	پردازش اطلاعات کوانتومی پاییز ۱۴۰۲	
ارائه ۷-۱		دکتر احمد خونساری

۱ مقدمه

در این ارائه با الگوریتم Deutsch آشنا می‌شویم. این الگوریتم کوانتومی اجازه می‌دهد که تابع تک ورودی ثابت [۱] را از توابع تک ورودی متوازن [۲] با یک بار فراخوانی تشخیص دهیم. در اسلایدهای ۲ تا ۴ یادآوری می‌شود که برای طراحی الگوریتم‌های کوانتومی (مدارهای کوانتومی) باید قید یکانی [۳] بودن آن‌ها رعایت شود. با این چالش پیش‌تر در هنگام آشنایی با مدار Toffoli آشنا شدیم. ملاحظه کردیم که لازم است تعداد ورودی‌ها و خروجی‌های مدارهایی که طراحی می‌کنیم برابر باشد و برای دستیابی به این هدف و حفظ معکوس پذیری محاسبات می‌توان به شکل زیر رفتار کرد:

۱. فرض کنید می‌خواهیم برای یک تابع $f(x)$ که تعداد ورودی‌های آن n بیت و تعداد خروجی‌های آن m بیت است مداری طراحی کنیم.

۲. برای مدار یکانی مدنظر به تعداد $n+m$ سیم (کیوبیت) ورودی و $n+m$ کیوبیت خروجی در نظر می‌گیریم (تعداد ورودی و خروجی مدار کوانتومی برابر است).

۳. در سمت ورودی، به n کیوبیت اول که ورودی را در خود ذخیره می‌کنند $|x\rangle$ می‌گوییم. به m کیوبیت بعدی $|y\rangle$ می‌گوییم (کیوبیت‌های کمکی) که می‌توانند مقدار دلخواه و مشخصی داشته باشند.

۴. در سمت خروجی، بر روی n کیوبیت اول همان ورودی $|x\rangle$ را بازتولید می‌کنیم. بر روی m کیوبیت بعدی مقدار $|y \oplus f(x)\rangle$ را تولید می‌کنیم که $f(x)$ حاصل اعمال تابع بر روی ورودی است و $\oplus$ عملگر XOR است.

می‌توان ملاحظه کرد که این مدار معکوس‌پذیر است (شکل اسلاید شماره ۴ را ببینید) و به این ترتیب می‌توان آن را با استفاده از gateهای کوانتومی یک و دو ورودی بازسازی کرد.

[1] Constant
[2] Balanced
[3] Unitary

برای ملاحظه معکوس‌پذیری، به تساوی زیر دقت کنید:

$$|y \oplus f(x) \oplus f(x)\rangle = |y\rangle \tag{1}$$

۲ الگوریتم Deutsch

در اسلاید شماره ۵ با مفهوم توابع تک ورودی ثابت و متوازن آشنا می‌شوید و جدول صحّت و مدارهای کوانتومی معادل آن‌ها را ملاحظه می‌کنید. به صورت خاص، تابع ثابت به ازای هر ورودی (صفر یا یک) همیشه یک خروجی ثابت را تولید می‌کند (به دو ردیف اول جدول نگاه کنید). اما توابع متوازن در نیمی از اوقات صفر و در نیمه دیگر اوقات یک را به عنوان خروجی تولید می‌کنند. ردیف‌های سه و چهار جدول را بررسی کنید. مدارهای کوانتومی ارائه شده را بررسی کنید و سعی کنید متوجه شوید که چگونه هر کدام از آن‌ها تابع متناظر را پیاده‌سازی می‌کنند.

در ادامه ما فرض می‌کنیم که یکی از این چهار مدار را به ما داده‌اند. اما ما از پیاده‌سازی داخلی آن اطلاعی نداریم. همچنین، از ما خواسته‌اند فقط با یک فراخوانی مدار (ارسال یک ورودی و مشاهده یک خروجی) تشخیص دهیم که مدار از نوع ثابت است و یا از نوع متوازن. توجه کنید که اگر این مدارها «کلاسیک» بودند (یعنی ورودی و خروجی از نوع بیت داشتند و نه کیوبیت) ما باید مدار را «دو» بار فراخوانی می‌کردیم تا بتوانیم نوع آن را تشخیص دهیم (این موضوع را بررسی کنید!). اما در ادامه ملاحظه می‌کنیم که به دلیل کوانتومی بودن مدار با استفاده از الگوریتم Deutsch می‌توان پس از یک بار فراخوانی نوع تابع را مشخص کرد. اسلاید شماره ۶ را ببینید.

