‌های کوانتومی جزء دوم یک مدار کوانتومی هستند. به طور کلی، گیت‌های کلاسیک، توابعی روی مثلاً یک یا دو بیت ورودی هستند که می‌توان آنها را به عنوان دینامیکی کلاسیک روی آن بیت‌ها در نظر گرفت. یک گیت کوانتومی نیز دینامیکی کوانتومی روی کیوبیت‌های ورودی آن است که ساختار ریاضی آن با استفاده از معادله‌ی شرودینگر[۱۵] بدست می‌آید. دنباله‌ای از گیت‌های کوانتومی که روی بیت‌های کوانتومی اعمال می‌شود بخش اصلی یک مدار کوانتومی را تشکیل می‌دهد.

مدارهای کوانتومی یک تفاوت مهم با مدارهای کلاسیک دارند. در مدار شکل ۲ دیدیم که مثلاً بیت ورودی x به عنوان ورودی سه گیت مختلف در نظر گرفته شده است. با این حال با توجه به ناممکن بودن همانندسازی کوانتومی در مدارهای کوانتومی نمی‌توانیم از کیوبیت‌ها کپی بسازیم و آنها را به عنوان ورودی گیت‌های مختلف در نظر بگیریم. به این دلیل مدارهای کوانتومی الگوی ساده‌تری دارند. فرم کلی یک مدار کوانتومی در شکل ۳ نمایش داده شده است.

در توصیف آزمایش دو-شکاف دیدیم که اندازه‌گیری، بخش مهمی از یک آزمایش کوانتومی است. در یک کامپیوتر کوانتومی نیز اندازه‌گیری، حاصل محاسبه را مشخص می‌کند. به همین دلیل، برخلاف مدارهای کلاسیک، در مدارهای کوانتومی مؤلفه‌ی اندازه‌گیری نیز اضافه می‌شود که معمولاً در انتهای مدار قرار می‌گیرد.

حال با فهمیدن ساختار یک مدار کوانتومی می‌توانیم عملکرد یک کامپیوتر کوانتومی را بفهمیم. یک کامپیوتر

[14] Qubit
[15] Schrödinger equation



شکل ۳: در حالت کلی یک مدار کوانتومی شامل کیوبیت‌های ورودی، کیوبیت‌های کمکی و گیت‌های کوانتومیِ تک-کیوبیتی و دو-کیوبیتی است. اندازه‌گیری کوانتومی در انتهای مدار اعمال می‌شود. در این مدار ۵ لایه از گیت‌های کوانتومی به کار برده شده است. بنابراین عمق این مدار ۵ است و زمان اجرای آن ۵ واحد زمان طول می‌کشد.

کوانتومی برای حل یک مسأله ابتدا ورودی یا ورودی‌های مسأله را که با دنباله‌ای از ۰ و ۱ نمایش داده شده‌اند، به عنوان حالات اولیه‌ی کیوبیت‌های ورودی یک مدار کوانتومی قرار می‌دهد. علاوه بر کیوبیت‌های ورودی، ممکن است از کیوبیت‌های دیگری نیز به عنوان کیوبیت کمکی[۱۶] استفاده کند. سپس دنباله‌ای از گیت‌های کوانتومی، مثلاً گیت‌های تک-کیوبیتی و دو-کیوبیتی روی کیوبیت‌های مدار اعمال می‌کند و در انتها با اندازه‌گیری کیوبیت‌ها، خروجی محاسبه را مشخص می‌کند.

۲.۲ کامپیوتر کوانتومی به چه کار می‌آید؟

حال که با عملکرد کلی کامپیوترهای کوانتومی آشنا شدیم می‌توانیم به این سؤال بپردازیم که یک کامپیوتر کوانتومی به چه کار می‌آید. می‌توان نشان داد که کلاس خاصی از مدارهای کوانتومی می‌توانند کارکردی مشابه مدارهای کلاسیک با پیچیدگی محاسباتی یکسان داشته باشند. بنابراین کامپیوترهای کوانتومی، حداقل از دید نظری، توان رایانه‌های کلاسیک را دارند. با این حال، انتظار داریم که در مقایسه با رایانه‌های کلاسیک بتوانیم مسائل بیشتری را با کامپیوترهای کوانتومی حل کنیم.

حل مسائل بیشتر یا یافتن راه حل بهتر برای آنها با استفاده از کامپیوترهای کوانتومی، برتری کوانتومی[۱۷] نامیده می‌شود. برتری کوانتومی به طور نظری ثابت شده است ولی پیاده‌سازی عملی آن مورد مناقشه است. نکته‌ی بعدی در این رابطه مفید بودن برتری کوانتومی است چرا که بعضاً ادعاهایی در مورد برتری کوانتومی در مورد مسائلی می‌شود که مصنوعی هستند و کاربرد خاصی ندارند. به همین دلیل گاهی برای مشخص کردن این تفاوت از اصطلاح مزیت کوانتومی[۱۸] استفاده می‌شود که منظور برتری کوانتومی است برای مسائلی که کاربردی هستند.

در ادامه بعضی از مهم‌ترین مسائلی را می‌آوریم که احتمالاً با پیچیدگی محاسباتی کمتر روی کامپیوترهای کوانتومی قابل حل هستند و می‌توانند منجر به مزیت کوانتومی شوند.

❑ **الگوریتم تجزیه‌ی شور:** هر عدد صحیح را می‌توان به صورت حاصل‌ضرب اعداد اول تجزیه کرد، ولی یافتن

[16] Ancillary qubit
[17] Quantum supremacy
[18] Quantum advantage

این تجزیه کار ساده‌ای نیست. در واقع تاکنون حتی برای یافتن یک مقسوم‌علیه از یک عدد داده شده، روش مؤثری بدست نیامده است. یک روش برای یافتن مقسوم‌علیه این است که عدد داده شده را بر همه‌ی اعداد کمتر از آن یکی-یکی تقسیم کنیم تا نهایتاً یک مقسوم‌علیه بیابیم. منتهی این کار بسیار طول می‌کشد و پیچیدگی محاسباتی بالایی دارد.

قابل ذکر است که امنیت یکی از مهم‌ترین سیستم‌های رمزنگاری به نام RSA براساس سختیِ مسأله‌ی تجزیه به عوامل اول است. اگر مسأله‌ی تجزیه را حل کنیم، این سیستم رمزنگاری دیگر قابل اعتماد نخواهد بود. تأکید می‌کنیم که در اینجا منظور تجزیه‌ی اعداد بسیار بزرگ است.

پیتر شور[۱۹] در سال ۱۹۹۴ نشان داد که مسأله‌ی تجزیه به عوامل اول روی یک کامپیوتر کوانتومی قابل حل است [۱۵]. الگوریتم تجزیه‌ی شور براساس حل مسأله‌ی لگاریتم گسسته[۲۰] است. در واقع شور با الگوریتم کوانتومی خود نشان داد که نه تنها سیستم رمزنگاری RSA بلکه بخش اعظمی از سیستم‌های رمزنگاری فعلی که براساس سختی مسأله‌ی لگاریتم گسسته هستند، در حضور کامپیوترهای کوانتومی امنیت خود را از دست می‌دهند.

الگوریتم تجزیه‌ی شور دو پیامد بسیار مهم داشت. اول اینکه توجه محققین به اهمیت کامپیوترهای کوانتومی و کاربردهای آنها بیش از پیش جلب شد. الگوریتم شور نشان داد که رایانش کوانتومی می‌تواند در حل مسائل طبیعی و مهمی چون تجزیه کاربرد عملی داشته باشد. پیامد دوم توجه به امنیت سیستم‌های رمزنگاری در حضور کامپیوترهای کوانتومی بود. بعد از الگوریتم شور، یافتن سیستم‌های رمزنگاری که در حضور کامپیوترهای کوانتومی نیز امن باشند اهمیت وافری پیدا کرد. این مسأله منجر به توسعه دادن زمینه‌ی تحقیقاتی جدیدی با عنوان رمزنگاری پساکوانتومی[۲۱] شد.

- **الگوریتم جستجوی گروور:** یکی از الگوریتم‌های کوانتومی مهمی که بعد از الگوریتم شور طراحی شد الگوریتم جستجوی گروور[۲۲] بود. فرض کنید که بخواهیم یک پایگاه داده شامل n گزینه را جستجو کنیم. در واقع فرض کنید که یک گزینه از n گزینه‌ی پایگاه داده علامت‌گذاری شده و هدف یافتن آن مورد است. یک الگوریتم طبیعی برای حل این مسأله بررسی یک-به-یک گزینه‌ها است تا جایی که گزینه‌ی علامت‌گذاری شده پیدا شود. اگر گزینه‌ی علامت‌گذاری شده در اوایل لیست باشد، خیلی سریع به جواب می‌رسیم و اگر در انتهای لیست باشد باید کل n مورد از لیست را بخوانیم. در حالت کلی، به طور متوسط نیاز داریم تا نصف پایگاه داده، یعنی $\frac{n}{۲}$ مورد را بررسی کنیم.

  گروور در سال ۱۹۹۶، یعنی دو سال بعد از طراحی الگوریتم تجزیه‌ی شور، نشان داد که با یک کامپیوتر کوانتومی می‌توان گزینه علامت‌گذاری شده را با حدود $\sqrt{n}$ بررسی پیدا کرد [۷]. برای مقایسه‌ی کارایی الگوریتم گروور با الگوریتم کلاسیک فرض کنید که بخواهیم پایگاه داده‌ای شامل اطلاعات ۹۰ میلیون ایرانی را جستجو کنیم. در این صورت برای اجرای الگوریتم کلاسیک باید حدود ۴۵ میلیون بار به پایگاه داده دسترسی پیدا کنیم در صورتی که الگوریتم گروور به حدود ۱۰ هزار دسترسی نیاز دارد.

  الگوریتم جستجوی گروور منجر به پیشرفت‌های مهمی در طراحی الگوریتم‌های کوانتومی شد. با این حال برای فهم کارایی این الگوریتم باید به نکته‌ای مهم توجه کرد. در الگوریتم گروور فرض بر این است که پایگاه

[19] Peter Shor
[20] Discrete logarithm
[21] Post-quantum cryptography
[22] Grover's search algorithm

داده به صورت کوانتومی ذخیره شده است و دسترسی به آن به صورت همدوس[۲۳] امکان‌پذیر است. این فرض برای پایگاه‌های داده‌ی کنونی برقرار نیست و برای محقق شدن آن نیازمند پایگاه‌های داده‌ی کوانتومی هستیم. توجه کنید که طراحی و ساخت پایگاه‌های داده‌ی کوانتومی مسأله‌ای جدا از ساخت کامپیوترهای کوانتومی است و نیاز به تکنولوژیِ اگرچه مرتبط، ولی متفاوتی است.

