رایانش کوانتومی

سلمان ابوالفتح بیگی*

کلیسای ساگرادا فامیلیا (Sagrada Familia) یکی از مشهورترین بناهای اسپانیا محسوب می‌شود. ساخت این کلیسا توسط آنتونی گائودی (Antoni Gaudi) در سال ۱۸۸۳ شروع شد و انتظار می‌رود در سال ۲۰۲۶ یعنی صد سال پس از مرگ معمارش به پایان برسد. یکی از دلایلِ به درازا کشیدن اتمام بنا پیچیدگی‌ها و ظرافت‌هایی است که گائودی در طراحی آن به کار برد. او اعتقاد داشت که هیچ ساختاری زیباتر از تنهٔ یک درخت یا اسکلت انسان نیست و در معماری با تکیه به دانسته‌های هندسی‌اش از طبیعت الهام می‌گرفت. این دیدگاه گائودی در معماریِ قسمت اصلی کلیسا کاملاً به چشم می‌خورد. گنبد این بخش بر روی تعداد زیادی ستون نازک قرارگرفته است. با پیوستن چند ستون نازک، ستون‌های دیگری تشکیل شده‌اند و این روند ادامه پیدا می‌کند تا به ستون‌های اصلی گنبد که روی زمین قرار گرفته‌اند می‌رسد. این ساختار شاخه‌های سربه‌فلک کشیدهٔ درختان جنگل را تداعی می‌کند. در طراحی این بخش، انحنایی که هر یک ستون‌ها باید داشته باشد و همچنین نحوهٔ به هم پیوستن آنها به طوری که بنا ساختاری پایدار داشته باشد، مسئلهٔ پیچیده‌ای است که حل آن با ابزارهای محاسباتی قرن نوزدهم غیرممکن به نظر می‌رسد. گائودی به جای انجام محاسبات از یک ماکت برای تعیین ساختار پایدار ستون‌ها کمک گرفت. او به ازای هر ستون طنابی متناسب با طول آن در نظر گرفت. طناب‌های اولیه را به سقف ماکت متصل کرد و طناب‌های متناظر با ستون‌های به هم پیوسته را به هم گره زد. در آخر وزنه‌هایی با جرم مشخص را به طناب‌های متناظر با ستون‌های متصل به زمین آویزان کرد. بقیهٔ کار را نیروی جاذبه انجام داد و انحنای هر ستون مشخص شد.

وقتی نیروی f به جسمی با جرم m وارد می‌شود، جسم بنابر قوانین نیوتن با شتاب a در راستای نیرو حرکت می‌کند به طوری که $f = ma$. گویی طبیعت قبل از حرکت جسم معادلهٔ $f = ma$ را برای مجهول a حل و شتاب آن را محاسبه می‌کند. می‌توان برای حل محاسبات پیچیده‌تر نیز همانند معادلات خطی آزمایش‌هایی طراحی کرد به گونه‌ای که جواب آزمایش، حاصل محاسبات را مشخص کند. مسئلهٔ طراحی ستون‌های ساگرادا فامیلیا و ماکت گائودی مثالی از چنین محاسبه و آزمایشی است.

* پژوهشکدهٔ ریاضیات.

سلمان ابوالفتح بیگی

گاهی محاسبه از طراحی و اجرای آزمایش ساده‌تر است. برای مثال محاسباتی را که در تحلیل مدارهای الکتریکی پیش می‌آیند می‌توان به صورت مستقیم و بدون دسترسی به مدار انجام داد. امروزه نرم‌افزارهایی وجود دارند که به تنهایی آزمایشگاهی برای تحلیل مدارهای الکتریکی محسوب می‌شوند. کافی است اجزای یک مدار را به عنوان ورودی به نرم‌افزار داد تا براساس معادلات الکترومغناطیس، مدار را بررسی و پارامترهایش را محاسبه کند. نکتهٔ دیگر این است که رایانه‌ای که این نرم‌افزار را اجرا می‌کند خود نیز براساس قوانین الکترومغناطیس ساخته شده است؛ یعنی، از فیزیک برای شبیه‌سازی فیزیک استفاده می‌کنیم.

