محاسبات کوانتمی (۲۲۶۷۱) ترم بهار ۱۳۹۱-۱۳۹۰

مدرس: سلمان ابوالفتح بیگی نویسنده: حامد کبیری کناری

جلسه ۷

۱ مدل محاسباتی مداری کلاسیک

در حالت کلی یک محاسبه را می‌توان اعمال یک تابع $f : \{0,1\}^n \to \{0,1\}^m$ بر روی یک ورودی $x \in \{0,1\}^n$ در نظر گرفت. برای این کار یک محاسبه را به اجزاء کوچک‌تر تقسیم می‌کنیم. «مدل مداری» برای محاسبات کلاسیک دارای بخش‌های زیر است.

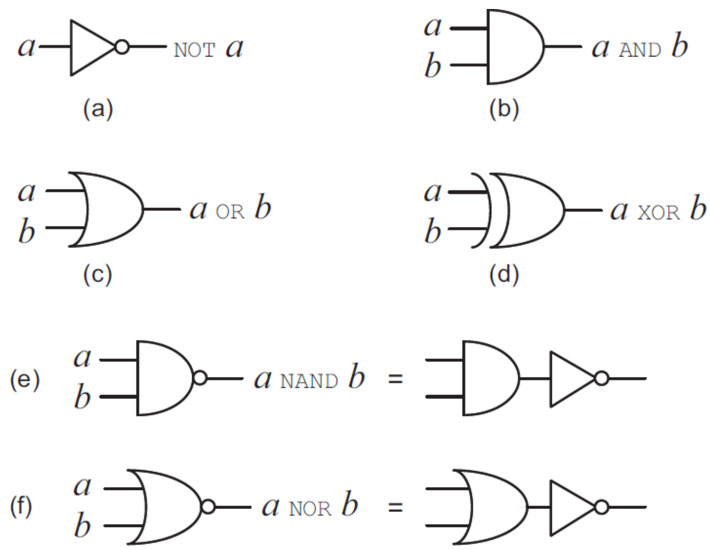
۱. **نمایش اطلاعات:** در مدارهای کلاسیک اطلاعات به صورت بیت نمایش داده می‌شوند. به طور مثال در محاسبه تابع $f : \{0,1\}^n \to \{0,1\}^m$ باید n بیت ورودی و m بیت خروجی در مدار در نظر گرفت.

۲. **بیت کمکی:** بیت هایی هستند که در ابتدای مدار یک مقدار ثابت مستقل از ورودی $x \in \{0,1\}^n$ را دارا می باشند و در طول محاسبه از آنها (مثلاً برای ذخیره‌ی حاصل بخشی از محاسبات) استفاده می‌شود. به این بیت‌ها، بیت‌های کمکی[۱] گفته می‌شود.

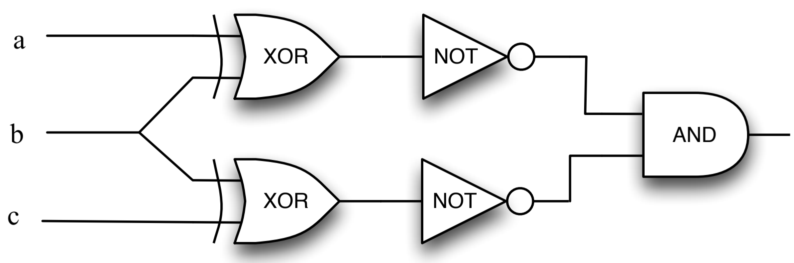
۳. **FANOUT:** در برخی از مدارها لازم است که از یک بیت کپی برداری، و در جای دیگر استفاده شود. به این عمل FANOUT گفته می‌شود.

۴. **گیت های محاسباتی:** بخش‌هایی از مدار که محاسبات ساده‌ای را انجام می‌دهند و از دنبال هم قرار دادن این گیت‌ها محاسبات در مدار انجام می‌شود . مهم‌ترین گیت‌های محاسباتی که در مدارها مورد استفاده قرار می‌گیرند در شکل زیر نشان داده شده‌اند.

[۱] Ancilla



مثلا شکل زیر یک مدار را نشان می دهد که دارای سه بیت ورودی است. خروجی این مدار 1 است در صورتی که هر سه ورودی یکسان باشند ($a = b = c$) و در غیر این صورت خروجی 0 خواهد بود.