بنابراین، حتی با وجود کامپیوترهای کوانتومی، لزوماً نمی‌توان الگوریتم جستجوی گروور را روی پایگاه‌های داده‌ی فعلی پیاده‌سازی کرد. با این حال، گاهی هدف از اجرای الگوریتم جستجو، یافتن پارامتری است که مثلاً یک تابع مورد نظر را بهینه می‌کند. در این صورت، نیازی به پایگاه داده‌ای به معنای مرسوم آن نداریم زیرا پایگاه داده‌ی ما چیزی جز لیست اعداد نیست. بنابراین اجرای الگوریتم گروور روی چنین مسائلی حتی در صورت عدم دسترسی به پایگاه‌های داده‌ی کوانتومی قابل تصور است.

- **شبیه‌سازی سیستم‌های کوانتومی:** شبیه‌سازی کوانتومی[۲۴] یکی از مهمترین کاربردهای رایانش کوانتومی است. ایده‌ی شبیه‌سازی کوانتومی اولین بار توسط ریچارد فاینمن[۲۵] ارائه شد. او که خود فیزیک‌دانی شناخته‌شده بود می‌دانست که فهمیدن رفتار بسیاری از سیستم‌های فیزیکی که در سطح بنیادی از قوانین مکانیک کوانتومی پیروی می‌کنند کار بسیار پیچیده‌ای است. توصیف ریاضی این سیستم‌ها اغلب شامل معادلات پیچیده‌ایست که حل تحلیلی آنها حتی برای سیستم‌های نسبتاً ساده فرآیندی پیچیده است. حتی استفاده از کامپیوترهای کلاسیک برای حل تقریبی این معادلات در عمل کاری غیر ممکن است زیرا حجم محاسبات مورد نیاز برای سیستم‌های چندذرّه‌ای (مانند مولکول‌ها یا جامدات) به طور نمایی رشد می‌کند. با توجه به این موضوع، فاینمن در سال ۱۹۸۲ پیشنهاد داد که برای شبیه‌سازی یک سیستم کوانتومی پیچیده، باید از یک سیستم کوانتومی دیگر استفاده کرد. یعنی به جای حل تحلیلی یا حل تقریبی معادلات روی یک کامپیوتر کلاسیک، باید یک آزمایشگاه کوانتومی برنامه‌پذیر بسازیم که رفتار سیستم کوانتومی مورد نظر را تقلید کند. در واقع فاینمن در سال ۱۹۸۲ برای اولین بار ایده‌ی ساخت کامپیوترهای کوانتومی را به طور خاص برای شبیه‌سازی کوانتومی مطرح کرد.

  شبیه‌سازی کوانتومی در دو دهه‌ی اخیر به یکی از موضوعات اصلی محاسبات کوانتومی تبدیل شده است و الگوریتم‌های متنوعی برای شبیه‌سازی یا تقلید[۲۶] سیستم‌های کوانتومی طراحی شده‌اند. این تحقیقات حتی به شبیه‌سازی سیستم‌های کوانتومی روی رایانه‌های کلاسیک نیز کمک کرده‌اند. با این حال، برای استفاده‌ی عملیِ کامل از نتایج این پژوهش‌ها به کامپیوترهای کوانتومی نیازمندیم.

  کاربردهای متنوعی برای شبیه‌سازی کوانتومی قابل تصور است. علاوه بر پیش‌بردن تحقیقات در زمینه‌هایی مانند شیمی کوانتومی یا فیزیک ماده چگال، شبیه‌سازی کوانتومی می‌تواند باعث پیشرفت در طراحی مواد[۲۷] شود. برای مثال، در حال حاضر طراحی دارو[۲۸] پروسه‌ای بسیار طولانی و گران‌قیمت است و یکی از دلایل آن سخت بودنِ مسأله‌ی یافتن ساختار الکترونی مولکول‌ها است. مثال دیگر، مسأله‌ی تولید آمونیاک است که فرآیندی بسیار پرهزینه است. میزان انرژی لازم برای تولید آمونیاک در جهان بین ۱ تا ۱/۵ درصد کل انرژی مصرفی بشر تقریب زده می‌شود. بهینه‌سازی این فرآیند، و به طور خاص فهمیدن ساختار الکترونی بعضی از

[23] Coherent
[24] Quantum simulation
[25] Richard Feynman
[26] Emulation
[27] Material design
[28] Drug design

مولکول‌های درگیر در این فرآیند منجر به صرفه‌جوییِ مقدار زیادی انرژی می‌شود. پیاده‌سازی الگوریتم‌های شبیه‌سازی کوانتومی با استفاده از رایانه‌های کوانتومی قدم مهمی برای حل این مسائل خواهد بود.

- **یادگیری ماشین کوانتومی:** یادگیری ماشین کوانتومی[۲۹] یکی دیگر از کاربردهای کامپیوترهای کوانتومی، علی‌الخصوص در عصر هوش مصنوعی تلقی می‌شود [۱۴]. هوش مصنوعی و رایانش کوانتومی به عنوان دو بازوی تحول در محاسبات در سال‌های اخیر شناخته می‌شوند و یادگیری ماشین کوانتومی تلفیق این دو حوزه است.

یادگیری ماشین کوانتومی را می‌توان بر حسب اینکه روی داده‌های کلاسیک یا کوانتومی پیاده‌سازی شود به دو دسته تقسیم کرد. اگر داده‌ها کلاسیک باشند، ابتدا باید آنها را به صورت کوانتومی کدگذاری کرد که این خود چالشی مهم در یادگیری ماشین کوانتومی است. در عصر اطلاعات، با وجود حجم بالای داده‌ها این مسأله نمود بیشتری پیدا می‌کند. توجه کنید که در حال حاضر الگوریتم‌های یادگیری ماشین کلاسیک این حجم عظیم داده‌ها را تحلیل می‌کنند. لذا اگر بخواهیم یادگیری ماشین کوانتومی نسبت به یادگیری ماشین کلاسیک برتری بیابد باید مسأله‌ی داده‌های ورودی را، حداقل برای نوع خاصی از داده‌ها حل کنیم.

در حال حاضر بعضاً برای کدگذاری کوانتومی داده‌های کلاسیک از الگوریتم‌های کاهش بُعد[۳۰] استفاده می‌شود. یعنی ابعاد داده‌ها با استفاده از این الگوریتم‌های کلاسیک کاهیده می‌شود و سپس داده‌های با ابعاد پایین به عنوان ورودی به کامپیوتر کوانتومی داده می‌شوند که البته کار ساده‌ای است. منتهی این کار نوعی تقلب است. الگوریتم‌های کاهش بُعد خود معمولاً حجم محاسباتی بالایی دارند و اجرای آنها در عمل مسأله را به حل خیلی نزدیک می‌کند. لذا معمولاً بعد از مرحله کاهش بُعد مسأله چنان ساده می‌شود که برای حل آن دیگر نیازی به کامپیوتر کوانتومی نیست!

رده‌ی دوم الگوریتم‌های یادگیری ماشین روی داده‌های کوانتومی پیاده‌سازی می‌شوند. داده‌های کوانتومی شامل حالت‌های خروجی یک آزمایش کوانتومی یا دینامیک یک سیستم کوانتومی هستند. توجه کنید که در یادگیری ماشین کوانتومی روی داده‌های کوانتومی کمتر با مشکل ورودی داده‌ها به کامپیوتر کوانتومی مواجه می‌شویم چرا که داده‌ها به طور ذاتی کوانتومی هستند. از این نقطه نظر، یادگیری ماشین کوانتومی روی مسائل مرتبط با سیستم‌های کوانتومی امیدوارانه‌تر به نظر می‌رسد.

- **بهینه‌سازی کوانتومی:** هدف از بهینه‌سازی کوانتومی حل کردن مسائل بهینه‌سازی پیچیده‌ای است که حل آنها برای کامپیوترهای کلاسیک عملی نیست. بهینه‌سازی کوانتومی ارتباط تنگاتنگی با یادگیری ماشین کوانتومی دارد زیرا الگوریتم‌های یادگیری ماشین اغلب شامل بهینه‌سازی پارامترهای یک مدل هستند. به علاوه، از بهینه‌سازی کوانتومی برای حل مسائل بهینه‌سازی ترکیبیاتی[۳۱] نیز استفاده می‌شود. این مسائل عموماً در اصطلاح NP-سخت هستند و امید است که با استفاده از کامپیوترهای کوانتومی بتوان جواب‌های بهتری (در مقایسه با رایانه‌های کلاسیک) برای آنها یافت.

الگوریتم‌های بهینه‌سازی کوانتومی معمولاً مکاشفه‌ای[۳۲] هستند و تا زمانی که در عمل خوب جواب ندهند، نمی‌توان برتری آنها نسبت به الگوریتم‌های کلاسیک را تضمین کرد.

[29] Quantum machine learning
[30] Dimension reduction algorithms
[31] Combinatorial optimization
[32] Heuristic

لیست الگوریتم‌های کوانتومی که در اینجا به آن پرداختیم به هیچ وجه کامل نیست. هدف آشنایی مختصری بود با دو الگوریتم کوانتومی خاص به عنوان نماینده‌هایی از دو دسته از الگوریتم‌های بسیار مهم محاسبات کوانتومی. به علاوه، به حوزه‌هایی پرداختیم که رایانش کوانتومی می‌تواند در آنها سهمی داشته باشد و به عنوان گزینه‌هایی برای مزیت کوانتومی شناخته می‌شوند.

۳ چالش‌های ساخت کامپیوترهای کوانتومی

در بخش قبل با مدل مداری کوانتومی و بعضی از حوزه‌های کاربردی رایانش کوانتومی آشنا شدیم. در این بخش به این سؤال می‌پردازیم که برای ساخت کامپیوترهای کوانتومی چه چالش‌هایی را باید پشت سر بگذاریم.

یک کامپیوتر کوانتومی باید بتواند حالات کیوبیت‌ها را ذخیره و با اعمال گیت‌های کوانتومی آنها را پردازش کند. اندازه‌گیری کوانتومی نیز یکی از اجزای مهم یک کامپیوتر کوانتومی است. به طور طبیعی یک کامپیوتر کوانتومی با یک کامپیوتر کلاسیک کنترل می‌شود. یعنی کامپیوتر کلاسیک تعداد کیوبیت‌های مورد نیاز و حالات اولیه‌ی آنها را برحسب ورودی مسأله مشخص می‌کند. سپس دنباله‌ی گیت‌هایی که باید توسط کامپیوتر کوانتومی اعمال شود را اعلام می‌کند. در انتها حاصل اندازه‌گیری کوانتومی را دریافت و خروجی را معین می‌کند.