آیا می‌توان بخش‌های دیگر فیزیک مانند مکانیک را نیز شبیه‌سازی کرد؟ رایانه چه قابلیت‌هایی باید داشته باشد تا بتواند هر آزمایش فیزیکی را تحلیل کند؟ پر واضح است که تا زمانی که درک کاملی از فیزیک حاکم بر طبیعت نداشته باشیم عبارت «هر آزمایش فیزیکی» همراه با ابهام است. پس نباید انتظار جوابی کامل و دقیق را برای این سؤال داشته باشیم. نکتهٔ دیگر این است که باید مشخص شود منظور از رایانه در این سؤال چیست.

ماشین تورینگ (Turing machine) مدلی فرضی برای محاسبه است و تعریفی دقیق و ریاضی‌وار از رایانه به دست می‌دهد. نظریهٔ چرچ-تورینگ (Church-Turing thesis) نه تنها مدل ماشین تورینگ را توجیه‌پذیر می‌کند، بلکه جوابی برای سؤال فوق نیز ارائه می‌دهد.

نظریهٔ چرچ-تورینگ: هر محاسبه‌ای که با آزمایشی فیزیکی قابل اجراست، به وسیلهٔ ماشین تورینگ نیز قابل پیاده‌سازی است.

به دلیل همان ابهامی که در تعریف آزمایش فیزیکی وجود دارد، این نظریه قابل اثبات نیست. با وجود این، تاکنون مثال نقضی برای آن یافت نشده

است و ماشین تورینگ به عنوان مدل جهانی محاسبه در نظرگرفته می‌شود.

آزمایش‌هایی که تا اینجا از آنها صحبت شد همگی در محدودهٔ فیزیک کلاسیک قرار دارند. در اوایل قرن گذشته پدیده‌هایی در طبیعت مشاهده شد که با نتایج مبتنی بر فیزیک کلاسیک ناسازگار بودند. تابش جسم سیاه (black body radiation) و اثر فتوالکتریک (photoelectric effect) مثال‌هایی بودند که فیزیک کلاسیک توصیف معقولی برای آنها ارائه نمی‌کرد و ایده‌های اولیهٔ نظریهٔ فیزیک کوانتومی از تحلیل این پدیده‌ها به وجود آمدند. براساس فیزیک کوانتومی، نظریه‌های کلاسیک فیزیک مانند مکانیک نیوتنی صرفاً تقریبی از واقعیت را بیان می‌کنند و این تقریب حداقل در تحلیل برهم‌کنش‌های زیراتمی ناتوان است. در نتیجه، رابطهٔ بین فیزیک و محاسبه را می‌توان در مورد فیزیک کوانتومی نیز در نظرگرفت.

آیا ماشین تورینگ قابلیت پیاده‌سازی محاسبات مربوط به آزمایش‌های فیزیک کوانتومی را دارد؟

برای پاسخ به این سؤال باید با مفاهیم اصلی فیزیک کوانتومی آشنا شویم. برای توصیف هر سیستم فیزیکی ابتدا باید فضای حالات آن سیستم را مشخص کرد. برای مثال، در مکانیک کلاسیک فضای حالات یک ذره با مکان و تکانه‌اش بیان می‌شود. لذا این فضا یک فضای حقیقی شش بعدی است (سه مؤلفه برای مکان و سه مؤلفه برای تکانه) و حالت ذره در هر لحظه از زمان با یک نقطه در این فضا مشخص می‌شود. در نظریهٔ فیزیک کوانتومی، به ازای هر سیستم فیزیکی یک فضای هیلبرت[1] وجود دارد. همچنین فضای هیلبرت متناظر با سیستم ترکیبی دو ذره از ضرب تانسوری[2] فضاهای آن دو ذره به دست می‌آید. حالت سیستم فیزیکی در هر لحظه از زمان با برداری به طول واحد در فضای هیلبرت متناظر توصیف می‌شود. نکتهٔ بعدی، تحول حالت یک سیستم در طول زمان است. این تحول با خم در فضای حالات بیان می‌شود. در فیزیک کوانتومی این خم از معادلهٔ شرودینگر (Schrödinger equation) به دست می‌آید:

$$i\hbar\frac{\partial}{\partial t}\psi t = H\psi_{\circ}$$

در این معادلهٔ دیفرانسیل، ψ_t حالت سیستم در زمان t است، $i=\sqrt{-1}$، و $\hbar$ ثابت پلانک (Plank's constant) است. همچنین H عملگری خطی و هرمیتی است که روی فضای هیلبرت متناظر اثر می‌کند و به آن همیلتونی (Hamiltonian) گویند. همیلتونی در واقع نوع برهم‌کنش ذرات مختلف سیستم را توصیف می‌کند. اگر H مستقل از زمان باشد، جواب معادلهٔ شرودینگر

$$\psi_t = e^{\frac{it}{\hbar}H}\psi$$

است.[3] با توجه به هرمیتی بودن H، $U=e^{-\frac{it}{\hbar}H}$ عملگری یکانی و حافظ ضرب داخلی است. پس بیان دیگر معادلهٔ شرودینگر این است که تحول زمانی سیستم‌های کوانتومی توسط عملگرهای یکانی مشخص می‌شود. تا اینجا فضای حالت سیستم‌های کوانتومی، سیستم‌های ترکیبی و تحول زمانی آنها را توضیح دادیم. آخرین مؤلفهٔ نظریهٔ فیزیک کوانتومی کمیت‌ها و مشاهدات فیزیکی هستند. هرکمیت فیزیکی با یک پایهٔ متعامد یکه در فضای هیلبرت متناظر مشخص می‌شود. اگر سیستم در حالت ψ باشد، با اندازه‌گیری آن در پایهٔ متعامد یکهٔ $\{v_{\circ}, v_{۱}, \ldots\}$ حاصل با احتمال $|(v_k,\psi)|^{۲}$ برابر k خواهد بود[1] که در آن منظور از (v_k,ψ) ضرب داخلی بردارهای v_k و ψ است. اگر حاصل اندازه‌گیری k باشد حالت سیستم از ψ به v_k تغییر می‌کند. پس برخلاف فیزیک کلاسیک، در فیزیک کوانتومی با اندازه‌گیری (مشاهدهٔ) یک سیستم در آن تغییر به وجود می‌آید.

به مسئلهٔ شبیه‌سازی فیزیک کوانتومی روی ماشین تورینگ برگردیم. هر آزمایش فیزیکی دنباله‌ای از تحول‌های زمانی و اندازه‌گیری‌هاست. برای مثال ممکن است در یک آزمایش، ذرات یک سیستم ابتدا برای مدتی برهم‌کنش داشته باشند و بعد یک اندازه‌گیری انجام دهیم. سپس برحسب این که حاصل اندازه‌گیری چه باشد برهم‌کنش دیگری را روی سیستم اعمال کنیم و الی آخر. در فیزیک کوانتومی حالت اولیهٔ سیستم با یک بردار واحد مشخص می‌شود و هر یک از تحول‌های زمانی، متناظر با یک عملگر یکانی است. پس حالت سیستم بعد از یک تحول زمانی از ضرب یک ماتریس در یک بردار به دست می‌آید. همچنین اندازه‌گیری متناظر با یک پایهٔ متعامد یکه است و حاصل آن با یک توزیع احتمال مشخص می‌شود. این توزیع احتمال از محاسبهٔ تعدادی حاصلضرب داخلی به دست می‌آید و حالت سیستم به یکی از اعضای پایه تغییر پیدا می‌کند. بنابراین، شبیه‌سازی یک آزمایش فیزیک کوانتومی با ضرب ماتریسی و محاسبهٔ حاصلضرب داخلی امکان‌پذیر است. این دو عمل بر روی یک رایانهٔ معمولی و در واقع روی ماشین تورینگ قابل اجرا هستند. بنابراین فیزیک کوانتومی مثال نقضی برای نظریهٔ چرچ-تورینگ نیست و آن را می‌توان روی ماشین تورینگ شبیه‌سازی کرد.

