محاسبات کوانتمی (۲۲۶۷۱) ترم بهار ۱۳۹۱-۱۳۹۰

مدرس: سلمان ابوالفتح بیگی نویسنده: آمنه فرهادیان

جلسه ۸

---

۱ اجزای مدارهای کوانتومی

۱. ورودی‌ها

اگر $x_i \in \{0,1\}$ و $x = x_1x_2\cdots x_n$ نمایش کلاسیک ورودی باشد، آنگاه ورودی مدار کوانتومی به صورت $|x\rangle = |x_1\rangle \otimes \cdots \otimes |x_1\rangle$ یعنی یکی از اعضای پایه‌ی استاندارد متناظر با n کیوبیت، داده می شود.

۲. کیوبیت های کمکی [۱]

کیوبیت هایی هستند که در ابتدا ثابت ($|0\rangle$) هستند و در طول الگوریتم تغییر می کنند.

۳. گیت‌های کوانتومی

عملگرهای یکانی که روی تعداد کمی کیوبیت اثر می‌کنند. از جمله عملگرهای یکانی می‌توان به گیت‌های زیر اشاره کرد.

Hadamard	$-\boxed{H}-$	$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$	Pauli-Z	$-\boxed{Z}-$	$\begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}$
Pauli-X	$-\boxed{X}-$	$\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$	Phase	$-\boxed{S}-$	$\begin{bmatrix}1 & 0\\0 & i\end{bmatrix}$
Pauli-Y	$-\boxed{Y}-$	$\begin{bmatrix}0 & -i\\i & 0\end{bmatrix}$	$\pi/8$	$-\boxed{T}-$	$\begin{bmatrix}1 & 0\\0 & e^{i\pi/4}\end{bmatrix}$

۴. اندازه‌گیری

در مدارهای کوانتمی فقط اندازه‌گیری ساده، یعنی اندازه‌گیری یک کیوبیت در پایه استاندارد $\{|0\rangle, |1\rangle\}$ را در نظر می‌گیریم.

سؤال: آیا یک اندازه‌گیری پیچیده بر حسب این اندازه‌گیری ساده قابل بیان است؟ پاسخ این سؤال در حالت کلی مثبت است. در اینجا مثالی خاص را بررسی می‌کنیم.

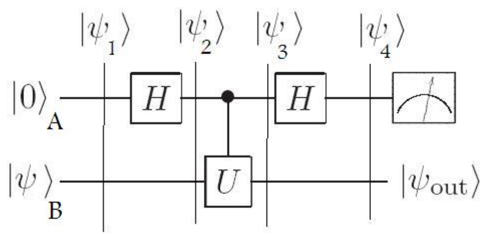
---

[۱] Ancilla

فرض کنید $\{P, Q\}$ یک اندازه‌گیری تصویری است که می خواهیم آن را روی سیستم B که در حالت $|\psi_B\rangle$ قرار دارد، اعمال کنیم. بنابر شرط کامل بودن، داریم $P + Q = I_B$. با ضرب طرفین در P داریم $P^2 + PQ = P$. چون $P^2 = P$ پس $PQ = 0$. به همین ترتیب داریم $QP = 0$. حال تعریف کنیم $U = P - Q$. با توجه به تعریف U داریم

$$\begin{cases} U^2 = (P-Q)^2 = P^2 + Q^2 - PQ - QP = P + Q = I \\ U^\dagger = P^\dagger - Q^\dagger = P - Q = U \end{cases} \tag{۱}$$

بنابراین U عملگری یکانی است. حال مدار شکل ۱ را در نظر بگیرید.



شکل ۱: مدار اندازه‌گیری تصویری $\{P, Q\}$

$$\begin{aligned} |\psi_1\rangle &= |0\rangle|\psi\rangle \\ |\psi_2\rangle &= (H \otimes I)|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|\psi\rangle \\ |\psi_3\rangle &= \frac{1}{\sqrt{2}}(|0\rangle \otimes |\psi\rangle + |1\rangle \otimes U|\psi\rangle) \end{aligned}$$

و

$$\begin{aligned} |\psi_4\rangle &= \frac{1}{\sqrt{2}}(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|\psi\rangle + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)U|\psi\rangle) \\ &= |0\rangle \otimes (\frac{I+U}{2})|\psi\rangle + |1\rangle \otimes (\frac{I-U}{2})|\psi\rangle \\ &= |0\rangle P|\psi\rangle + |1\rangle Q|\psi\rangle \end{aligned}$$