۱.۳ تکنولوژی‌های کوانتومی

در بخش اول مقاله با ارائه‌ی مثال‌های ماشین حساب پاسکال و رایانه‌های امروزی توضیح دادیم که برای ساخت کامپیوترهای کلاسیک می‌توان از تکنولوژی‌های مختلفی استفاده کرد. به طور مشابه، برای ساخت کامپیوترهای کوانتومی نیز می‌توان از فناوری‌های کوانتومیِ گوناگونی بهره برد.

برای تقریب به ذهن می‌توانیم با آزمایش دو-شکاف شروع می‌کنیم. در آن آزمایش دیدیم که حالت هر ذره می‌تواند عبور از شکاف اول، عبور از شکاف دوم یا برهم‌نهی آنها باشد. اگر عبور از شکاف اول را به عنوان حالت ۰، عبور از شکاف دوم را به عنوان حالت ۱ و برهم‌نهی آنها را نیز در نظر بگیریم، می‌توانیم حالت یک کیوبیت را در این سیستم کوانتومی نمایش دهیم. البته این روش در عمل چندان کارا نیست.

خاصیت ابررسانایی[۳۳] یک تکنولوژی کوانتومی است که در عمل برای ساخت کامپیوترهای کوانتومی استفاده می‌شود. بعضی از مواد در بازه‌های دماییِ مشخص (مثلاً در دماهای بسیار پایین) مقاومت الکتریکی خود را از دست می‌دهند و در اصطلاح ابررسانا می‌شوند. حال حلقه‌ی فلزی ابررسانایی را تصور کنید که الکتریسیته بدون مقاومت در آن جریان پیدا می‌کند. این جریان الکتریکی می‌تواند در جهت ساعت‌گرد، پاد ساعت‌گرد یا برهم‌نهی آن دو باشد. لذا از آن حلقه‌ی فلزی می‌توان برای نمایش حالات یک کیوبیت استفاده کرد.

تکنولوژی‌های دیگری که برای نمایش کیوبیت‌ها استفاده می‌شوند شامل اپتیک کوانتومی،[۳۴] یون‌های به دام افتاده،[۳۵] فازهای توپولوژیک ماده[۳۶] و اتم‌های خنثی[۳۷] هستند. هر یک از این تکنولوژی‌ها مزایا و معایب خاص خود

[33] Superconductivity
[34] Quantum optics
[35] Trapped ions
[36] Topological phases of matter
[37] Neutral atoms

تکنولوژی	بعضی از شرکت‌های پیشتاز
ابررسانایی	IBM, Google, Rigetti
یون‌های به دام افتاده	Quantinuum, IonQ, Oxford Ionics
اتم‌های خنثی	Atom Computing, QuEra
اپتیک	PsiQuantum, Xanadu
فازهای توپولوژیک	Microsoft

جدول ۱: بعضی از تکنولوژی‌های کوانتومی مورد استفاده در ساخت کامپیوترهای کوانتومی و شرکت‌های پیشتازی که از آنها استفاده می‌کنند.

را دارند. برای مثال کامپیوترهایی که براساس ابررسانایی طراحی می‌شوند فقط در دماهای نزدیک به صفر کِلوین کارا هستند. در حالی که اپتیک کوانتومی در دمای اتاق نیز کارایی دارد. از طرف دیگر سرعت اعمال گیت‌های دو-کیوبیتی روی سیستم‌های ابررسانایی نسبت به اتم‌های خنثی یا یون‌های به دام افتاده بیشتر است. محققین در دانشگاه‌ها، مؤسسات تحقیقاتی و شرکت‌های مختلف با توجه به مزایای هر یک از این تکنولوژی‌ها، فناوری مورد نظر خود برای ساخت کامپیوترهای کوانتومی را انتخاب و تلاش می‌کنند تا معایب آن را برطرف کنند [۸]. در جدول ۱ لیستی از شرکت‌های مختلف و تکنولوژی مورد استفاده‌ی آنها برای ساخت کامپیوتر کوانتومی آمده است.

۲.۳ مسأله‌ی نویز و کدهای تصحیح خط

تصویری که تا کنون در مورد مدارهای کوانتومی و ساخت کامپیوتر کوانتومی ارائه شد، تصویری نسبتاً ایده‌آل است. نمایش کیوبیت‌ها در یک سیستم کوانتومی معمولاً همراه با نویز است. حتی اگر در ابتدای کار بتوانیم حالات کیوبیت‌ها را بدون هیچ خطایی در سیستم کوانتومی مورد نظر ایجاد کنیم، نویز حالت این کیوبیت‌ها را در طول محاسبات تحت تأثیر قرار خواهد داد. به علاوه، معمولاً اعمال گیت‌های کوانتومی خود عاری از نویز نیست و کامپیوتر کوانتومی بجای اجرای یک گیت مورد نظر، آن را همراه با خطا اعمال می‌کند. اندازه‌گیری کوانتومی نیز متأثر از نویز است و تجمیع این خطاها احتمالاً باعث می‌شود که خروجی مدار کوانتومی چیزی غیر از نویز نباشد.

نویز در سیستم‌های محاسباتی یا مخابراتی کلاسیک نیز وجود دارد. در این سیستم‌ها برای کم کردن اثر نویز از کدهای تصحیح خطا[۳۸] استفاده می‌شود. ایده‌ی کلی این است که با اضافه کردن افزونگی،[۳۹] اطلاعات را به صورتی کدگذاری کنیم که تحت تأثیر نویز همچنان قابل بازیابی باشند. در واقع، در ابتدای کار اطلاعاتِ ورودیِ مسأله را همراه با افزونگی کدگذاری می‌کنیم و محاسبات را با اعمال گیت‌های منطقی روی اطلاعات کدگذاری‌شده انجام می‌دهیم. به علاوه، در حین محاسبه به طور مرتب فرآیند تصحیح خطا و بازیابی اطلاعات را تکرار می‌کنیم تا از تجمیع نویز در طول زمان جلوگیری کنیم.

توجه کنید که استفاده از کدهای تصحیح خطا برای کم کردنِ اثر نویز، بدون هزینه نیست. افزونگیِ کدهای تصحیح خطا منجر به افزایش حجم محاسبات شده و فرآیند اعمال گیت‌های منطقی را مطول می‌کند. به علاوه، فرآیند تصحیح خطا که به طور مرتب در حین محاسبات تکرار می‌شود، به حجم محاسبات اضافه شده و هزینه‌ی زیادی را تحمیل می‌کند.

[38] Error correcting codes
[39] Redundancy

نکته‌ی نهایی در مورد کدهای تصحیح خطا بهینه بودن آنها است. توجه کنید که فرآیند کدگذاری و تصحیح خطا خود تحت تأثیر نویز است. بنابراین اگر یک کد و الگوریتم تصحیح خطای آن بهینه نبوده و حجم محاسباتی آن زیاد باشد، استفاده‌ی از آن در عمل بی‌معنی است. با این کار برای حذف بخشی از نویز، حجم محاسبات را چنان زیاد می‌کنیم که در عمل نویز بیشتری بر ما تحمیل می‌شود.

بعد از یافتن الگوریتم تجزیه‌ی شور بعضی از متخصصین اعتقاد داشتند که این الگوریتم هیچ‌گاه در عمل پیاده‌سازی نخواهد شد، زیرا سیستم‌های کوانتومی بسیار نویزی هستند و کدهای تصحیح خطای کوانتومی وجود ندارند. نکته‌ی مورد اشاره‌ی این افراد این بود که فضای حالات یک بیت کلاسیک گسسته است و فقط یک نوع خطا برای آن قابل تصور است: حالت بیت از ۰ به ۱ یا بالعکس تغییر کند. بنابراین، طراحیِ کدهای کلاسیکی که نسبت به نویز کلاسیک مقاوم باشند امکان‌پذیر است. ولی به دلیل اصل برهم‌نهی، فضای حالات یک کیوبیت پیوسته است و در نتیجه فضای خطاهای قابل تصور روی یک سیستم کوانتومی نیز فضایی پیوسته است. تصحیح کردن دامنه‌ای پیوسته از خطاها هم در عمل امکان‌پذیر نیست. یعنی نمی‌توان یک کد کوانتومی طراحی کرد که بتواند همه‌ی نویزهای کوانتومی را تصحیح کند.

پیتر شور در سال ۱۹۹۵، یعنی یک سال بعد از طراحی الگوریتم تجزیه‌ی خود نشان داد که استدلال فوق دقیق نیست و یک کد تصحیح خطای کوانتومی ۹-کیوبیتی وجود دارد. او نشان داد که نویز در سیستم‌های کوانتومی گرچه در ظاهر پیوسته، ولی در واقع گسسته است. او نشان داد که حداقل برای دسته‌ای خاص از کدهای کوانتومی، اگر بتوان دو نوع خاص از خطاهای کوانتومی را تصحیح کرد، آنگاه می‌توان هر خطای دیگری را نیز تصحیح کرد [۱۶]. کار مهم شور نشان که محاسبات کوانتومی حتی در حضور نویز نیز قابل تصور است.

در سال‌های بعد با بسط نظریه‌ی کدهای تصحیح خطای کوانتومی، کدهای بهتری نسبت به کد ۹-کیوبیتی شور طراحی شد. با این حال برای استفاده‌ی عملی آنها در کامپیوترهای کوانتومی، همچنان باید فاصله‌ی بین نویز حاضر در تکنولوژی‌های کوانتومی فعلی و شدتِ نویز قابل تصحیح در این کدهای کوانتومی از بین برود. یادآوری می‌کنیم که فرآیند کدگذاری و تصحیح خطا، خود تحت تأثیر نویز هستند. بنابراین اگر کد تصحیح خطای کوانتومی به اندازه کافی و در نسبت با نویز موجود در سیستم‌های کوانتومی بهینه نباشد، استفاده از آن در عمل عاری از فایده است. به نظر می‌رسد که برای فائق آمد به مشکل نویز، هم باید کدهای تصحیح خطای بهتری طراحی کرد و هم سیستم‌های کوانتومی را پایدارتر کرد تا کمتر تحت تأثیر نویز قرار بگیرند و فاصله‌ی مذکور از بین برود.