توجه کنید که شبیه‌سازی سیستم‌های کوانتومی بسیار پرکاربردتر از شبیه‌سازی آزمایش‌های فیزیک کلاسیک است. آزمایش‌های فیزیک کوانتومی معمولاً روی ذرات زیراتمی انجام می‌شوند و در نتیجه کنترل شرایط آزمایشگاه به طوری که خطاهای محیطی تأثیری روی حاصل آزمایش نداشته باشند کار سخت و پرهزینه‌ای است. توانایی شبیه‌سازی چنین آزمایشی این امکان را فراهم می‌سازد که بدون داشتن فناوری پیشرفته تقریبی از حاصل آن را داشته باشیم. سؤالی که در اینجا پیش می‌آید این است که آیا شبیه‌سازی سیستم‌های کوانتومی واقعاً کم هزینه است؟ برای پاسخ به این سؤال ابتدا نگاهی دقیق‌تر به شبیه‌سازی فیزیک کلاسیک خواهیم داشت.

فضای حالت یک سیستم کوانتومی با یک فضای هیلبرت مشخص می‌شود. در فیزیک کلاسیک، فضای حالت در کلی‌ترین شکل خود یک مجموعهٔ دلخواه است. کوچک‌ترین سیستم کلاسیک «بیت» نامیده می‌شود و متناظر با یک مجموعهٔ دو عضوی است که اعضای آن با $\{۰, ۱\}$ نمایش داده می‌شوند. فضای حالت متناظر با n بیت $\{۰, ۱\}^n$ است. همچنین تحول زمانی متناظر با n بیت با یک نگاشت $f : \{۰, ۱\}^n \to \{۰, ۱\}^n$

۱. فضای هیلبرت یک فضای برداری ضرب داخلی مختلط است که با متری که ضرب داخلی آن القا می‌کند کامل است.

۲. ضرب تانسوری دو فضای برداری با بعدهای d و d' یک فضای برداری با بعد dd' است.

۳. منظور از e^X که در آن X یک عملگر خطی است، $e^X = \sum_{k=۰}^{\infty} \frac{۱}{k!}X^k$ است.

۱. از آنجا که ψ برداری واحد است $|(\psi,\psi)|^{۲} = ۱$ و $\sum_k |(v_k,\psi)|^{۲}$.

مشخص می‌شود. اگر حالت اولیهٔ سیستم $x \in \{0,1\}^n$ باشد، حالت آن پس از تحول زمانی، $f(x)$ خواهد شد.

در یک سیستم فیزیکی، هر ذره فقط با ذرات مجاورش برهم‌کنش دارد. براین اساس در یک بازهٔ زمانی به اندازهٔ کافی کوچک حداکثر تعداد محدودی ذره برهم‌کنش دارند. پس با تقسیم تحول به m بازهٔ زمانی فرض می‌کنیم $f = g_m \circ g_{m-1} \cdots \circ g_1$ به طوری که g_iها حداکثر روی (برای مثال) سه مؤلفه اثر نابدیهی[1] دارند. با داشتن نگاشت $g : \{0,1\}^3 \to \{0,1\}^3$ و $y \in \{0,1\}^3$، برای محاسبهٔ $g(y)$ روی یک ماشین تورینگ تعداد محدودی مرحله کافی است. بنابراین برای محاسبهٔ $f(x) = g_m \circ g_{m-1} \cdots \circ g_1(x)$ کافی است ابتدا $g_1(x)$ را به دست بیاوریم. این کار در حداکثر $O(n)$ قدم قابل انجام است. بعد از روی $g_1(x)$، $g_2(g_1(x))$ را محاسبه کرده و ادامه می‌دهیم تا این که به $f(x)$ برسیم. با این روش تعداد مرحله‌های لازم $O(mn)$ خواهد بود.