در اسلاید شماره ۷ نحوه کار الگوریتم Deutsch را ملاحظه می‌کنید. به عنوان ورودی مقدار $|01\rangle$ آماده می‌شود:

$$|x\rangle = |0\rangle \tag{2}$$

$$|y\rangle = |1\rangle. \tag{3}$$

سپس، هر دو ورودی از مدار هادامارد گذرانده می‌شوند و به این ترتیب در حالت superposition قرار می‌گیرند. در نتیجه، مقدار کیوبیت‌ها به شکل زیر تغییر می‌کند:

$$|x\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \tag{4}$$

$$|y\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{5}$$

محاسبات انتهای اسلاید ۷ را ملاحظه کنید. سپس این مقادیر به مدار ناشناخته داده می‌شود. بر اساس اینکه این مدار واقعاً کدام تابع را پیاده‌سازی می‌کند، خروجی ۴ حالت متفاوت را می‌تواند داشته باشد که در میانه اسلاید ۸ نمایش داده شده‌اند. توجه کنید که کیوبیت اول تغییر نمی‌کند، و کیوبیت دوم حاصل XOR کیوبیت دوم و خروجی تابع است. نتیجه به رنگ آبی متمایز شده است. با مقداری محاسبات جبری و فاکتورگیری، می‌توان چهار حالت را به صورت

دو حالت انتهایی اسلاید ۸ خلاصه‌سازی کرد. به صورت خاص، اگر تابع ثابت باشد (یعنی $f(0) = f(1)$) خروجی مدار ناشناخته به شکل زیر خواهد بود:

$$\pm \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \tag{۶}$$

و اگر مدار ناشناخته از نوع متوازن بوده باشد، خروجی آن به شکل زیر خواهد بود:

$$\pm \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right).$$

این خروجی نشان می‌دهد که توابع ثابت فقط در یک فاز سراسری (یعنی $\pm$) با یکدیگر تفاوت دارند و همچنین توابع متوازن نیز فقط در فاز سراسری متفاوت هستند. بنابراین کافی است که کیوبیت اول را در پایه هادامارد اندازه‌گیری کرد (اعمال gate هادامارد و اندازه‌گیری در پایه‌های محاسباتی). اگر حاصل اندازه‌گیری صفر باشد، مدار ناشناخته از نوع ثابت بوده است و اگر حاصل اندازه‌گیری یک باشد مدار ناشناخته از نوع متوازن بوده است. اسلاید ۹ را ببینید.

در اسلاید ۱۰ با دو مفهوم جدید که در تئوری‌های پیچیدگی کوانتومی مورد استفاده قرار می‌گیرند آشنا می‌شوید.

۱. پیچیدگی پرس‌وجو [۴] نوعی از پیچیدگی است که تعداد فراخوانی‌های یک تابع را اندازه‌گیری می‌کند. ملاحظه کردیم که با استفاده از محاسبات کوانتومی پیچیدگی پرس‌وجوی تشخیص توابع ثابت از متوازن به نسبت روش‌های کلاسیک تفاوت بنیادینی را نشان داد. به این ترتیب که می‌توان توابع (تک ورودی) ثابت و متوازن را با یک فراخوانی از یکدیگر تشخیص داد، در حالی که این دستاورد در حوزه کلاسیک غیرممکن است.

۲. همچنین با مفهوم «سروش [۵]» و «جعبه سیاه [۶]» آشنا شدیم. در این ارائه، مداری که تابع ثابت و یا متوازن را پیاده‌سازی کرده بود یک «جعبه سیاه» بود. به این معنی که این مدار یک کار مشخصی را انجام می‌داد (یک محاسبات از پیش تعیین‌شده) اما ما از آن اطلاعی نداشتیم. در این ارائه هدف ما «شناخت» این جعبه سیاه با حداقل تعداد فراخوانی بود. استفاده از مفهوم سروش در حوزه محاسبات کوانتومی کاربردهای متعددی دارد که در آینده با آن‌ها بیشتر آشنا خواهید شد.

۳ الگوریتم Deutsch-Jozsa

در ادامه با الگوریتم Deutsch-Jozsa آشنا می‌شویم که گسترش الگوریتم Deutsch به حالتی است که تعداد ورودی‌های تابع بیش از یک بیت یا کیوبیت باشد. به صورت خاص، فرض می‌کنیم که یک تابع $f : \{0,1\}^n \to \{0,1\}$

[4] Query Complexity
[5] Oracle
[6] Black Box

داریم که تعداد ورودی‌های آن n و یک خروجی «صفر» یا «یک» دارد. ما از قبل می‌دانیم که این تابع یا «متوازن» است و یا «ثابت».