۳.۳ وضعیت فعلی فناوری

حال که با یکی از مهم‌ترین مشکلات در راستای ساخت کامپیوترهای کوانتومی آشنا شدیم، می‌توانیم به وضعیت فعلی فناوری در این زمینه بپردازیم. در جدول ۲ اطلاعاتی در مورد ادوات محاسباتی کوانتومی بعضی از شرکت‌های فعال در ساخت کامپیوترهای کوانتومی آورده شده است [۱۹]. البته این جدول براساس اطلاعات این شرکت‌ها تا سال ۲۰۲۴ تهیه شده است و لزوماً مطابق با آخرین دستاوردهای آنها نیست. با این حال، تا حد خوبی وضعیت فعلی فناوری کوانتومی را نمایش می‌دهد. در این جدول می‌بینیم که بسته به نوع تکنولوژی، تعداد کیوبیت‌های این شرکت‌ها بین چند-ده تا چند-صد کیوبیت است. به علاوه می‌بینیم که ارتباطی بین تعداد کیوبیت‌ها و نویز موجود در این سیستم‌ها وجود دارد به طوری که هر چه تعداد کیوبیت‌ها بیشتر می‌شود، نویز موجود نیز افزایش پیدا می‌کند.

بعضی از این شرکت‌ها کدهای تصحیح خطای ساده‌ای را روی سیستم کوانتومی خود پیاده‌سازی کرده‌اند که البته فرآیند بسیار پیچیده‌ای است و دستاورد مهمی محسوب می‌شود [۲]. با این حال تعداد کیوبیت‌های این ادوات چنان کم است که با پیاده‌سازی این کدها قدرت محاسباتی این ادوات در عمل از بین می‌رود.

Oxford Ionics	Quantinuum H2	IonQ Forte	Quera	IBM Heron r2	Google Willow	
$۲/۹ \times ۱۰^{-۴}$	$۸/۵ \times ۱۰^{-۴}$	۴×۱۰^{-۳}	۵×۱۰^{-۳}	$۲/۲ \times ۱۰^{-۳}$	$۳/۳ \times ۱۰^{-۳}$	ε
۱۰	۳۰	۳۶	۲۵۶	۱۵۶	۱۰۵	N

جدول ۲: ε مقدار نویز و N تعداد کیوبیت‌های هر یک از ادوات محاسباتی کوانتومی را نمایش می‌دهند.

سؤال مهم این است که آیا می‌توان در حین افزایش تعداد کیوبیت‌های این ادوات نویز را نیز کنترل کنند؟ در این صورت پیاده‌سازی کدهای تصحیح خطای کوانتومی نیز امکان‌پذیر شده و به ساخت کامپیوترهای کوانتومی نزدیک خواهیم شد.

۴.۳ معیارهای دیگر در مقایسه‌ی ادوات کوانتومی

در بالا ادوات کوانتومی چند شرکت را برحسب تعداد کیوبیت‌ها و نویز موجود در آنها مقایسه کردیم. با این حال معیارهای دیگری نیز در مقایسه‌ی این ابزارهای کوانتومی اهمیت دارند و مقایسه‌ی صرف برحسب دو معیار فوق ناقص است.

یک پارامتر مهم در کامپیوترهای کوانتومی مدت زمان لازم برای اعمال گیت‌های دو-کیوبیتی است. اگر این زمان زیاد باشد، حتی با وجود تعداد کیوبیت‌های بیشتر، ممکن است که آن کامپیوتر کوانتومی در عمل عاری از فایده باشد. به علاوه، این زمان باید در مقایسه با زمان پایداری[۴۰] سیستم کوانتومی بسیار کمتر باشد. زیرا در غیر این صورت قبل از اینکه گِیتی اعمال و فرآیند تصحیح خطا انجام شود، کیوبیت‌های سیستم تباه می‌شوند.

معیار مهم دیگر همبندی[۴۱] یا توپولوژی کیوبیت‌های سیستم است. برای مثال در شکل ۴ تراشه‌ی کوانتومی اخیر شرکت گوگل به نام Willow نمایش داده شده است که در آن کیوبیت‌ها در یک شبکه دوبُعدی قرار دارند و هر کیوبیت با چهار کیوبیت دیگر در ارتباط است. در این تراشه گیت‌های دو-کیوبیتی فقط بین کیوبیت‌های مجاور قابل اعمال هستند و این محدودیتی روی مدارهای قابل پیاده‌سازی روی این تراشه ایجاد می‌کند. در مقایسه، اداوت شرکت‌هایی که از تکنولوژی یون‌های به دام افتاده استفاده می‌کنند همبندی بالاتری نسبت به این تراشه دارند.

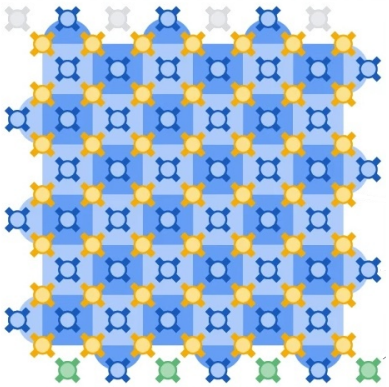
معیار دیگری که باید به آن اشاره کنیم مقیاس‌پذیری[۴۲] است. ممکن است که یک تکنولوژی شاخص‌های خوبی تا تعداد مشخصی کیوبیت داشته باشد ولی مقیاس‌پذیر نباشد. به طور مثال، شرکت Oxford Ionics توانسته است در مقایسه با شرکت‌های دیگر نویز را تا حد بیشتری کنترل کند، ولی با تعداد کیوبیت‌های کمتر. سؤال این است که آیا این شرکت می‌تواند در حین افزایش تعداد کیوبیت‌ها، شاخص‌های دیگر از جمله نویز را نیز بهبود ببخشد؟

۵.۳ اجرای الگوریتم تجزیه‌ی شور

در اینجا برای اطلاع از فاصله‌ی تکنولوژی بین ادوات محاسباتیِ کنونیِ شرکت‌های مختلف و کامپیوترهای کوانتومی ایده‌آل، بعضی از شاخصه‌های یک کامپیوتر کوانتومی برای اجرای الگوریتم تجزیه‌ی شور را مرور می‌کنیم.

فرض کنید که بخواهیم عددی را تجزیه کنیم که نمایش دودویی آن ۲۰۴۸ بیت دارد. به علاوه، فرض کنید که

[40] Stability time
[41] Connectivity
[42] Scalability



شکل ۴: شمای دوبُعدی تراشه‌ی کوانتومی شرکت گوگل

بخواهیم از کامپیوتری کوانتومی استفاده کنیم که کیوبیت‌های آن، همانند تراشه‌ی گوگل در شکل ۴، در یک شبکه‌ی دو-بُعدی قرار گرفته‌اند. در این صورت به حدود ۲۰ میلیون کیوبیت نیاز داریم [۶]. نیاز به این تعداد کیوبیت با این فرض است که مقدار نویز در این کامپیوتر کوانتومی از مرتبه‌ی $۱۰^{-۳}$ است و بتوانیم یک کد تصحیح خطای خاص را با دوره‌ی زمانی[۴۳] یک میکروثانیه پیاده‌سازی کنیم.

مشاهده کنید که برای پیاده‌سازی یکی از الگوریتم‌های مهم کوانتومی روی تراشه‌های دو-بعدی به میلیون‌ها کیوبیت نیاز داریم که فاصله‌ی زیادی با چند صد کیوبیت فعلی دارد. توجه کنید که اگر بتوانیم نویز، همبندی یا دیگر شاخص‌ها را بهبود دهیم، تعداد کیوبیت‌های لازم نیز کمتر می‌شود [۵]. از طرف دیگر می‌توانیم نحوه‌ی پیاده‌سازی الگوریتم‌ها را نیز بهبود ببخشیم. با این حال با توجه به شاخصه‌های فوق، تا ساخت یک کامپیوتر کوانتومی که بتواند الگوریتم‌های معمول کوانتومی را اجرا کند، باید راه پرچالشی را طی کنیم.

ادوات کوانتومی فعلی حاصل فائق آمدن بر چالش‌های زیادی توسط متخصصین این حوزه هستند و خود پیشرفت چشم‌گیری در تکنولوژی کوانتومی محسوب می‌شوند. با این حال، اطلاق عنوان کامپیوتر کوانتومی به این ادوات صحیح نیست چرا که این ادوات مقیاس بسیار کوچک‌تری نسبت به یک کامپیوتر دارند و مقیاس‌پذیر کردن تکنولوژی ساخت آنها نیز پرچالش به نظر می‌رسد.

۴ محاسبات کوانتومی در کوتاه‌مدت و میان‌مدت

در بخش قبل دیدیم که تا ساخت یک کامپیوتر کوانتومی و استفاده از همه‌ی مواهب آن مسیر پرچالشی پیش رو داریم. سؤالی که در اینجا پیش می‌آید این است که آیا ادوات کوانتومی فعلی یا ادوادتی که طی چند سال آینده ساخته می‌شوند بدون کاربرد هستند؟ آیا نمی‌توانیم بعضی از الگوریتم‌های کوانتومی را روی این ادوات اجرا کنیم؟ آیا این ادوات نمی‌توانند نقشی همانند ماشین حساب پاسکال را برای ما بازی کنند که قابلیت‌های رایانه‌های عصر حاضر را نداشت، ولی می‌توانست بعضی محاسبات را انجام دهد؟

توجه کنید که پیاده‌سازی کدهای تصحیح خطا برای ادوات کوانتومی فعلی کار سنگینی است. حتی اگر تعداد کیوبیت‌های این ادوات (با حفظ شاخصه‌های دیگر) به هزار هم برسد، باز هم اجرای کدهای تصحیح خطا روی آنها

[43] Cycle time

چندان کارا نیست. لذا به نظر می‌رسد که ادوات فعلی را باید با حضور نویز پذیرفت. سؤال این است که یک دستگاه کوانتومی نویزی با مثلاً صد، هزار یا ۱۰ هزار کیوبیت به چه کار می‌آید؟ آیا برای چنین دستگاهی کاربردی قابل تصور است؟

به عصر حاضر که در آن ادوات کوانتومی نویزی هستند و مقیاس میانی[۴۴] دارند گاهی عصر «نیسک»[۴۵] گفته می‌شود [۱۲]. سؤال این است که ادوات کوانتومی عصر نیسک چه کاربردهایی دارند؟

۱.۴ تأثیر نویز روی یک کیوبیت

قبل از اینکه به سؤال فوق پاسخ دهیم باید تأثیر نویز روی یک سیستم کوانتومی را بهتر درک کنیم. برای این کار با یک کیوبیت شروع می‌کنیم. فضای حالات یک کیوبیت را می‌توان همانند شکل ۵ با یک کُره به شعاع ۱ در فضای سه‌بُعدی نمایش داد که به آن کره‌ی بُلوخ[۴۶] می‌گویند. هر نقطه‌ی درون کره‌ی بلوخ متناظر با حالتی از یک کیوبیت است که آن را با نماد ρ نمایش می‌دهیم. به طور خاص مرکز کره یا همان مبدأ مختصات متناظر با حالت یک کیوبیت است که به طور کاملاً تصادفی آماده‌سازی شده است. بنابراین کیوبیتی که حالت آن متناظر با مرکز کره‌ی بلوخ باشد حاوی هیچ اطلاعاتی نیست و هرچه از مبدأ مختصات دور شده و به مرز کره نزدیک می‌شویم به حالاتی می‌رسیم که حاوی اطلاعات بیشتری هستند.