حال تحول زمانی ذرات کوانتومی را در نظر بگیرید. فضای حالت کوچک‌ترین سیستم کوانتومی یک فضای هیلبرت دوبعدی است که بیت کوانتومی (کیوبیت) نامیده می‌شود. از آنجا که فضای هیلبرتِ متناظر با یک سیستم ترکیبی از ضرب تانسوری فضاهای کوچک‌تر به دست می‌آید، فضای حالت n کیوبیت یک فضای 2^n بعدی است. همچنین براساس معادلهٔ شرودینگر تحول زمانی این n کیوبیت به وسیلهٔ یک ماتریس یکانی U با اندازهٔ $2^n \times 2^n$ مشخص می‌شود. اگر حالت اولیه ψ باشد، پس از تحول زمانی سیستم به حالت $U\psi$ می‌رود. $U\psi$ یک بردار به طول 2^n است و برای به دست آوردن آن حداقل 2^n قدم لازم است. حتی اگر مانند حالت قبل نیز فرض کنیم $U = V_m V_{m-1} \cdots V_1$ که در آن هر یک از V_iها عملگری است یکانی که حداکثر روی سه کیوبیت اثر می‌کند، باز محاسبهٔ $U\psi$ در $O(mn)$ مرحله امکان‌پذیر نیست و در حالت کلی به 2^n قدم نیاز داریم. بنابراین، شبیه‌سازی یک سیستم کوانتومی دلخواه شامل $n = 100$ کیوبیت با $m = 10000$، قرن‌ها طول می‌کشد و رویایی بیش نیست. پیاده‌سازی فیزیک کوانتومی بر روی ماشین تورینگ گرچه امکان‌پذیر است، به دلیل حجم بسیار زیاد محاسبات عملی به نظر نمی‌رسد.

بار دیگر به مثال نرم‌افزارهای شبیه‌سازی مدار بر می‌گردیم. در آنجا اشاره شد که رایانه‌ای که نرم‌افزار را اجرا می‌کند خود براساس قوانین الکترومغناطیس ساخته شده است و از خود فیزیک برای شبیه‌سازی فیزیک کمک گرفته می‌شود. به طور دقیق‌تر، از فیزیک کلاسیک برای شبیه‌سازی فیزیک کلاسیک استفاده می‌شود. در قدم بعدی، فیزیک کوانتومی را به وسیلهٔ فیزیک کلاسیک شبیه‌سازی کردیم و دیدیم که گرچه امکان‌پذیر است، به دلیل پیچیدگی‌های موجود، کاربردی نیست. ریچارد فاینمن (Richard Feynman) برای اولین بار در سال ۱۹۸۲ این ایده را مطرح کرد که برای شبیه‌سازی سیستم‌های کوانتومی، به جای فیزیک کلاسیک از خود فیزیک کوانتومی کمک بگیریم. او پیشنهاد داد که کامپیوتری بسیازیم که براساس اصول فیزیک کوانتومی ساخته شود. در دههٔ ۱۹۹۰ ایدهٔ رایانش کوانتومی نه تنها برای شبیه‌سازی سیستم‌هایی کوانتومی، بلکه برای حل مسائل کلاسیک نیز پیگیری شد تا جایی که در سال ۱۹۹۴ پیتر شور (Peter Shor) الگوریتمی کوانتومی طراحی کرد که یک عدد طبیعی را به طور بهینه به عوامل اولش تجزیه می‌کند.[1] از آن سال به بعد ایدهٔ رایانش کوانتومی جدی‌تر پیگیری شد.