فرض کنید که تابع f به صورت یک جعبه سیاه در اختیار ما قرار گرفته است و از قبل نیز مطمئن هستیم که آن تابع حتماً یا ثابت است و یا متوازن. هدف ما این است که متوجه شویم این جعبه سیاه از کدام نوع است؟ اگر این جعبه سیاه به صورت کلاسیک کار کند، لازم است که $\frac{2^n}{2}+1$ بار به آن ورودی دهیم و خروجی را مشاهده کنیم، پیش از آنکه بتوانیم تصمیم‌گیری کنیم. توجه کنید که در کل 2^n حالت متفاوت ورودی متصور هستند. یک تابع متوازن به اندازه نیمی از آن‌ها ورودی یکسانی را تولید می‌کنید و به این ترتیب با مشاهده نیمی از ورودی‌ها امکان تشخیص آن از یک تابع ثابت وجود ندارد. اما اگر یک ورودی بیشتر از نصف را نیز مشاهده کنیم می‌توانیم فرق بین متوازن و ثابت را متوجه شویم. اما اگر جعبه سیاه به صورت کوانتومی کار کند با استفاده از الگوریتم Deutsch-Jozsa می‌توانیم با یک فراخوانی نوع آن را تشخیص دهیم. اسلاید شماره ۱۲ را ببینید.

در اسلاید ۱۳ مدار الگوریتم Deutsch-Jozsa را می‌بینیم که بسیار به مدار Deutsch شبیه است. در اینجا نیز ابتدا ورودی را در حالت $|0\rangle^{\otimes n}$ قرار می‌دهیم و خروجی را در حالت $|1\rangle$ آماده می‌کنیم. سپس بر روی تمام سیم‌ها پیش از ورود به دریچه‌ای که تابع ناشناخته را پیاده‌سازی می‌کند دریچه هادامارد را اعمال می‌کنیم. ورودی به حالت زیر می‌رود (حالت برهم‌نهاده تمام حالت‌های ممکن):

$$\sum_{x\in\{0,1\}^n}\frac{1}{\sqrt{2^n}}|x\rangle \tag{۷}$$

و خروجی نیز در حالت زیر قرار می‌گیرد:

$$\frac{|0\rangle-|1\rangle}{\sqrt{2}} \tag{۸}$$

در صورتی که تابع بر روی این مقادیر اعمال شود، اگر خروجی تابع صفر باشد، سیم خروجی تغییر نمی‌کند. اما اگر خروجی تابع یک باشد سیم خروجی از $|0\rangle$ به $|1\rangle$ و از $|1\rangle$ به $|0\rangle$ تغییر می‌کند:

$$|x\rangle(|0\rangle-|1\rangle)\rightarrow f(x)=0\rightarrow|x\rangle(|0\oplus 0\rangle-|1\oplus 0\rangle)=|x\rangle(|0\rangle-|1\rangle) \tag{۹}$$

$$|x\rangle(|0\rangle-|1\rangle)\rightarrow f(x)=1\rightarrow|x\rangle(|0\oplus 1\rangle-|1\oplus 1\rangle)=|x\rangle(|1\rangle-|0\rangle) \tag{۱۰}$$

حاصل این مسئله به صورت ضریب $-1^{f(x)}$ در حالت سیستم اعمال می‌شود (فرمول دوم اسلاید ۱۴ را ببینید). در واقع این نوعی از پدیده Phase Kickback است که در آن کیوبیت هدف در نهایت بدون تغییر باقی‌مانده است و یک فاز سراسری به سیستم اضافه شده است. حال n سیم ورودی پس از اعمال تابع f را از یک دریچه هادامارد گذر می‌دهیم. ابتدا به تساوی زیر نگاه کنید:

$$H^{\otimes n}|x\rangle=\frac{1}{\sqrt{2^n}}\sum_{z\in\{0,1\}^n}(-1)^{x.z}|z\rangle \tag{۱۱}$$

این عملیات یک حالت n کیوبیتی $|x\rangle$ را به حالت برهم‌نهاده می‌برد. در این حالت برهم‌نهاده تمام حالت‌های مختلف n کیوبیتی وجود دارد و به همین خاطر به ازای تمام $z \in \{0,1\}^n$ بردارهای $|z\rangle$ لحاظ شده‌اند. ضریب $\frac{1}{\sqrt{2^n}}$ نیز نشان می‌دهد احتمال حضور در تمام این حالت‌ها برابر است.