بنابراین اگر نتیجه اندازه‌گیری صفر باشد، سیستم به حالت $P|\psi\rangle$ و اگر یک باشد به $Q|\psi\rangle$ تغییر حالت می دهد. حال با محاسبه احتمال صفر در خروجی داریم.

$$\begin{aligned} P(0) &= \mathrm{tr}((|0\rangle\langle 0|_A \otimes I_B)|\psi_4\rangle\langle\psi_4|) \\ &= \mathrm{tr}(|0\rangle\langle 0|_A(tr_B(|\psi_4\rangle\langle\psi_4|))) \\ &= \mathrm{tr}(|0\rangle\langle 0|_A(\langle\psi|P|\psi\rangle|0\rangle\langle 0|_A + \langle\psi|Q|\psi\rangle|1\rangle\langle 1|_A)) \\ &= \langle\psi|P|\psi\rangle \end{aligned}$$

به همین ترتیب داریم

$$P(1) = \langle\psi|Q|\psi\rangle$$

بنابراین اندازه‌گیری تصویری $\{P, Q\}$ با استفاده از اندازه‌گیری در پایه‌ی استاندارد قابل پیاده سازی است.

۲ اصل به تاخیر انداختن اندازه‌گیری

در الگوریتم‌های کلاسیک از جمله‌های شرطی استفاده می شود. پیاده‌سازی جمله شرطی نیازمند بررسی برقراری شرط است. بنابراین در الگوریتم‌های کوانتومی ممکن است نیاز به اندازه‌گیری در وسط مدار داشته باشیم. یعنی در وسط مدار با توجه به حاصل یک اندازه‌گیری، کاری را انجام دهیم. مثلاً اگر حاصل اندازه‌گیری 0 بود گیت X را اعمال کند و اگر 1 بود گیت Z را اعمال کند.

طبق اصل به تأخیر انداختن اندازه‌گیری[۲] در مدارهای کوانتومی همواره می توان اندازه‌گیری را به انتهای مدار انتقال داد به گونه‌ای که حاصل مدار تغییری نکند. یعنی در یک مدار کوانتمی می‌توان فرض کرد که اندازه‌گیری‌ها فقط در انتهای مدار انجام می‌شوند. مثال زیر ایده‌ی دلیل برقراری این اصل را نشان می‌دهد.

مثال: فرض کنیم در یک مدار اندازه‌گیریی روی کیوبیت A انجام می‌دهیم. اگر حاصل اندازه‌گیری 0 بود، کاری انجام نمی‌دهیم، ولی اگر 1 بود روی سیستم B گیت یکانی U را اعمال می‌کنیم. مدار معادل این عمل در سمت چپ شکل ۲ نشان داده شده است.

شکل ۲: نمونه‌ای از انتقال اندازه‌گیری به انتهای مدار

ابتدا عملکرد مدار سمت چپ را بررسی می‌کنیم و سپس نشان می دهیم که معادل با مدار سمت راست است. اگر ورودی مدار $|0\rangle_A|\psi_0\rangle_B + |1\rangle_A|\psi_1\rangle_B$ باشد، توزیع احتمال حاصل اندازه‌گیری در مدار سمت چپ به صورت زیر است.

