محاسبات کوانتمی (۲۲۶۷۱) ترم بهار ۱۳۹۱-۱۳۹۰

مدرس: سلمان ابوالفتح بیگی نویسنده: سلمان ابوالفتح بیگی

جلسه ۱

محاسبات کوانتمی[۱] علم ساخت و استفاده از کامپیوتری است که بر پایه‌ی اصول مکانیک کوانتم قرار گرفته است. شروع این نظریه را می‌توان به نکته‌ی پایه‌ای نسبت داد که ریچارد فاینمن[۲] در سال ۱۹۸۲ به آن اشاره کرد: «به نظر می‌رسد که مشکلاتی اساسی در راستای شبیه سازی سیستم‌های کوانتمی با استفاده از کامپیوترهای کلاسیک وجود دارد.» فاینمن پیشنهاد کرد که برای این کار از کامپیوتری استفاده شود که خود نیز «کوانتمی» کار کند. از این نظر کامپیوتر کوانتمی را می‌توان یک آزمایشگاه مکانیک کوانتم دانست.

برای شروع نظریه محاسبات کوانتمی اولین قدم مطالعه‌ی اصول مکانیک کوانتم است. در این جلسه ابتدا اجزای مهم این اصول را به طور خلاصه دوره می‌کنیم.

۱ معادله شرودینگر

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

معادله شرودینگر[۳] نقش قوانین نیوتن در فیزیک کوانتم را دارد. برای فهمیدن این معادله با فرمول بندی همیلتونی مکانیک کلاسیک[۴] شروع می‌کنیم.

۱.۱ مکانیک همیلتونی

ذره‌ای با جرم m را در نظر بگیرد که در یک فضای یک بعدی در حرکت است. مکان این ذره را با q و تکانه[۵] آن را با p نمایش می‌دهیم و فرض می‌کنیم که ذره در پتانسیل $V = V(q,t)$ قرار دارد. در این صورت انرژی کل ذره برابر است با

$$H = T + V$$

که $T = \frac{p^2}{2m}$ انرژی جنبشی آن است. دو معادله‌ی زیر را در نظر بگیرید.

$$\begin{cases} \dot{q} = \frac{\partial H}{\partial p} \\ \dot{p} = -\frac{\partial H}{\partial q} \end{cases} \tag{۱}$$

---

[۱] Quantum computation
[۲] Rechard Feynman
[۳] Schrödinger Equation
[۴] Hamiltonian mechanics
[۵] Momentum

در اینجا منظور از $\dot{x}$ مشتق تابع x نسبت به زمان (t) است ($\dot{x} = \frac{dx}{dt}$). از آنجا که V مستقل از p است، داریم

$$\frac{\partial H}{\partial p} = \frac{\partial T}{\partial p} = \frac{p}{m}$$

و لذا معادله اول چیزی جز تعریف تکانه $p = m\dot{q}$ نیست. به طور مشابه از آنجا که T مستقل از q است از معادله‌ی دوم بدست می‌آوریم

$$\dot{p} = -\frac{\partial V}{\partial q}.$$

در نتیجه از ترکیب این دو داریم

$$m\ddot{q} = -\frac{\partial V}{\partial q}$$

که همان قانون دوم نیوتن است. در واقع (۱) فرمول بندی معادلی با $F = ma$ است که به آن فرمول بندی همیلتونی گفته می‌شود و کل مکانیک کلاسیک را می‌توان براساس آن پایه ریزی کرد.