نویز در سیستم‌های کوانتومی فرم‌های مختلفی دارد. در اینجا برای مدل کردن نویز از کانال واقطبش[۴۷] استفاده می‌کنیم که به فرم زیر نوشته می‌شود:

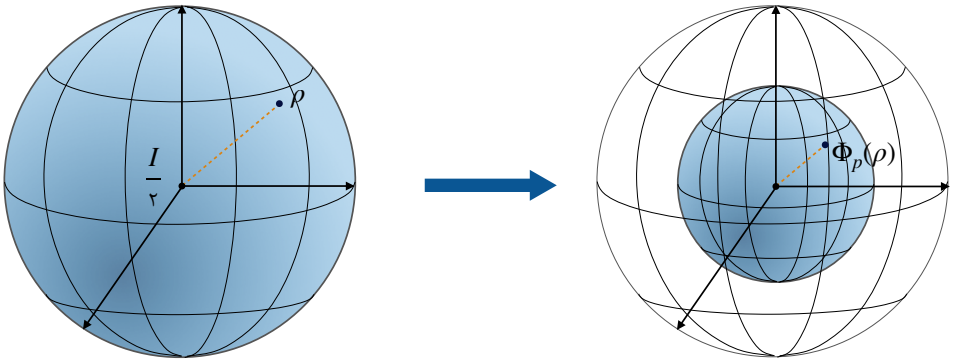
$$\Phi_p(\rho) = (۱-p)\rho + p\frac{I}{۲}.$$

در اینجا p پارامتر نویز و عددی بین ۰ و ۱ است و ρ حالت کیوبیتِ ورودی کانال و متناظر با یک نقطه از کره‌ی بلوخ است. همچنین $\frac{I}{۲}$ همان حالت کاملاً تصادفی متناظر با مرکز کره است. رفتار کانال واقطبش به این صورت است که به حالت ورودی ρ با احتمال p یک نویز کاملاً تصادفی اضافه می‌کند. تعبیر هندسی این نویز روی کره‌ی بلوخ به این صورت است که تحت نویز واقطبش، حالت ورودی ρکه متناظر با یک نقطه از کره است به اندازه‌ی ضریب $۱-p$ به مرکز کره نزدیک می‌شود. در واقع پس از اعمال نویز واقطبش، حالات یک کیوبیت دیگر با کره‌ی به شعاع واحد نمایش داده نمی‌شوند و کره‌ی متناظر شعاع $۱-p$ خواهد داشت [۱۰].

حال فرض کنید محاسبه‌ی روی یک کیوبیت به اندازه‌ی d واحد زمان طول بکشد و در هر واحد از زمان تحت تأثیر نویز واقطبش قرار گیرد. در این صورت در هر واحد زمان، شعاع کره‌ی متناظر با حالات کیوبیت با ضریب $۱-p$ کوچک می‌شود. در نتیجه در d واحد زمان، شعاع کرده مورد نظر برابر $(۱-p)^d$ خواهد بود و به طور نمایی کوچک می‌شود. مثلاً اگر مقدار نویز $p = ۱۰^{-۳}$ باشد، آنگاه شعاع کره در $d = ۱۰^۴$ واحد زمان تقریباً برابر صفر خواهد شد. یعنی در $d = ۱۰^۴$ واحد زمان، حالت کیوبیت چنان نزدیک مرکز کره‌ی بلوخ می‌شود که با $\frac{I}{۲}$ و یک حالت کاملاً تصادفی تفاوت چندانی ندارد.

به طور خلاصه، حالت کیوبیتی که تحت تأثیر نویز قرار گرفته است، بر حسب مدت زمان محاسبات به طور نمایی

[44] Intermediate scale
[45] NISQ era: Noisy Intermediate-Scale Quantum era
[46] Bloch sphere
[47] Depolarizing channel



شکل ۵: کره‌ی بلوخ و اثر نویز واقطبش روی آن

به یک حالت کاملاً تصادفی نزدیک می‌شود. در نتیجه بدون استفاده از کدهای تصحیح خطا، محاسبات طولانی روی یک کیوبیت عاری از فایده است.

۲.۴ تأثیر نویز روی محاسبات کوانتومی

حال یک مدار کوانتومی با n کیوبیتِ ورودی در نظر بگیرید. همچنین فرض کنید این کیوبیت‌ها همانند بالا تحت تأثیر نویز باشد و اجرای مدار d واحد زمان طول بکشد. همان‌طور که در شکل ۳ توضیح داده شده است زمان اجرای یک مدار متناظر با عمق[۴۸] مدار است. تحلیل فوق برای یک کیوبیت را می‌توان برای این n کیوبیت نیز تکرار کرد. البته در این حالت تحلیل ساده‌ی هندسی فوق کارا نیست و باید ابزار ریاضی بیشتری استفاده شود. با این حال می‌توان نشان داد که اگر d از مرتبه‌ای بیشتر از لگاریتم n باشد (مثلاً $d = n$ یا $d = \log^{۲} n$)، آنگاه همانند بالا خروجی مدار حاوی هیچ اطلاعاتی نیست [۱۸].

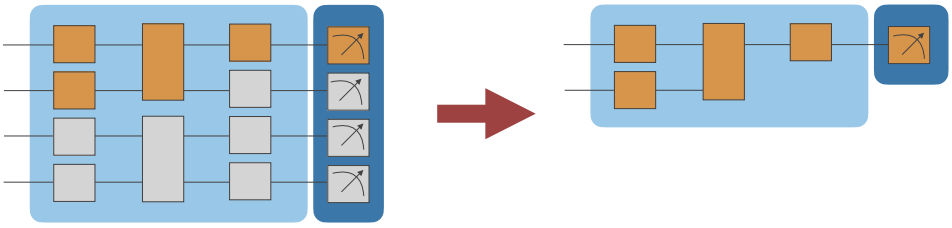
نتیجه اینکه محاسبات کوانتومی در حضور نویز و بدون استفاده از کدهای تصحیح خطا، فقط وقتی کارا است که عمق محاسبات حداکثر به صورت لگاریتمی رشد کند.

۳.۴ محاسبات با عمق کم

در بالا دیدیم که اجرای مدارهای کوانتومی با عمق بالا و در حضور نویز، خروجی بامعنایی ندارد و کار باطلی است. حال می‌خواهیم به محاسبات کوانتومی با عمق پایین، یعنی کمتر از لگاریتمی بپردازیم. در چنین مدارهایی عمق محدود باعث می‌شود که مقدار وابستگیِ کوانتومی تولید شده در انتهای مدار بسیار محدود شود. در نتیجه چنین مدارهایی احتمالاً رفتاری مشابه مدارهای کلاسیک دارند و توسط رایانه‌های کلاسیک قابل شبیه‌سازی هستند. در ادامه این شهود کلی را با ارائه‌ی مثالی توضیح می‌دهیم.

فرض کنید که در مدار شکل ۶ فقط به حاصل اندازه‌گیری کیوبیت اول علاقه‌مند باشیم. توجه کنید که حاصل این اندازه‌گیری به همه‌ی مدار وابسته نیست. در واقع، گیت‌های طوسی رنگ در این مدار تأثیری روی حاصل این

[48] Circuit depth



شکل ۶: حاصل اندازه‌گیری کیوبیت اول فقط به بعضی از کیوبیت‌ها و گیت‌های مدار وابسته است. لذا برای محاسبه‌ی حاصل این اندازه‌گیری می‌توانیم مدار را با در نظر گرفتن مخروط نوری آن ساده‌سازی کنیم.

اندازه‌گیری ندارند. اگر بخواهیم از اصطلاحات نسبیتی استفاده کنیم، این اندازه‌گیری فقط متأثر از مخروط نوری[۴۹] متناظر خود است. با در نظر گرفتن این مخروط نوری، مدار اولیه را می‌توان همانند شکل ۶ ساده‌سازی کرد به طوری که حاصل اندازه‌گیری کیوبیت اول در هر دو مدار یکسان باشد.

حال توجه کنید که مدار دوم، مدارِ بسیار کوچک‌تری است و روی تعداد کیوبیت کمتری اثر می‌کند. در حالت کلی تعداد کیوبیت‌های مدار ساده‌سازی شده به دو پارامتر بستگی دارد: یکی عمق مدار و دیگری همبندی کیوبیت‌های آن (پارامتری که در بخش قبل به آن اشاره شد). حال اگر این دو پارامتر کوچک باشند، می‌توان نشان داد که تعداد کیوبیت‌های مدار ساده‌سازی شده چنان کم است که این مدار را می‌توان روی یک کامپیوتر کلاسیک شبیه‌سازی کرد.

در مثال بالا فرض کردیم که فقط یک کیوبیت را اندازه‌گیری می‌کنیم در حالی که یک مدار کوانتومی در حالت کلی شامل اندازه‌گیری همه‌ی کیوبیت‌ها است. در این صورت، گرچه شهود فوق همچنان پابرجاست، استدلال بالا را باید اصلاح کرد. می‌توان نشان داد که در یک سیستم یک-بُعدی،[۵۰] اگر عمق مدار کمتر از لگاریتمی باشد، آنگاه می‌توان کل مدار را روی یک رایانه کلاسیک در عمل شبیه‌سازی کرد [۱۸]. برای سیستم‌های دو بُعدی، مانند تراشه‌ی گوگل در شکل ۴، همچنان شبیه‌سازی کلاسیک امکان‌پذیر است در صورتی که عمق مدار مرتبه‌ی کمتری داشته باشد.

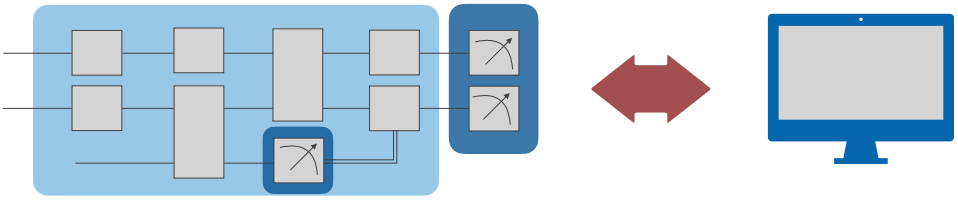
۴.۴ محاسبات ترکیبی

در بالا دیدیم که محاسبات کوانتومی در حضور نویز و بدون استفاده از کدهای تصحیح خطا فقط تا عمق محدودی معنی‌دار است. به علاوه، دیدیم که اگر عمق مدار کوانتومی کمتر از حدی مشخص باشد، شبیه‌سازی کلاسیک آن مدار امکان‌پذیر است. بنابراین، در حضور نویز، برتری کوانتومی فقط با مدارهایی امکان‌پذیر است که عمق آنها در بازه‌ای مشخص و محدود قرار دارد. به علاوه، این بازه به مقدار نویز و همبندی (توپولوژی) سیستم کوانتومی بستگی دارد.