$$P(0) = \langle\psi_0|\psi_0\rangle,$$

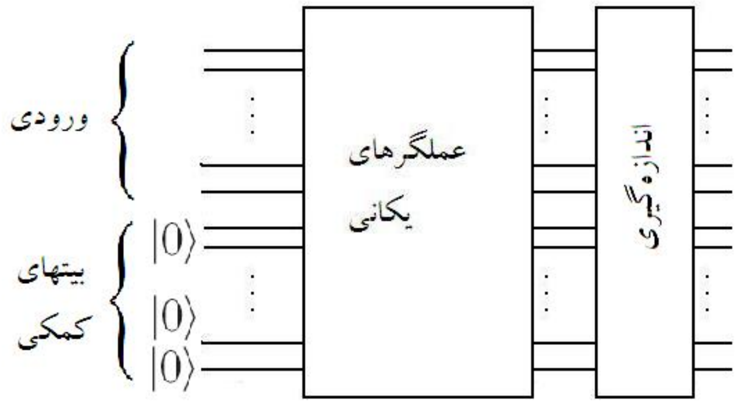
$$P(1) = \langle\psi_1|\psi_1\rangle.$$

همچنین خروجی مدار اگر حاصل اندازه‌گیری 0 باشد $|\psi_0\rangle$ و اگر 1 باشد، $U|\psi_1\rangle$ است. در مدار سمت راست، خروجی گیت $Controlled-U$ به ازای همان ورودی بالا، $|0\rangle|\psi_0\rangle + |1\rangle U|\psi_1\rangle$ است که اگر حاصل اندازه گیری 0 باشد به

[۲] Principle of deferred measurement

$|\psi_0\rangle$ و اگر حاصل اندازه گیری 1 باشد به $U|\psi_1\rangle$ تغییر حالت پیدا می کند. به وضوح توزیع احتمال حاصل اندازه‌گیری نیز همانند مدار قبل است. بنابراین مدار دوم که اندازه‌گیری آن به انتهای مدار انتقال پیدا کرده است، معادل مدار سمت چپ است.

از آنجا که در مدارهای کوانتومی می‌توان فرض کرد که همه اندازه‌گیری‌ها در انتهای مدار انجام می‌گیرد، شکل کلی یک مدار کوانتومی به شکل ۳ است. بنابراین تنها قسمت متغیر در مدار قسمت عملگر یکانی است.



شکل ۳: شکل عمومی یک مدار کوانتومی

سؤال: کدام عملگرهای یکانی را می‌توان بر حسب گیت‌های ساده‌ی کوانتومی نوشت؟ در حالت کلاسیک دیدیم که هر تابع $f:\{0,1\}^n \longrightarrow \{0,1\}^m$ توسط گیت های AND و NOT قابل پیاده سازی است. به این معنا یک مجموعه‌ی (متناهی) کامل از گیت‌های کلاسیک وجود دارد. حال سؤال این است که آیا مجموعه‌ی کاملی از گیت‌های کوانتومی وجود دارد یا خیر؟

قضیه ۱ هر عملگر یکانی را می توان به صورت حاصلضرب عملگرهای یکانی دو کیوبیتی نوشت.

قضیه ۲ هر عملگر یکانی دو کیوبیتی را می توان بر حسب $C-NOT$ و عملگرهای یکانی یک کیوبیتی نوشت.

از آنجا که الگوریتم‌های کوانتومی معمولاً احتمالی هستند، وجود کمی خطا در آنها قابل اغماض است. از این جهت لزومی ندارد که در یک الگوریتم کوانتمی بتوانیم یک عملگر یکانی U را «دقیقاً» اعمال کنیم. یعنی اگر بتوان U را «تقریباً» به صورت حاصل‌ضرب گیت‌های ساده نوشت، مدار متناظر به طور تقریبی همانند مدار ایده‌آل کار می‌کند.

توجه کنید که در مقایسه با حالت کلاسیک، تقریب زدن عملگرهای کلاسیک غیر قابل اجتناب است. در حالت کلاسیک تعداد توابع $f:\{0,1\}^n \longrightarrow \{0,1\}^m$ متناهی و این توابع یک مجموعه‌ی گسسته تشکیل می‌دهند. ولی عملگرهای یکانی n-کیوبیتی یک مجموعه‌ی پیوسته تشکیل می‌دهند که سایز آن نامتناهی است.

قضیه ۳ $\{H,S,T,C-NOT\}$ یک مجموعه کامل (تقریبی) از گیت های کوانتومی است.

یعنی هر عملگر یکانی دلخواه را می‌توان با هر تقریب دلخواه با گیت های بالا ساخت. به عبارت دقیق تر برای هر U و $\varepsilon>0$ وجود دارد $V_1,V_2,\cdots,V_k$ به طوری که $V_i\in\{H,S,T,C-NOT\}$ و $\parallel U-V_1\cdots V_k\parallel<\varepsilon$.

برای اثبات قضیه‌ی فوق با استفاده از قضیه ۲، کافی است نشان دهیم هر گیت یک کوبیتی را می‌توان با $\{H, S, T\}$ تقریب زد.