در حالت کلی وقتی n ذره داریم، برای هر کدام از آنها مختصات p_i, q_i را در نظر می‌گیریم. در این صورت هر «حالت»[۶] سیستم بوسیله یک نقطه $(\bar{p}, \bar{q}) := (p_1, \dots, p_n, q_1, \dots, q_n) \in \mathbb{R}^{2n}$ مشخص می‌شود. فضای همه حالات سیستم (در اینجا $\mathbb{R}^{2n}$) «فضای فاز» نامیده می‌شود. همیلتونی H شرایط فیزیکی‌ای که بر این n ذره حاکم است را توصیف می‌کند، و در صورت دانستن حالت سیستم در زمان $t = 0$ از معادلات زیر می‌توان حالت سیستم را در هر زمان t بدست آورد.

$$\begin{cases} \dot{q}_i = \frac{\partial H}{\partial p_i} \\ \dot{p}_i = -\frac{\partial H}{\partial q_i} \end{cases} \tag{۲}$$

۲.۱ کمیت‌های فیزیکی

یک کمیت فیزیکی به هر حالت سیستم $(\bar{p}(t), \bar{q}(t))$ در زمان t یک عدد $f\left(\bar{p}(t), \bar{q}(t)\right)$ نسبت می‌دهد. در واقع هر کمیت فیزیکی مستقل از زمان، چیزی جز یک تابع $f : \mathbb{R}^{2n} \to \mathbb{R}$ روی فضای فاز نیست. در اینصورت تغییرات این کمیت در طول زمان را می‌توان بر حسب همیلتونی بدست آورد. برای این کار نیاز به تعریف کروشه پواسون[۷] داریم. برای دو تابع $f, g : \mathbb{R}^{2n} \to \mathbb{R}$ تعریف می‌کنیم

$$\{f, g\} := \sum_{i=1}^{n} \frac{\partial f}{\partial q_i} \cdot \frac{\partial g}{\partial p_i} - \frac{\partial f}{\partial p_i} \cdot \frac{\partial g}{\partial q_i}.$$

حال برای تغییرات کمیت f داریم

$$\begin{aligned} \frac{df}{dt} &= \frac{\partial f}{\partial t} + \sum_{i=1}^{n} \frac{\partial f}{\partial q_i} \cdot \dot{q}_i + \frac{\partial f}{\partial p_i} \cdot \dot{p}_i \\ &= \sum_{i=1}^{n} \frac{\partial f}{\partial q_i} \cdot \frac{\partial H}{\partial p_i} - \frac{\partial f}{\partial p_i} \cdot \frac{\partial H}{\partial q_i} \\ &= \{f, H\} \end{aligned}$$

[۶] State
[۷] Poisson bracket

که در سطر دوم از معادلات (۲) و این فرض که f مستقل از زمان است استفاده کردیم. به طور خلاصه داریم

$$\frac{df}{dt} = \{f, H\}. \tag{۳}$$

برای مثال کمیت انرژی کل سیستم توسط همیلتونی H بیان می‌شود و داریم $\frac{dH}{dt} = \{H, H\} = 0$. یعنی انرژی کل یک سیستم بسته تحت زمان ثابت است که این همان قانون بقای انرژی است.

۳.۱ مکانیک کوانتم

در مکانیک کوانتم فضای فاز به جای $\mathbb{R}^{2n}$ یک فضای هیلبرت[۸] است، یعنی یک فضای برداری روی اعداد مختلط که مجهز به ضرب داخلی است و با متری که از ضرب داخلی آن بدست می‌آید کامل[۹] است. در واقع فضای فاز نه همه فضای هیلبرت، بلکه فقط شامل بردارهای به طول واحد در این فضا ست. اگر فضای هیلبرت را با $\mathcal{W}$ و ضرب داخلی آن را با $\langle \cdot, \cdot \rangle$ نمایش دهیم، هر حالت سیستم برداری است $\psi \in \mathcal{W}$ که $\|\psi\|^2 = \langle \psi, \psi \rangle = 1$.