نه تنها در مسئله‌های شبیه‌سازی، رایانش و طراحی الگوریتم بلکه در هر مسئلهٔ دیگر مبتنی بر فیزیک می‌توان مفاهیم کوانتومی را وارد کرد. امروزه نظریهٔ بازی‌ها، کدگذاری، رمزنگاری، پیچیدگی محاسبات، کنترل، مخابرات و نظریهٔ اطلاعات همگی در حالت کوانتومی مورد مطالعه قرار می‌گیرند. برای مثال نظریهٔ اطلاعات، علم چگونگی استفادهٔ بهینه از منابع مخابراتی برای انتقال اطلاعات است. ارتباط آن با فیزیک در آنجا ظاهر می‌شود که اطلاعات (برای مثال) با امواج رادیویی فرستاده می‌شود و کدگذاری و کدبرداری آن در فرستنده و گیرنده طبق اصول فیزیک کلاسیک انجام می‌شود. حال می‌توان پرسید که آیا کدگذاری و کدبرداری کوانتومی روشی بهتر برای انتقال اطلاعات فراهم می‌کند؟ این پرسش نظریهٔ اطلاعات کوانتومی را به وجود آورده است. مثال دیگر رمزنگاری است. از اصول فیزیک کوانتومی نتیجه می‌شود که سیستم‌های کوانتومی قابل کپی‌برداری نیستند (The no-cloning theorem). پس مکالمهٔ دو نفر از طریق یک کانال مخابراتی کوانتومی را نمی‌توان به طوری که آن دو نفر متوجه نشوند شنود کرد. زیرا شنودکننده ابتدا باید یک کپی از اطلاعات کوانتومی ردوبدل شده را برای خود فراهم و سپس آنها را رمزگشایی کند. به این ترتیب به نظر می‌رسد که رمزنگاری کوانتومی امنیت بیشتری را برای انتقال داده‌ها فراهم می‌کند.

آیا روزی کامپیوتر کوانتومی و ابزارهای کوانتومی برای انتقال اطلاعات و رمزنگاری ساخته خواهند شد؟ عده‌ای اعتقاد دارند که این ایده‌ها همواره در حد نظری باقی خواهند ماند. ولی شاید دلایل آنها همگی همانند ادعای وجود نداشتن کد کوانتومی برای تصحیح خطاهای محیطی[2] باشد که توسط پیتر شور نقض شد. امروزه برای اجرای پروتکل‌های کوانتومی و رایانش کوانتومی در محیط آزمایشگاه تلاش‌های بسیاری می‌شود. از جملهٔ این آزمایش‌ها می‌توان به اجرای الگوریتم شور برای تجزیهٔ عدد ۲۱ در دانشگاه بریستول (Bristol) اشاره کرد. همچنین سال گذشته شرکت سیستم‌های دی-ویو (D-Wave Systems Inc) ادعا کرد که یک کامپیوتر کوانتومی ۱۲۸ کیوبیتی ساخته است.[3] امروزه با تکنولوژی پیشرفتهٔ تارهای نوری، پروتکل‌های رمزنگاری کوانتومی مانند توزیع کلید (quantum key distribution) را می‌توان بین دو نفر با فاصلهٔ ۱۰۰ کیلومتر انجام داد. به تازگی اجرای پروتکل فرابرد کوانتومی (quantum teleportation) در فضای آزاد و در عرض دریاچهٔ چینگهای (Qinghai lake) با فاصلهٔ ۹۷ کیلومتر گزارش شده است.

به رغم تلاش‌های فراوانی که در دو دههٔ گذشته برای فهم و گسترش رایانش کوانتومی و نظریهٔ اطلاعات کوانتومی شده است هنوز سؤال‌های بسیار زیادی بی‌پاسخ مانده‌اند. نیاز به تحقیقات گسترده در رایانش کوانتومی، بسیاری از دانشگاه‌ها و مراکز تحقیقاتی را تشویق به سرمایه‌گذاری در این زمینه کرده است. این تحقیقات پیوندی واقعی بین ریاضیات، علوم کامپیوتر و فیزیک برقرار کرده‌اند که در فهم هر یک از آنها نیز کمک شایانی می‌کنند. امید است پیشرفت‌های علمی و عملی در این زمینه انقلابی در رایانش به وجود آورند.

۱. منظور این است که x و $g_i(x)$ غیراز سه مؤلفه مشخص در بقیهٔ $n-3$ مؤلفه برابرند.

۱. الگوریتم‌های کلاسیک شناخته شده برای این کار هیچ کدام در زمان چندجمله‌ای کار نمی‌کنند.

۲. منظور وجود error correcting code است.

۳. این ادعا توسط محققان مستقل تأیید نشده است.