نتیجه‌گیری فوق گرچه صحیح، ولی کامل نیست. نکته در این است که تا کنون فرض کرده‌ایم که مدار کوانتومی ما به فرم شکل ۳ است. با این حال فرم‌های دیگری از مدارهای کوانتومی نیز قابل تصور است. مثلاً ممکن است که بعضی از کیوبیت‌ها، بجای ابتدای مدار، در وسط مدار کوانتومی اضافه شوند تا کمتر تحت تأثیر نویز قرار بگیرند. به علاوه، ممکن است که اندازه‌گیری بعضی از کیوبیت‌ها، بجای انتهای مدار، در وسط مدار کوانتومی انجام شده، و حاصل آن اندازه‌گیری‌ها بخش‌های بعدی مدار را کنترل کند. همچنین قابل تصور است که محاسبات به صورت ترکیبیِ کوانتومی

[49] Light cone

[۵۰] یعنی کیوبیت‌ها پشت سر هم روی یک خط یا یک دایره قرار گرفته‌اند.



شکل ۷: در این مدار کوانتومی، کیوبیت سوم بجای ابتدای مدار، در اواسط مدار اضافه می‌شود و لذا تحت تأثیر نویز کمتری است. به علاوه، بعضی از اندازه‌گیری‌ها در وسط مدار می‌توانند پارامترهای بخش‌های دیگر محاسبه را کنترل کنند. همچنین رفت و برگشت بین محاسبات کوانتومی و محاسبات کلاسیک فرم ترکیبی محاسبه را شکل می‌دهد.

و کلاسیک [۵۱] انجام شود. یعنی بخشی از محاسبه توسط کامپیوتری کلاسیک و بخشی به صورت کوانتومی انجام شود و مطابق شکل ۷، در حین محاسبه بین این دو رفت و برگشت وجود داشته باشد. در این صورت چه بسا نتیجه‌گیری فوق تحت تأثیر قرار بگیرد.

واقعیت این است که ایده‌های بالا در تحلیل مدارهای نویزی با عمق بالا و مدارهای با عمق کم، در حضور محاسبات ترکیبی نیز کارا هستند چرا که به هر حال هر بخش محاسبه که به صورت کوانتومی انجام شود متناظر با یک مدار کوانتومی است و تحلیل‌های فوق بر آن مترتب است. با این حال، به دلیل در نظر گرفتن فرم‌های بیشتری از مدارهای کوانتومی، احتمالاً بازه‌ای که در آن برتری کوانتومی در حضور نویز قابل تصور است کمی وسیع‌تر می‌شود.

۵.۴ کاربردهای ادوات کوانتومی نویزی

حال می‌توانیم به سؤال ابتدای بخش در مورد کاربردهای محاسبات کوانتومی روی ادوات نویزی پاسخ دهیم: کدام یک از کاربردهای محاسبات کوانتومی روی ادوات نویزی عملی است؟

عمق مدار متناظر با الگوریتم تجزیه‌ی شور برای تجزیه‌ی یک عدد n بیتی از مرتبه‌ی $n^۲$ و بسیار بیشتر از لگاریتمی است. لذا تجزیه‌ی اعداد روی ادوات کوانتومی نویزی در عمل امکان‌پذیر نیست. به همین ترتیب، اجرای الگوریتم گروور و دسته‌ی بزرگی از الگوریتم‌های کوانتومی دیگر روی ادوات نویزی در عمل غیرممکن است. از بین کاربردهای دیگر کامپیوترهای کوانتومی، کلاس بزرگی از الگوریتم‌های شبیه‌سازی کوانتومی نیز در همین دسته قرار می‌گیرند و منجر به برتری کوانتومی در حضور نویز نمی‌شوند.

با این حال پیشنهاداتی برای حل مسائل شبیه‌سازی کوانتومی، یادگیری ماشین کوانتومی و بهینه‌سازی کوانتومی وجود دارد که لزوماً عمق مداری بالایی ندارند. این دسته از الگوریتم‌ها براساس مدارهای کوانتومیِ وَردِشی [۵۲] طراحی می‌شوند و در واقع مبنی بر الگوریتم‌های ترکیبی هستند. با این حال، تا کنون کارایی این الگوریتم‌ها در عمل به اثبات نرسیده است. برای نشان دادن کارایی این الگوریتم‌ها باید به طور خاص نشان داد که عمق مدارهای متناظر با این الگوریتم‌ها در بازه‌ی مناسبی قرار دارد به طوری که نه نویز آنها را بی‌معنی می‌کند و نه توسط کامپیوترهای کلاسیک قابل شبیه‌سازی هستند.

نکته‌ی دیگری که باید در مورد الگوریتم‌های وردشی کوانتومی مورد توجه قرار بگیرد مسأله‌ی فلات لم‌یزرع [۵۳]

[51] Hybrid quantum-classical computation
[52] Variational quantum circuits
[53] Barren plateau

است [۹]. نکته در این است که این الگوریتم‌ها سعی می‌کنند مقادیر بهینه‌ی متغیرهای یک مدار کوانتومی را با روش کاهش گرادیان[۵۴] پیدا کنند. ولی به دلیل ساختار مدارهای کوانتومی، معمولاً طول بردار گرادیانِ در این‌گونه مسائل بسیار کوچک است. در واقع، نمودار این توابع هدف همانند یک فلات لم‌یزرع تقریباً همه جا صاف است. لذا با اجرای الگوریتم کاهش گرادیان در هر مرحله، تابع هدف تغییر چندانی نکرده و لذا تعداد تکرارهای الگوریتم کاهش گرادیان بسیار (به صورت نمایی بر حسب اندازه‌ی مدار) زیاد است. بنابراین، حتی اگر بخش کوانتومی این الگوریتم‌های ترکیبی بدون هیچ نویزی اجرا شود، به دلیل مشکل فلات لم‌یزرع ممکن است اجرای کل فرآیند بهینه‌سازی بسیار طول بکشد و کارا نباشد.

۶.۴ نمونه‌گیری از مدارهای تصادفی

در انتهای این بخش به مسأله‌ی نمونه‌گیری از مدارهای تصادفی[۵۵] می‌پردازیم که در سال‌های اخیر در صدر اخبار مربوط به محاسبات کوانتومی قرار گرفته است.

نمونه‌گیری از مدارهای تصادفی یعنی پارامترهای یک مدار کوانتومی، از جمله گیت‌های آن را به طور کاملاً تصادفی انتخاب، آن را اجرا و در انتها حاصل اندازه‌گیری را به عنوان خروجی معرفی کنیم. این کار برای اولین بار توسط گروه کوانتومی شرکت گوگل در سال ۲۰۱۹ روی یک تراشه‌ی ۵۳-کیوبیتی انجام و به عنوان شاهدی از برتری کوانتومی ارائه شد [۳]. آنها ادعا کردند که این کار برتری کوانتومی را اثبات می‌کند چرا که هیچ کامپیوتر کلاسیکی نمی‌تواند در مدت زمانی معقول نمونه‌گیری از مدارهای تصادفی ۵۳-کیوبیتی را شبیه‌سازی کند. آنها برای صحت‌سنجی ادعای خود محکی را معرفی کردند به نام محک آنتروپی متقاطع[۵۶] و با استفاده از این محک نشان دادند که خروجی آزمایش آنها کاملاً نویزی نیست.

ادعای گروه کوانتومی گوگل به دلایل زیر به عنوان یک واقعیت علمی امری کاملاً پذیرفتنی نیست:

(آ) نکته‌ی اول این که محک آنتروپی متقاطع به عنوان ابزاری برای آزمودن خروجی یک فرآیند تصادفی چندان استاندارد نیست. به علاوه، به راحتی می‌توان الگوریتمی کلاسیک طراحی و اجرا کرد که همانند خروجی‌های تراشه‌ی گوگل این محک را ارضا کند.

(ب) نکته‌ی دوم این که ادعای گروه کوانتومی گوگل مبنی بر غیر عملی بودن شبیه‌سازی کلاسیک آزمایش آنها چندان دقیق نبود. در واقع، مدتی کوتاه بعد از ادعای آنها، الگوریتمی کلاسیک طراحی شد که مدار ۵۳-کیوبیتی گوگل را در مدت زمان یک روز شبیه‌سازی می‌کرد [۱۱]. بعد از آن هم الگوریتم‌های بهتری برای این کار طراحی شدند.

البته گروه گوگل در سال ۲۰۲۴ آزمایش فوق را روی تراشه‌ی ۱۰۵-کیوبیتی اخیر خود نیز تکرار و ادعا کرد که شبیه‌سازی کلاسیک این آزمایش دیگر امکان‌پذیر نیست. با این حال بعید نیست که با پیشرفت در طراحی الگوریتم‌های شبیه‌سازی، ادعای آنها باز هم نقض شود [۱۷].

(ج) نکته‌ی مهم دیگر درباره‌ی ادعای گروه گوگل مسأله‌ی نویز است. حتی اگر محک آنتروپی متقاطع را بپذیریم، به هر حال تراشه‌های گوگل نویزی هستند و خروجی آزمایش آنها دارای حدی از نویز است. با این حال منظور

[54] Gradient descent
[55] Random circuit sampling
[56] Cross-Entropy Benchmarking (XEB)

دانشگاه	مدرسین	سال شروع درس
U of Oxford	Artur Ekert	۱۹۹۶-۹۷
UC Berkeley	Umesh Vazirani	۱۹۹۷-۹۸
Caltech	John Presekill	۱۹۹۷-۹۸
MIT	Isaac Chuang, Neil Gershenfeld	۱۹۹۸-۹۹

جدول ۳: بعضی از اولین درس‌هایی که در مورد محاسبات کوانتومی در دانشگاه‌های مختلف جهان ارائه شدند. ارائه‌ی چنین درسی در ایران تقریباً هم‌زمان با کشورهای دیگر شروع شد.