قضیه‌ی زیر با استقرا روی n قابل اثبات است.

قضیه ۱ هر تابع $f : \{0,1\}^n \to \{0,1\}^m$ را می توان بر حسب گیت‌های AND و NOT نوشت .

تعریف ۲ مجموعه‌ی $\mathcal{G}$ از گیت‌ها را مجموعه‌ای کامل[۲] گویند هرگاه برای هر تابع $f : \{0,1\}^n \to \{0,1\}^m$ مداری وجود داشته باشد که گیت‌های تشکیل دهنده‌ی آن درون $\mathcal{G}$ باشند (مدار می‌تواند شامل $FANOUT$ و بیت کمکی نیز باشد) و تابع f را اعمال کند.

طبق این قضیه‌ی ۱، $\{AND, NOT\}$ یک مجموعه‌ی کامل است.

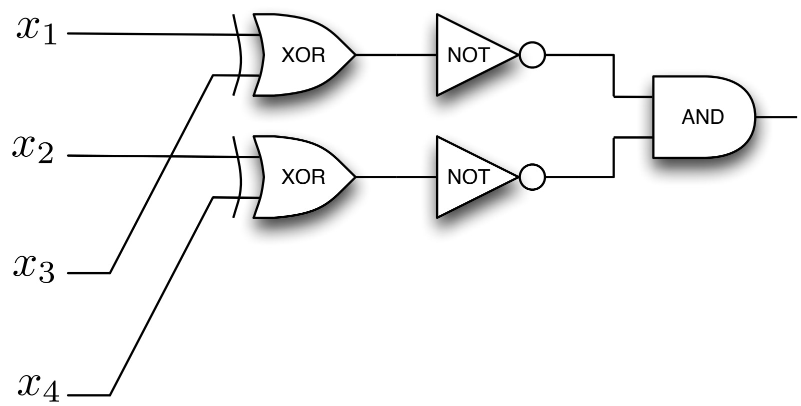
قضیه ۳ مجموعه $\{\ NAND\ \}$ یک مجموعه‌ی کامل است.

برای اثبات این قضیه، طبق قضیه‌ی ۱، کافی است گیت‌های AND و NOT را بر حسب $NAND$ بنویسیم.

[۲] Universal set of gates

تعریف ۴ یک خانواده از مدارها [۳] شامل مجموعه‌ای از مدارها $\{C_n\}_{n\geqslant 1}$ است که در آن C_n دارای n بیت ورودی است. پس برای انجام محاسبه با استفاده از این خانواده، اگر ورودی x شامل n بیت باشد از مدار C_n استفاده می‌کنیم.

مثلا فرض کنید تابع $f_n : \{0,1\}^{2n} \to \{0,1\}$ به این صورت باشد که $f(x_1 \dots x_{2n}) = 1$ اگر و فقط اگر $x_i = x_{n+i}$ برای $i = 1, \dots, n$. خانواده‌ی مدارهایی که توابع f_n را محاسبه می‌کنند برای $n = 2$ دارای ساختار زیر می‌باشد.



۲ پیچیدگی محاسبات

برای تحلیل هر الگوریتم (مدار) از مقدار زمان اجرای الگوریتم و مقدار حافظه‌ی مصرفی استفاده می شود. زمان اجرای مدار بر حسب تعداد گیت‌های درون مدار قابل بیان است. مثلا در مدار محاسباتی تابع f_n در مثال بالا به $2n + \lceil \log n \rceil$ گیت نیاز است. تعریف مقدار حافظه‌ی مصرفی بر حسب مدل مداری کمی پیچیده است، ولی به طور خلاصه مربوط به تعداد بیت‌های کمکی و همچنین مقدار موازی سازی مدار می‌شود.

برای یک خانواده از مدارها $\{C_n\}_{n\geqslant 1}$ تعداد گیت‌های C_n را با t_n و مقدار حافظه‌ی مورد نیاز آن را با s_n نشان می‌دهیم. رابطه‌ی $s_n \leq t_n \leq 2^{s_n}$ همواره برقرار است.

تعریف ۵ اگر برای یک مسأله، خانواده‌ای (یکنواخت) از مدارها وجود داشته باشد که آن مسأله را حل کند و برای آن خانواده چند جمله‌ای $P(n)$ وجود داشته باشد به طوری که $t_n \leq P(n)$، آنگاه آن مسأله درون کلاس پیچیدگی[۴] چند جمله‌ای است. کلاس همه مسأله‌های چند جمله‌ای را با P نمایش می‌دهیم.