کمیت‌های فیزیکی در مکانیک کوانتم به جای توابع روی فضای فاز، عملگرهای خطی[۱۰] روی فضای هیلبرت هستند. برای مثال انرژی کل سیستم یک علمگر خطی خودالقاح (هرمیتی)[۱۱] $H : \mathcal{W} \to \mathcal{W}$ است. معادلات (۲) در مکانیک کوانتم به معادله شرودینگر تبدیل می‌شوند

$$i\hbar \frac{\partial \psi}{\partial t} = H\psi \tag{۴}$$

که در آن $i = \sqrt{-1}$ و $\hbar$ ثابت پلانک[۱۲] است. در حالت کلی H می‌تواند به زمان بستگی داشته باشد. ولی اگر مستقل از t باشد، خواهیم داشت

$$\psi(t) = e^{-\frac{it}{\hbar} H}\, \psi(0). \tag{۵}$$

اگر سیستم در حالت ψ باشد و $F : \mathcal{W} \to \mathcal{W}$ یک کمیت فیزیکی، «متوسط» F برابر خواهد بود با

$$\langle F \rangle := \langle F\psi, \psi \rangle.$$

[۸] Hilbert space
[۹] Complete
[۱۰] Linear operator
[۱۱] Hermitian
[۱۲] Planck's constant

در نتیجه تغییرات $\langle F\rangle$ در زمان را می‌توان محاسبه کرد.

$$\begin{aligned}\frac{d}{dt}\langle F\rangle &= \frac{d}{dt}\langle F\psi,\psi\rangle\\ &= \langle F\psi,\frac{d}{dt}\psi\rangle + \langle F\frac{d}{dt}\psi,\psi\rangle\\ &= \langle F\psi,-\frac{i}{\hbar}H\psi\rangle + \langle -\frac{i}{\hbar}FH\psi,\psi\rangle\\ &= \langle \frac{i}{\hbar}HF\psi,\psi\rangle - \langle \frac{i}{\hbar}FH\psi,\psi\rangle\\ &= \langle \frac{i}{\hbar}[H,A]\psi,\psi\rangle\\ &= \langle \frac{i}{\hbar}[H,A]\rangle\end{aligned}$$

که در سطر چهارم از $\langle \phi, X\phi'\rangle = \langle X^\dagger\phi,\phi'\rangle$ و اینکه $H = H^\dagger$ هرمیتی است استفاده کردیم. همچنین $[X,Y] = XY - YX$ براکت لی[۱۳] یا جابجاگر[۱۴] دو عملگر X و Y است. لذا رابطه

$$\frac{d}{dt}\langle F\rangle = \langle \frac{i}{\hbar}[H,A]\rangle$$

را به دست می‌آوریم که معادل کوانتمی (۳) است.

۲ مطالبی که در نظریه محاسبات کوانتمی مطالعه می‌شوند

همان طور که گفته شد اصلی‌ترین هدف نظریه محاسبات کوانتمی ساخت یک کامپیوتر کوانتمی است. این نظریه شامل مباحث مختلفی از جمله ذخیره اطلاعات، کدگذاری و پردازش آنها، انتقال اطلاعات (مخابرات) و رمزنگاری می‌شود. برای آشنا شدن با اجزای این نظریه بهتر است با نظریه‌ی کاملاً کلاسیک شروع کنیم.

۱.۲ نمایش اطلاعات

اولین قدم برای انجام هر محاسبه‌ای (حل هر مسأله‌ای) نمایش «داده‌های مسأله» است. برای مثال مسأله‌ی جمع دو عدد طبیعی را در نظر بگیرید. ما اعداد را با دنباله‌ای از ارقام نمایش می‌دهیم. مثلاً در سیستم دو-دویی[۱۵] هر عدد با دنباله‌ای از ارقام 0 و 1 مشخص می‌شود. نمایش داده‌ها به صورت دو-دویی فقط مختص اعداد نیست. سیستم یونیکد[۱۶] روشی است برای نمایش هر گونه اطلاعات متنی به صورت دنباله‌های 0 و 1. حتی اطلاعات صوتی و تصویری نیز از این قاعده مستثنی نیستند. توجه کنید که در اینجا تأکید بر روی روش دو-دویی نیست. ایده‌ی مهمی که وجود دارد تجزیه‌ی حجمی از داده‌ها به اجزای کوچکتر است به طوری که نمایش تک تک این اجزا ساده‌تر باشد. بر این اساس هر داده یک دنباله‌ی $a_1, a_2, \dots, a_n$ است که هر از پارامترهای a_i یکی از چند مقدار مشخص را می‌گیرد. در سیستم دو-دویی $a_i \in \{0,1\}$ و a_i یک بیت[۱۷] نامیده می‌شود.