گروه گوگل از شبیه‌سازی کلاسیک، شبیه‌سازی بدون نویز و دقیق است که چندان منصفانه به نظر نمی‌رسد. در بالا دیدیم که گاهی نویز باعث می‌شود یک مدار کوانتومی قابل شبیه‌سازی شود و احتمالاً اگر پارامتر نویز را در نظر بگیریم شبیه‌سازی کلاسیک کار ساده‌تری باشد.

(د) نکته‌ی دیگر این است که محاسبات مربوط به نمونه‌گیری از مدارهای تصادفی هیچ مسأله‌ی مفیدی را حل نمی‌کند و صرفاً دنباله‌هایی تصادفی تولید می‌کند. البته کار گروه گوگل به عنوان قدم اول در اثبات عملی بودن مزیت کوانتومی قابل تحسین است، ولی خود مزیتی کوانتومی (حداقل با آن تعریفی که قبلاً ذکر شد) نیست.

در اینجا باید به نمونه‌گیری بوزونی[۵۷] نیز اشاره کنیم که مسأله‌ایست مشابه با نمونه‌گیری از مدارهای تصادفی ولی برای سیستم‌های اپتیکی [۱]. نکات فوق در مورد نمونه‌گیری بوزونی نیز کم و بیش قابل ذکر هستند از جمله این که ادعا می‌شد که شبیه‌سازی آنها امکان‌پذیر نیست ولی بعدها الگوریتم‌های شبیه‌سازی متنوعی برای آنها طراحی و اجرا شدند.

۵ توسعه‌ی فناوری کوانتومی در کشور

محاسبات کوانتومی از اواسط دهه‌ی ۱۹۹۰ به عنوان مدل جدیدی از محاسبه مورد توجه جدی قرار گرفته است. از همان دوره برنامه‌ریزی برای تربیت نیروی انسانی به عنوان بازوی پیشرفت در این زمینه در دانشگاه‌های تراز اول شروع شد. ظاهراً اولین درس رسمیِ محاسبات کوانتومی توسط آرتور اِکِرت[۵۸] در سال تحصیلی ۹۷-۱۹۹۶ در دانشگاه آکسفورد ارائه شد. در سال‌های بعد دروس مشابهی در دانشگاه‌های دیگر طراحی و ارائه شدند که لیست بعضی از این دروس در جدول ۳ آمده است.

در ایران درس محاسبات کوانتومی برای اولین بار در سال تحصیلی ۲۰۰۰-۱۹۹۹ در دانشکده‌ی فیزیک دانشگاه صنعتی شریف توسط وحید کریمی‌پور ارائه شد. همان‌طور که می‌بینیم تدریس این موضوع در ایران با فاصله‌ی کمی از کشورهای دیگر شروع شده است. با این حال، وضعیت نیروی انسانیِ متخصص در این زمینه در کشور قابل قبول نیست. انتظار بر این است که با گذشت بیش از ۲۵ سال از ارائه‌ی اولین درس محاسبات کوانتومی در کشور، حداقل ۵۰ متخصص شناخته‌شده در این زمینه در کشور داشته باشیم. به علاوه توقع داریم که دروس متنوعی در زمینه‌ی تکنولوژی کوانتومی در دانشگاه‌های کشور طراحی و ارائه شده باشند. با این حال متأسفانه تعداد متخصصین این رشته

[57] Boson sampling
[58] Artur Ekert

در کشور به زحمت از تعداد انگشتان یک دست عبور می‌کند و تعداد دروس با کیفیت در این زمینه کمتر از تعداد انگشتان یک دست است.

در سال‌های اخیر تکنولوژی کوانتومی مورد توجه سیاست‌گذاران و مسؤولین کشور در بخش‌های مختلف قرار گرفته است. با این حال، راهبرد توسعه‌ی آن در کشور معیوب است. متأسفانه برنامه‌ریزی در این زمینه حتی در بخش دانشگاهی و تحت امر وزارت علوم، تحقیقات و فناوری نیز طبق نظر متخصصین این رشته انجام نمی‌شود و سیاست‌های اتخاذ شده در این بستر منجر به تربیت نیروی انسانی متخصص نخواهد شد.

استفاده از مواهب فناوری کوانتومی در کشور مستلزم توجه جدی سیاست‌گذاران به دو امر مهم زیر است:

- محاسبات کوانتومی شاخه‌ای کاملاً تخصصی است و پیچیدگی‌ها و ظرافت‌های خاص خود را دارد. لذا امکان‌سنجی استفاده از محاسبات کوانتومی و دیگر تکنولوژی‌های کوانتومی در کشور کار افراد خبره‌ای است که اطلاعات خود را از منابع دست اول دریافت می‌کنند و نه افرادی که تخصص چندانی در این زمینه ندارند و براساس شنیده‌های نادرست یا نادقیق تصمیم‌گیری می‌کنند.

  امکان‌سنجی و هدف‌گذاری در این زمینه باید توسط افرادی انجام شود که هم با نیازهای میان‌مدت و بلندمدت کشور آشنایی دارند و هم بر کاربردهای واقعی تکنولوژی کوانتومی مسلط هستند. بعضی از این کاربردها در میان‌مدت قابلیت تحقق دارند و بعضی از آنها در بلندمدت. علاوه بر مسأله‌ی زمان‌بندی، محدودیت‌ها، پتانسیل و نیازهای کشور مؤلفه‌های مهمی در الویت‌بندی اهداف کشور در راستای توسعه‌ی تکنولوژی کوانتومی هستند.

  رونویسی ناقص و اجرای ناقص‌تر برنامه‌های دیگر کشورها منجر به توسعه‌ی فناوری کوانتومی در کشور نخواهد شد. این امر مستلزم برنامه‌ریزی مبتنی بر نیازهای واقعی کشور است و باید توسط نیروی انسانی متخصص انجام گیرد.

- تربیت نیروی انسانی متخصص، به‌روز و باانگیزه چه در برنامه‌ریزی و چه در اجرای سیاست‌های توسعه‌ای امری غیر قابل انکار است. این امر بدون حمایت مؤثر از محققین و دانشجویان، و ارتباط تنگاتنگ آنها با مراکز و محققین بین‌المللی تحقق نمی‌یابد.

  تکنولوژی کوانتومی منبعث از شاخه‌های مختلفی از علم مانند فیزیک، شیمی، ریاضی، علوم کامپیوتر و مهندسی است. زیرشاخه‌هایی مانند الگوریتم، رمزنگاری، کدگذاری، هوش مصنوعی، مخابرات، اپتیک، الکترونیک و الکترومغناطیس همگی در توسعه‌ی فناوری کوانتومی مؤثر هستند و این امر مستلزم برنامه‌ی جامعی در جهت رشد بیش از پیش در همه‌ی این شاخه‌ها است. تمرکز صرف روی بعضی از این رشته‌ها منجر به توسعه‌ی پایدار این تکنولوژی در کشور نخواهد شد.

  متأسفانه نیروهای انسانی متخصص در کشور به دلایل گوناگون رانده می‌شوند، مهاجرت می‌کنند یا به کنجی می‌خزند. نتیجه‌ی این امر اتلاف منابع و به بیراهه رفتن استراتژی‌های توسعه در کشور می‌شود.

۶ جمع‌بندی

در این بخش به جمع‌بندی مطالب فوق و ذکر نکاتی که در بالا مغفول ماندند می‌پردازیم.

- کامپیوتر کوانتومی صرفاً یک کامپیوتر سریع نیست. در واقع ادوات کوانتومی فعلی در مقایسه با رایانه‌های کلاسیک بسیار کند هستند به این معنی که اعمال یک گیت دو-کیوبیتی روی آنها بسیار کندتر از اجرای یک

عملیات دو-بیتی روی یک رایانه‌ی کلاسیک است. محاسبات کوانتومی یک مدل محاسباتی کاملاً متفاوت است که حاصل نظریه‌ی فیزیک کوانتومی است. لذا کامپیوتر کوانتومی یک دستگاه محاسباتی است که براساس فیزیک کوانتومی ساخته می‌شود. به علاوه، یک کامپیوتر کوانتومی لزوماً نمی‌تواند هر مسأله‌ای را سریع‌تر از کامپیوترهای کلاسیک حل کند. برای بعضی مسائل خاص، الگوریتم‌های کوانتومی خاصی قابل طراحی است که آن مسائل را سریع‌تر از بهترین الگوریتم‌های کلاسیک فعلی حل می‌کند.

- در حال حاضر شرکت‌های گوناگونی در کشورهای مختلف روی نرم‌افزار و سخت‌افزار کوانتومی سرمایه‌گذاری کرده‌اند. در بخش سخت‌افزار، این شرکت‌ها از تکنولوژی‌های متفاوتی برای ساخت کامپیوتر کوانتومی استفاده می‌کنند. بعضی از این شرکت‌ها ادواتی کوانتومی ساخته‌اند که اطلاق عنوان کامپیوتر کوانتومی به آنها چندان صحیح نیست، چرا که اولاً این ادوات مقیاس بسیار کوچکی دارند و ثانیاً نویزی هستند. به علاوه، مسأله‌ی مقیاس‌پذیری این ادوات موضوع چالش برانگیزی است.

- تعداد کیوبیت‌ها معیار کاملی برای مقایسه‌ی ادوات کوانتومی نیست. مقدار نویز، توپولوژی و همبندی کیوبیت‌های دستگاه، سرعت اجرای گیت‌های کوانتومی، زمان پایداری و مقیاس‌پذیر بودن تکنولوژی از دیگر معیارهای مهم برای مقایسه‌ی ادوات محاسباتی کوانتومی است.

- استفاده از کدهای تصحیح خطای کوانتومی می‌تواند مسأله نویز در محاسبات کوانتومی را حل کند. با این حال پیاده‌سازی عملی آنها ساده نیست و تا کنون محقق نشده است. یکی از دلایل این امر مقیاس بسیار کوچک و در عین حال نویز زیاد ادوات کوانتومی فعلی است.

- تا محقق شدن اجرای کدهای تصحیح خطای کوانتومی می‌توانیم سعی کنیم که الگوریتم‌هایی طراحی کنیم که حتی در حضور نویز نیز کارا باشند. قابل توجه است که این الگوریتم‌ها باید پارامترهای خاصی داشته باشند. اگر عمق یک مدار کوانتومی زیاد باشد، خروجی آن در حضور نویز عاری از هر گونه اطلاعات است. همچنین، اگر عمق یک مدار کم باشد آنگاه می‌توان آن را روی یک کامپیوتر کلاسیک شبیه‌سازی کرد. لذا در حضور نویز پیاده‌سازی مدارهایی با معنی است که عمق آنها در بازه‌ی مشخصی قرار بگیرید. این بازه برحسب مقدار نویز و همبندی کیوبیت‌های دستگاه کوانتومی و در مقایسه با قدرت رایانه‌های کلاسیک تعیین می‌شود.