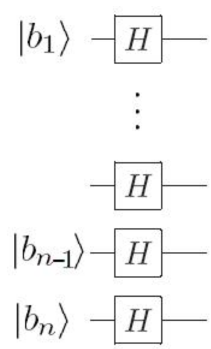
توجه کنید که اگر T را از مجموعه‌ی کامل $\{H, S, T, C-NOT\}$ حذف کنیم، هر مدار کوانتمی بر حسب سه گیت باقی مانده را می‌توان به طور «بهینه» به صورت کلاسیک شبیه‌سازی کرد.

۳ تبدیل فوریه روی گروه $\mathbb{Z}_2^n$

عملکرد گیت یک کیوبیتی هادامارد روی ورودی‌های $|0\rangle$ و $|1\rangle$ به صورت زیر است.

$$
\begin{aligned}
|0\rangle &\longrightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
|1\rangle &\longrightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)
\end{aligned}
$$

پس اگر ورودی $|b_i\rangle$ به صورت صفر یا یک باشد، خروجی عملگر هادامارد به صورت $\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{b_i}|1\rangle)$ است. حال با در نظر گرفتن ورودی $|x\rangle = |b_1\rangle, \cdots, |b_n\rangle$ به مدار شکل ۴، خروجی به صورت زیر خواهد شد.



شکل ۴: تبدیل فوریه روی گروه Z_2^n

$$
\begin{aligned}
H^{\otimes n}|x\rangle &= H|b_1\rangle \otimes \cdots \otimes H|b_n\rangle \\
&= (\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{b_1}|1\rangle) \otimes \cdots \otimes \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{b_n}|1\rangle)) \\
&= \frac{1}{\sqrt{2^n}} \sum_{a_1,\cdots,a_n \in \{0,1\}^n} (-1)^{a_1 b_1 + \cdots + a_n b_n} |a_1 \cdots a_n\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x.y} |y\rangle
\end{aligned}
$$

که در آن اگر $y = a_1 \ldots a_n$ آنگاه $x.y := a_1 b_1 + \cdots + a_n b_n$

۱.۳ الگوریتم Deutsch–Jozsa

الگوریتم Deutsch–Jozsa که در سال ۱۹۸۲ مطرح شد به حل مسأله زیر می پردازد.

ورودی: تابع $F : \{0,1\}^n \to \{0,1\}$
شرط: یا F به ازای تمام ورودی‌ها صفر می دهد و یا F دقیقاً به ازای نصف ورودی‌ها صفر و به ازای نصف دیگر یک است.
خروجی: F کدام یک از دو حالت گفته شده است؟

یک الگوریتم احتمالاتی کلاسیک برای حل این مسأله این است که به ازای یک ورودی دلخواه خروجی تابع را چک کنیم . اگر یک بود حتماً تابع در حالت دوم است و اگر صفر بود، یا در حالت اول و یا در حالت دوم است که انتخاب تصادفی یکی از این دو حالت منجر به یک الگوریتم احتمالاتی می شود. حال اگر به دنبال یک الگوریتم کلاسیک باشیم که بتواند به صورت قطعی پاسخ درست دهد، باید حداقل $2^{n-1}+1$ تا از ورودی ها را چک کنیم. در اینجا نشان می‌دهیم که الگوریتمی کوانتومی وجود دارد که با فقط یک بار استفاده از تابع می‌تواند به پاسخ قطعی حالت تابع برسد.

قبل از پرداختن به الگوریتم کوانتومی توجه کنید که ابتدا باید «سؤال پرسیدن» از تابع F را به صورت کوانتمی مدل‌سازی کنیم. به طور کلاسیک ما به سادگی فرض می‌کنیم که با ورودی x می‌توان خروجی $F(x)$ را بدست آورد. به طور کوانتمی ممکن این عمل را به صورت $|x\rangle \to |F(x)\rangle$ مدل کنیم، ولی توجه کنید که «سؤال پرسیدن» در دنیای کوانتمی باید یکانی باشد. حال آنکه $|x\rangle \to |F(x)\rangle$ یکانی نیست چون بعد فضای ورودی و خروجی یکسان نیست. حتی اگر عملگر $|x\rangle \to |F(x)\rangle|\underbrace{00\cdots0}_{n-1}\rangle$ را در نظر بگیرم باز هم یکانی نیست چون ضرب داخلی را حفظ نمی‌کند. به ازای x, x' مختلف داریم $\langle x|x'\rangle = 0$، در حالی که ممکن است $F(x) = F(x')$.