---

[۱۳] Lie bracket
[۱۴] Commutator
[۱۵] Binary
[۱۶] Unicode
[۱۷] Bit

حال این سؤال پیش می‌آید که چطور این اطلاعات به ابزار محاسبگر داده شود. صفحه نمایش ماشین حساب را در نظر بگیرید. اگر خود را به سیستم دو-دویی محدود کنیم، این صفحه قابلیت نمایش اعداد با حداکثر، به طور مثال، ده رقم را دارد. جایگاه هر یک از این ارقام با یک لامپ مشخص می‌شود که روشن یا خاموش بودن لامپ مربوط به a_i تعیین کننده‌ی این است که $a_i = 1$ یا $a_i = 0$. مثال کلی‌تر نمایش اطلاعات به وسیله یک مدار الکتریکی است که n جزء آن علامت‌گذاری شده است. اگر مقدار جریان عبوری از جزء i-ام بیشتر از حدی از پیش تعیین شده باشد، این را به عنوان $a_i = 1$ می‌گیریم و در غیر این صورت $a_i = 0$. مثال پیچیده‌تر اسپین[۱۸] n الکترون است. اگر اسپین i-ام (در راستایی از پیش تعیین شده) به سمت بالا باشد آن را به عنوان $a_i = 1$ می‌گیریم و در صورت پایین بودن $a_i = 0$.

۲.۲ الگوریتم

به مسأله محاسبه مجموع دو عدد بر می‌گردیم. برای انجام عمل جمع آن را به دنباله‌ای از دو عمل آسان‌تر تقسیم می‌کنیم: (۱) جمع ارقام، (۲) «ده بر یک». برای مثال عمل جمع در مبنای دو، دنباله‌ای است از اعمال دو تابع

$$\mathrm{AND}, \mathrm{XOR} : \{0,1\} \times \{0,1\} \to \{0,1\}$$

که $\mathrm{XOR}(x,y) = x + y \pmod 2$ و $\mathrm{AND}(x,y) = xy$. کیلومترشمار اتومبیل مثالی است از وسیله‌ای ساده که قابلیت انجام این دو عمل را دارد.

به طور کلی هر وسیله محاسبه (کامپیوتر) وسیله‌ای است که علاوه بر نمایش اطلاعات، قابلیت اعمال دنباله‌ای از «توابع ساده» بر روی آنها را دارد. $\mathrm{AND}, \mathrm{XOR}$ دو مثال از این توابع ساده هستند. مثال‌های دیگر شامل $\mathrm{OR}, \mathrm{NOT}$ است: $\mathrm{OR}(x,y) = xy + x + y \pmod 2$ و $\mathrm{NOT}(x) = x + 1 \pmod 2$.

توابع $\mathrm{XOR}, \mathrm{AND}, \mathrm{OR}, \mathrm{NOT}$ در اصطلاح گیت[۱۹] نامیده می‌شوند. $\mathrm{AND}, \mathrm{XOR}, \mathrm{OR}$ گیت‌های دو-بیتی[۲۰] و NOT یک گیت یک-بیتی هستند.

قضیه زیر با استقراء روی n قابل اثبات است.

قضیه ۱ هر تابع $F : \{0,1\}^n \to \{0,1\}^m$ را می‌توان برحسب گیت‌های AND, OR, NOT نوشت.

به مجموعه $\{\mathrm{AND}, \mathrm{OR}, \mathrm{NOT}\}$ با خاصیت قضیه فوق یک مجموعه عام از گیت‌ها[۲۱] گفته می‌شود. با فرض کردن قضیه فوق می‌توان نشان داد $\{\mathrm{AND}, \mathrm{NOT}\}$ نیز یک مجموعه عام از گیت‌ها ست (کافی است OR را با استفاده از قوانین دمورگان[۲۲] برحسب AND و NOT بنویسیم). همچنین $\mathrm{NAND} := \mathrm{NOT} \circ \mathrm{AND}$ نیز یک مجموعه عام است، ولی $\{\mathrm{NOT}, \mathrm{XOR}\}$ عام نیست.