مثال:

$$H^{\otimes 3}|101\rangle = \frac{1}{\sqrt{2^n}}\Big((-1)^{101.000}|000\rangle(-1)^{101.001}|001\rangle(-1)^{101.010}|010\rangle(-1)^{101.011}|011\rangle \qquad (۱۲)$$

$$(-1)^{101.100}|100\rangle(-1)^{101.101}|101\rangle(-1)^{101.110}|110\rangle(-1)^{101.111}|111\rangle\Big) \qquad (۱۳)$$

$$= \frac{1}{\sqrt{2^n}}\Big(|000\rangle - |001\rangle + |010\rangle - |011\rangle - |100\rangle + |101\rangle - |110\rangle + |111\rangle\Big) \qquad (۱۴)$$

توجه کنید که ضربی که در توان $1-$ قرار دارد به صورت زیر انجام می‌گیرد:

$$x.z = (x_{n-1}z_{n-1} + \cdots + x_1 z_1 + x_0 z_0). \qquad (۱۵)$$

سپس این مقدار را در حالت سیستم جایگذاری می‌کنیم و به حالت زیر می‌رسیم:

$$|\psi_3\rangle = \sum_{x\in\{0,1\}^n} \frac{1}{\sqrt{2^n}}(-1)^{f(x)} \sum_{z\in\{0,1\}^n} \frac{1}{\sqrt{2^n}}(-1)^{x.z}|z\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \qquad (۱۶)$$

که این مقدار به معادله انتهای اسلاید ۱۴ خلاصه می‌شود. حال دقت کنید، اگر تابع مطلوب ما ثابت باشد، حالت‌های زیر رخ می‌دهد:

$$f(x) = 0 \rightarrow \mathbb{P}\{|z\rangle = |0\rangle^{\otimes n}\} = |\sum_{x\in\{0,1\}^n} \frac{1}{2^n}(-1)^{x.0+0}| = |1| = 1 \qquad (۱۷)$$

$$f(x) = 1 \rightarrow \mathbb{P}\{|z\rangle = |0\rangle^{\otimes n}\} = |\sum_{x\in\{0,1\}^n} \frac{1}{2^n}(-1)^{x.0+1}| = |-1| = 1 \qquad (۱۸)$$

بنابراین نتیجه می‌گیریم که اگر تابع «ثابت باشد» احتمال اینکه n سیم مرتبط با ورودی پس از اعمال تابع و دریچه هادامارد در حالت $|0\rangle^{\otimes n}$ قرار بگیرند برابر یک است. به طور مشابه، اگر تابع متوازن باشد حالت زیر رخ می‌دهد:

$$\mathbb{P}\{|z\rangle = |0\rangle^{\otimes n}\} = |\sum_{x\in\{0,1\}^n} \frac{1}{2^n}(-1)^{x.0+f(x)}| \qquad (۱۹)$$

$$= |\sum_{x\in\{0,1\}^n} \frac{1}{2^n}(-1)^{f(x)}| = 0. \qquad (۲۰)$$

دقت کنید که تابع متوازن به ازای نیمی از ورودی‌ها x برابر صفر و به ازای نیمی از آن‌ها برابر یک است. بنابراین حاصل جمع آن صفر می‌شود. یعنی احتمال حضور در حالت $|0\rangle^{\otimes n}$ صفر است. در نتیجه یک راه ساده برای تشخیص ثابت و یا متوازن بودن تابع در اختیار داریم. اگر کیوبیت‌های مرتبط با $|x\rangle$ را اندازه گرفتیم و تمام آن‌ها صفر بودند (یعنی

سیستم در حالت $|0\rangle^{\otimes n}$ بوده است) پس تابع ثابت است. اما اگر حتی یک اندازه گیری «یک» را بدست بیاوریم در می‌یابیم تابع از نوع متوازن بوده است. اسلاید ۱۵ را ببینید.

در نهایت، در اسلاید ۱۶ ملاحظه می‌کنید که ممکن است دستیابی به یک «تسریع نمایی» از طریق الگوریتم Deutsch-Jozsa امکان‌پذیر باشد. به این ترتیب که اگر بخواهیم نوع یک تابع را مشخص کنیم به جای $2^{n-1}+1$ فراخوانی فقط یک فراخوانی انجام می‌دهیم. بنابراین اگر تابع در جای دوری قرار داشته باشد که برای شناسایی آن لازم باشد ورودی به آن‌جا ارسال شود و خروجی از آن‌جا دریافت شود، با استفاده کردن از مدل کلاسیک به جای مدل کوانتومی تعداد دفعات رد و بدل کردن پیام به صورت نمایی رشد می‌کند. البته اگر شرایط به الگوریتم‌های دارای خطای محدود [۷] گسترش دهیم خواهیم دید که الگوریتم‌های تصادفی کلاسیک وجود دارند که با تعداد فراخوانی‌های «ثابت [۸]» می‌توانند به خطاهای کوچکی دست پیدا کنند. به این ترتیب تسریعی مشاهده نمی‌شود!

[7] Bounded-error Algorithms
[8] Constant