سؤال پرسیدن کوانتمی از یک تابع معمولاً به یکی از دو صورت زیر مدل می‌شود.

$$T_F|x\rangle = (-1)^{F(x)}|x\rangle$$

و یا

$$O_F|x\rangle|y\rangle = |x\rangle|F(x) \oplus y\rangle.$$

در T_F، $F(x)$ در یک فاز قرار می‌شود. در O_F، $|y\rangle$ حالت یک کیوبیت است و منظور از $\oplus$ جمع در مبنای دو است. توجه کنید که هر دوی T_F, O_F یکانی هستند. برای $|\psi\rangle = \sum_x \alpha_x|x\rangle$ داریم

$$T_F|\psi\rangle = \sum_x \alpha_x(-1)^{F(x)}|x\rangle$$

و

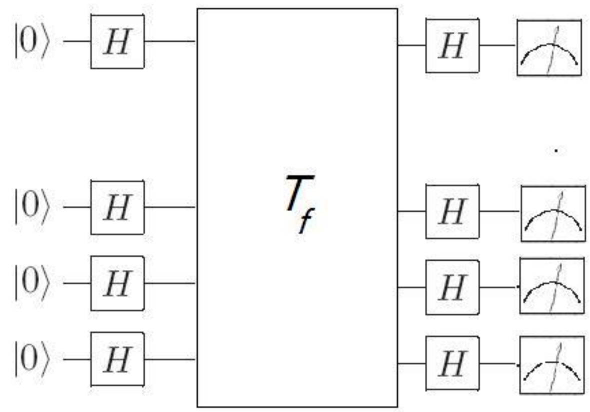
$$O_F|\psi\rangle|0\rangle = \sum_x \alpha_x|x\rangle|F(x)\rangle.$$

توجه کنید که این دو مدل مختلف سؤال پرسیدن کوانتمی با هم معادل هستند زیرا طبق تعریف

$$\begin{aligned} O_F|x\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) &= (-1)^{F(x)}|x\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) \\ &= \left(T_F \otimes I\right)|x\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right). \end{aligned}$$

پس گاهی از T_F استفاده می‌کنیم و گاهی از O_F.

حال مدار کوانتومی شکل ۵ را در نظر بگیرید. اگر ورودی مدار $|\underbrace{0\cdots0}_{n}\rangle$ باشد، خروجی آن به صورت زیر است.



شکل ۵: الگوریتمی برای تشخیص حالت تابع F

$$
\begin{aligned}
|\underbrace{0\cdots0}_{n}\rangle &\xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \\
&\xrightarrow{T_F} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{F(x)}|x\rangle \\
&\xrightarrow{H^{\otimes n}} \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{F(x)} \sum_{y\in\{0,1\}^n} (-1)^{x.y}|y\rangle \\
&= \frac{1}{2^n} \sum_{y\in\{0,1\}^n} \left(\sum_{x\in\{0,1\}^n} (-1)^{F(x)+x.y} \right) |y\rangle
\end{aligned}
$$

اگر در حالت اول باشیم، یعنی تابع F متحد با صفر باشد، T_F عملگر همانی است، و از آنجا که $H^2 = I$ مدار معادل شکل، مدار همانی است. پس خروجی همان ورودی یعنی $|\underbrace{0\cdots0}_{n}\rangle$ است و در هنگام اندازه‌گیری همواره 0 می‌گیریم.

فرض کنید که در حالت دوم باشیم. در این صورت ضریب $|y\rangle = |\underbrace{0\cdots0}_{n}\rangle$ برابر است با $\sum_x (-1)^{F(x)}$. از آنجا که نصف $F(x)$ ها صفر و نصف دیگر یک است، پس نصف $(-1)^{F(x)}$ ها 1 و نصف دیگر -1 است. در نتیجه ضریب $|\underbrace{0\cdots0}_{n}\rangle$ در خروجی مدار بالا صفر است. به عبارت دیگر خروجی مدار بر $|\underbrace{0\cdots0}_{n}\rangle$ عمود است و حاصل حداقل یکی از n اندازه‌گیری 1 است.

به طور خلاصه اگر حاصل همه‌ی اندازه‌گیری‌ها 0 شد در حالت اول هستیم و اگر حداقل یکی از آنها 1 شد در حالت دوم هستیم.