هر وسیله‌ای که قابلیت اعمال یک مجموعه عام از گیت‌ها را داشته باشد، قابلیت انجام «هر محاسبه‌ای» را دارد. زیرا یک محاسبه چیزی نیست جز اعمال یک تابع بر روی داده‌های آن. از این زاویه یک «الگوریتم» روشی است برای تقسیم یک مسأله به اجزای کوچک‌تر، یا به عبارت دیگر نوشتن یک تابع بر حسب گیت‌ها.

[۱۸] Spin
[۱۹] Gate
[۲۰] Two-bit gate
[۲۱] Universal set of gates
[۲۲] De Morgan’s laws

۳.۲ تصحیح خطا به وسیله کدگذاری

کامپیوتری را در نظر بگیرید که در آن کم یا زیاد بودن جریان در قسمت‌های مختلف یک مدار نشان‌دهنده اطلاعات ورودی مسأله باشد، و قابلیت اعمال گیت‌های یک مجموعه عام را نیز داشته باشد. بدون شک دمای محیط بر خواص فیزیکی مدارهای این کامپیوتر تأثیر می‌گذارد. همچنین کم یا زیاد شدن ولتاژ تأمین کننده انرژی کامپیوتر بر کارایی آن مؤثر است. در نتیجه مثلاً اگر یکی از بیت‌های داده مسأله $a_i = 1$ باشد، با توجه به این تأثیرات محیطی ممکن است به $a_i = 0$ تبدیل شده و در درستی محاسبه اخلال وارد کند. ابزاری که برای جلوگیری از این گونه خطاها استفاده می‌شود کدگذاری[۲۳] اطلاعات است.

مثال زیر ایده‌ی کدگذاری اطلاعات را به خوبی توضیح می‌دهد. فرض کنید اطلاعات ورودی شامل سه بیت $a_1a_2a_3 = 010$ باشد. فرض کنید که تأثیرات محیطی باعث شوند که در طول محاسبات هر یک از این بیت‌ها با احتمال p با خطا مواجه شود، یعنی با احتمال p، a_i به $\mathrm{NOT}(a_i)$ تبدیل شود. همچنین فرض کنید که این خطاها از هم مستقل هستند، در نتیجه 010 با احتمال p^2 به 100 تبدیل می‌شود.

برای جلوگیری از خطا هر بیت a را با aaa نمایش می‌دیم. مثلاً بجای استفاده از یک اسپین برای نمایش هر بیت، از سه اسپین استفاده می‌کنیم و جهت هر سه اسپین را برابر می‌گیریم. در این صورت سه بیت 010 در کامپیوتر با 000111000 نشان داده می‌شوند.

حال فرض کنید که در حین محاسبه خطا ایجاد شده و دنباله ذخیره شده در کامپیوتر 010111000 باشد. با توجه به نحوه کدگذاری اطلاعات متوجه می‌شویم که سه بیت اول باید یکسان باشند و لذا خطا رخ داده: یا همگی باید 1 باشند و یا 0. اگر قبل از خطا همگی 1 بوده باشند، یعنی روی بیت اول و سوم خطا ایجاد شده و این با احتمال p^2 اتفاق می‌افتد. در حالت دیگر خطا فقط روی بیت دوم است و احتمال آن p است. در نتیجه ما فرض می‌کنیم خطای اتفاق افتاده، پیشآمد با احتمال بیشتر یعنی p است. لذا اطلاعات ذخیره شده را به صورت 000111000 تصحیح[۲۴] می‌کنیم. توجه کنید قبل از کدگذاری احتمال بروز خطا روی هر بیت از اطلاعات p بود، ولی با استفاده از کدگذاری $a \mapsto aaa$ احتمال خطا به $p' = 3p^2(1-p) + p^3$ کاهش پیدا کرد. برای کم‌تر کردن احتمال خطا کافی است اطلاعات کد شده را دوباره و دوباره کد کنیم.[۲۵]

CD مثالی از کاربرد کدگذاری است که بعضاً اطلاعات ذخیره شده، حتی با وجود خش بر روی آن قابل بازیابی است.