- پروتکل‌های تخفیف خطا[۵۹] نیز راهکاری برای اجرای الگوریتم‌های کوانتومی روی اداوات نویزی ارائه می‌دهند که در بالا به آنها نپرداختیم. با این حال، این پروتکل‌ها در دامنه‌ی خاصی از پارامترها کارایی دارند [۱۳، ۱۹]. لذا برای اجرای یک مدار کوانتومی خاص روی یک دستگاه باید پارامترهای آن مدار برای آن دستگاه و بر حسب پروتکل تخفیف خطای متناظر بهینه شوند. این کار احتمالاً بتواند اجرای دسته‌ی خاصی از الگوریتم‌های کوانتومی را روی اداوات نویزی فعلی در دامنه‌ی خاصی از پارامترها میسر کند.

- الگوریتم تجزیه‌ی شور یکی از اولین و مهم‌ترین الگوریتم‌های کوانتومی است برای تجزیه‌ی اعداد صحیح به عوامل اول آنها. در صورت اجرای این الگوریتم و بعضی از تعمیم‌های آن، بخش اعظمی از سیستم‌های رمزنگاری فعلی ناامن می‌شوند. این الگوریتم در حضور نویز قابلیت اجرا ندارد چون عمق مدار کوانتومی متناظر آن زیاد است.

[59] Error mitigation

- با ناامن شدن سیستم‌های رمزنگاری فعلی نیاز به طراحی روش‌های جدید رمزنگاری که در حضور کامپیوترهای کوانتومی نیز امنیت دارند، امری ضروری است. در این راستا دو پشنهاد عمده وجود دارد: یکی رمزنگاری کوانتومی و دیگری رمزنگاری پساکوانتومی.

  (۱) رمزنگاری کوانتومی براساس مخابرات کوانتومی و شامل مجموعه‌ای از پروتکل‌ها برای توزیع کلید کوانتومی[۶۰] است. در این پروتکل‌ها، مخابرات کوانتومی برای تولید و به اشتراک گذاشتن یک کلید امن به کار می‌رود. سپس آن کلیدِ امن به طور کلاسیک و با استفاده از روش‌هایی مانند پد یک‌بار مصرف[۶۱] برای مخابرات امن به کار برده می‌شود.

  پیاده‌سازی رمزنگاری کوانتومی در مقیاس بزرگ بسیار هزینه‌بر است و تا کنون محقق نشده است زیرا نیاز به زیرساخت‌هایی کوانتومی دارد که بعضی از چالش‌های نظری و عملی آن هنوز مرتفع نشده‌اند.

  (۲) رمزنگاری پساکوانتومی به مجموعه‌ای از پروتکل‌های رمزنگاری اطلاق می‌شود که حتی در حضور کامپیوترهای کوانتومی نیز امن هستند. این پروتکل‌ها کاملاً کلاسیک هستند و اجرای آنها نیاز به زیرساخت جدید چندانی ندارد. لذا، حداقل در مقیاس بزرگ، رمزنگاری پساکوانتومی بسیار عملی‌تر از رمزنگاری کوانتومی به نظر می‌رسد.

- الگوریتم کوانتومی گروور یک پایگاه داده را با فرض وجود دسترسیِ کوانتومی به آن جستجو می‌کند. شرط اخیر برای پایگاه‌های داده‌ی فعلی برقرار نیست. با این حال، برای بعضی مسائلِ جستجو این شرط قابل تحقق است. عمق مدارهای متناظر با این الگوریتم زیاد است و برای اجرای آنها باید کدهای تصحیح خطا پیاده‌سازی شوند. با این وجود، حتی در صورت پیاده‌سازی کدهای تصحیح خطا، اجرای الگوریتم جستجوی گروور لزوماً کارا نیست. نکته در این است که بهبود پیچیدگی محاسباتی تضمین شده توسط الگوریتم گروور نسبت به الگوریتم‌های کلاسیک از درجه‌ی دو است،[۶۲] و این مقدار از بهبود چندان زیاد نیست که در عمل بتواند کارا باشد. توجه کنید که همان‌طور که در بالا گفته شد، ادوات کوانتومی فعلی نسبت به رایانه‌های کلاسیک بسیار کند هستند. به علاوه، حجم محاسباتی الگوریتم‌های کوانتومی در صورت پیاده‌سازی کدهای تصحیح خطا بسیار بیشتر می‌شود. لذا بهبود درجه‌ی دو یا حتی درجه‌ی سه در الگوریتم‌های کوانتومی، لزوماً حل سریع‌تر مسائل را تضمین نمی‌کند [۴].

- یادگیری ماشین کوانتومی و بهینه‌سازی کوانتومی از کاربردهای محاسبات کوانتومی در کوتاه‌مدت و میان‌مدت محسوب می‌شوند. با این حال یادگیری ماشین کوانتومی روی داده‌های خاصی عملی به نظر می‌رسد. نکته در این است که دادن داده‌های کلاسیک با حجم بالا به عنوان ورودیِ الگوریتم‌های کوانتومی چالش برانگیز است. از طرف دیگر مشکل فلات لم‌یزرع باعث می‌شود که بخش اعظمی از الگوریتم‌های یادگیری ماشین کوانتومی در عمل کارا نباشند. همچنین در حضور نویز، عمق مدارهای کوانتومی متناظر باید در بازه‌ی خاصی قرار بگیرند. رعایت همه‌ی این نکات در طراحی الگوریتم‌های یادگیری ماشین کوانتومی که در عمل قابل پیاده‌سازی باشند ضروری است.

- شبیه‌سازی سیستم‌های کوانتومی یکی دیگر از کاربردهای مهم و بلکه مهم‌ترین کاربرد کامپیوترهای کوانتومی است. شبیه‌سازی کوانتومی علاوه بر بهبود فهم ما از سیستم‌های کوانتومی، به طراحی مواد از جمله داروها

[60] Quantum key distribution

[61] One-time pad

[۶۲] پیچیدگی محاسباتی الگوریتم گروور از مرتبه‌ی $\sqrt{n}$ و پیچیدگی محاسباتی الگوریتم‌های کلاسیک جستجو از مرتبه‌ی n است.

کمک خواهد کرد. به دلایلی که در بالا به آنها اشاره شد، پیاده‌سازی الگوریتم‌های شبیه‌سازی کوانتومی در کوتاه‌مدت و میان‌مدت چالش برانگیز است. با این حال، به نظر می‌رسد که اجرای این الگوریتم‌ها نسبت به الگوریتم‌های کوانتومی دیگر عملی‌تر باشد.

- مزیت کوانتومی عبارت است از حل عملی یک مسأله با استفاده از یک دستگاه کوانتومی به طوری که کامپیوترهای کلاسیک در عمل قادر به حل آن نباشند. به علاوه، علاقه‌مندیم که آن مسأله ساختگی نبوده و مسأله‌ای مفید باشد. با این تعریف، مزیت کوانتومی تا کنون محقق نشده است. به طور خاص نمونه‌گیری از مدارهای تصادفی و نمونه‌گیری بوزونی مزیت کوانتومی محسوب نمی‌شوند.

- توسعه‌ی فناوری کوانتومی در کشور مستلزم تربیت نیروی انسانی متخصص است. این تکنولوژی دارای پیچیدگی‌ها و ظرافت‌هایی است که به بعضی از آنها در بالا اشاره شده است. لذا نه تنها پیاده‌سازی عملی برنامه‌ها، بلکه حتی امکان‌سنجی و هدف‌گذاری درست در راستای استفاده از آن با مطالعه‌های سطحی بدست نمی‌آید و باید توسط متخصصین امر انجام شود.

References

[1] S. Aaronson and A. Arkhipov. The computational complexity of linear optics. In *Proceedings of the forty-third annual ACM symposium on Theory of computing*, pages 333–342, 2011.

[2] G. Q. AI and Collaborators. Quantum error correction below the surface code threshold. *Nature*, 638(8052):920–926, 2025.

[3] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell, et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.

[4] R. Babbush, J. R. McClean, M. Newman, C. Gidney, S. Boixo, and H. Neven. Focus beyond quadratic speedups for error-corrected quantum advantage. *PRX quantum*, 2(1):010103, 2021.

[5] M. Cain, Q. Xu, R. King, L. R. Picard, H. Levine, M. Endres, J. Preskill, H.-Y. Huang, and D. Bluvstein. Shor's algorithm is possible with as few as 10,000 reconfigurable atomic qubits. *arXiv preprint arXiv:2603.28627*, 2026.

[6] C. Gidney and M. Ekerå. How to factor 2048 bit rsa integers in 8 hours using 20 million noisy qubits. *Quantum*, 5:433, 2021.

[7] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, 1996.

[8] J. Jang-Jaccard, P. Caroff, E. Blezinger, V. Mulder, A. Mermoud, and V. Lenders. Quantum technologies: Trends and implications for cyber defense, 2026.

[9] J. R. McClean, S. Boixo, V. N. Smelyanskiy, R. Babbush, and H. Neven. Barren plateaus in quantum neural network training landscapes. *Nature communications*, 9(1):4812, 2018.

[10] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[11] E. Pednault, J. A. Gunnels, G. Nannicini, L. Horesh, and R. Wisnieff. Leveraging secondary storage to simulate deep 54-qubit sycamore circuits. *arXiv preprint arXiv:1910.09534*, 2019.

[12] J. Preskill. Quantum computing in the nisq era and beyond. *Quantum*, 2:79, 2018.

[13] Y. Quek, D. Stilck França, S. Khatri, J. J. Meyer, and J. Eisert. Exponentially tighter bounds on limitations of quantum error mitigation. *Nature Physics*, 20(10):1648–1658, 2024.

[14] M. Schuld and F. Petruccione. *Machine learning with quantum computers*, volume 676. Springer, 2021.

[15] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.

[16] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. *Physical review A*, 52(4):R2493, 1995.

[17] B. Wold and V. Kasirajan. Revisiting quantum supremacy: Simulating sycamore-class circuits using hybrid cpu/gpu hpc workloads. *arXiv preprint arXiv:2512.07311*, 2025.

[18] Y. Yan, Z. Du, J. Chen, and X. Ma. Limitations of noisy quantum devices in computing and entangling power. *npj Quantum Information*, 11(1):188, 2025.

[19] Z. Zimborás, B. Koczor, Z. Holmes, E.-M. Borrelli, A. Gilyén, H.-Y. Huang, Z. Cai, A. Acín, L. Aolita, L. Banchi, et al. Myths around quantum computation before full fault tolerance: What no-go theorems rule out and what they don't. *arXiv preprint arXiv:2501.05694*, 2025.