۴.۲ نظریه‌ی محاسبات کوانتمی

مفاهیمی که تا کنون توضیح داده شد مانند نمایش اطلاعات به وسیله‌ی بیت‌ها، گیت‌ها، الگوریتم و کدگذاری، هیچ کدام مختص فیزیک کلاسیک نیستند. در حضور نظریه‌ی فیزیک کوانتم، مسأله نمایش و ذخیره‌ی اطلاعات کوانتمی مطرح می‌شود. برای نمایش اطلاعات کوانتمی، همانند دنیای کلاسیک، آنها را به اجزای کوچک‌تر تقسیم می‌کنیم. از آنجا که فضای فاز هر سیستم کوانتمی یک فضای برداری است، هر کدام از این اجزای کوچک چیزی جز یک فضای برداری با بعد

[۲۳] Coding
[۲۴] Decode
[۲۵] Concatenation of codes

پایین نیست. به عنوان مثال یک فضای برداری با بعد دو معادل کوانتمی یک بیت است و کیوبیت[۲۶] خوانده می‌شود.

در دنیای کلاسیک گیت‌ها توابع (تحول‌های زمانی) ساده‌ای هستند که بر روی سیستم‌های فیزیکی قابل تصورند. در دنیای کوانتمی تحولات زمانی یک سیستم به وسیله معادله شرودینگر، و یا به طو معادل (در صورتی که همیلتونی مستقل از زمان باشد) با رابطه (۵) داده می‌شوند. توجه کنید که عملگر خطی $e^{\frac{-it}{\hbar}H}$، از آنجا که H هرمیتی است، یک عملگر یکانی[۲۷] است. پس در سیستم‌های کوانتمی تحول زمانی به وسیله‌ی عملگرهای خطی یکانی داده می‌شوند. لذا گیت‌های کوانتمی عملگرهای یکانی‌ای هستند که روی فضاهای برداری با بعد پایین تعریف شده‌اند. برای بدست آوردن قضیه‌ای همانند قضیه ۱، باید مجموعه‌ای از گیت‌های کوانتمی یافت که هر عملگر یکانی دیگر را بتوان بر حسب آنها نوشت. از این نقطه نظر یک الگوریتم کوانتمی چیزی جز نوشتن یک عملگر یکانی برحسب گیت‌های کوانتمی یک مجموعه عام نیست.

همان طور که کدگذاری در دنیای کلاسیک باعث جلوگیری از تأثیر محیط بر ذخیره و پردازش اطلاعات می‌شود، در دنیای کوانتمی نیز نیاز به کدهای کوانتمی داریم.

از دیگر مباحثی که در نظریه محاسبات کوانتمی به آنها پرداخته می‌شود می‌توان به پیچیدگی محاسبات[۲۸]، مخابرات[۲۹] و نظریه‌ی اطلاعات[۳۰]، رمزنگاری[۳۱] و نظریه کنترل[۳۲] نام برد. برای مثال نظریه‌ی پیچیدگی محاسبات سعی در دسته‌بندی مسائل محاسباتی بر حسب سختی و آسانی آنها روی یک کامپیوتر کلاسیک دارد. پیچیدگی محاسبات کوانتمی [۳۳] سعی در دسته‌بندی مسائل در حضور یک کامپیوتر کوانتمی دارد. به طور مشابه نظریه‌های رمزنگاری کوانتمی، اطلاعات کوانتمی، و غیره قابل تعریف هستند.

---
[۲۶] Qubit
[۲۷] Unitary
[۲۸] Computational complexity theory
[۲۹] Communication
[۳۰] Information theory
[۳۱] Cryptography
[۳۲] Control thoery
[۳۳] Quantum complexity thoery