به طور مشابه EXP کلاس مسائلی است که برای حل آنها خانواده‌ای (یکنواخت) از مدارها وجود دارد به طوری که برای یک چند جمله‌ای $P(n)$ داشته باشیم $t_n \leq 2^{P(n)}$. طبق تعریف $P \subseteq EXP$.

تعریف ۶ اگر برای یک مسأله خانواده‌ای (یکنواخت) از مدارها وجود داشته باشد که آن مسأله را حل کند و برای آن خانواده چند جمله‌ای $P(n)$ وجود داشته باشد به طوری که $s_n \leq P(n)$، آنگاه آن مسأله درون کلاس پیچیدگی‌ای است

[۳] Circuit family
[۴] Complexity class

که با $PSPACE$ نشان داده می‌شود.

با توجه به $s_n \leq t_n \leq 2^{s_n}$ رابطه‌ی زیر برقرار است:

$$P \subseteq PSPACE \subseteq EXP.$$

تعریف ۷ مدار احتمالاتی (الگوریتم محاسباتی) مداری می باشد که در آن برخی از بیت های کمکی حالت احتمالاتی دارند. یعنی با احتمال $1/2$ یک و با احتمال $1/2$ صفر می باشند.

تعریف ۸ کلاس پیچیدگی BPP[5] شامل تمام مسأله‌هایی می باشد که برای آنها مدار احتمالاتی‌ای با زمان چند جمله‌ای وجود دارد که با احتمال حداقل $2/3$ نتیجه درست را محاسبه می کند، و احتمال خطا در آنها حداکثر $1/3$ است.

توجه کنید که در تعریف BPP عدد $2/3$ قابل تغییر به هر عدد $p > 1/2$ است. در واقع حتی اگر احتمال جواب درست مثلاً به صورت $1/2 + 1/n^2$ باشد باز به همان کلاس پیچیدگی BPP (که با پارامتر $2/3$ تعریف شده) می‌رسیم. طبق تعریف BPP شامل P است، و می‌توان نشان داد $BPP \subseteq PSPACE$.

۳ مدارهای کوانتومی

اجزاء مدارهای کوانتمی به صورت زیر هستند.

۱. **نمایش اطلاعات:** در مدارهای کوانتومی اطلاعات با کیوبیت‌ها (سیستم‌های کوانتمی دو بعدی) نمایش داده می‌شوند. اگر ورودی مسأله دنباله‌ی $x_1, x_2, ..., x_n$ از بیت‌های کلاسیک باشد، آن را در یک مدار کوانتمی با

$$|x_1\rangle \otimes |x_2\rangle \otimes ... \otimes |x_n\rangle = |x_1 x_2 \dots x_n\rangle$$

نمایش می‌دهیم.

۲. **کیوبیت کمکی:** در مدارهای کوانتومی نیز می توان از کیوبیت‌های کمکی همانند مدارهای کلاسیک استفاده کرد. کیوبیت‌های کمکی در حالت $|0\rangle$ آماده سازی می‌شوند.

۳. **گیت‌های یکانی:** در حالت کلاسیک یک گیت در واقع یک تابع (یک تحول زمانی کلاسیک) است که روی تعداد کمی بیت عمل می‌کند. در فیزیک کوانتم، تحول‌های زمانی با تبدیلات خطی یکانی داده می‌شوند. بنابراین گیت‌های کوانتمی، تبدیلات یکانی‌ای هستند که روی تعدادی کمی کیوبیت عمل می‌کنند. مهم ترین گیت های کوانتومی در زیر معرفی شده اند .

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

[5] Bounded-error Probabilistic Polynomial time

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

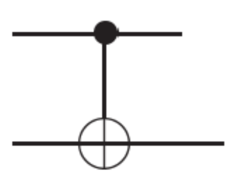
هریک از این گیت ها را در مدارهای کوانتومی با نام خود نشان می دهند. در زیر تصویر این گیت ها در مدارهای کوانتومی نشان داده شده است.

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

دسته‌ی دیگری از گیت‌های کوانتومی گیت‌های کنترلی هستند. یکی از مهم ترین گیت‌ها از این دسته گیت $CNOT$ است که دو کیوبیت ورودی دارد که یکی کیوبیت کنترل و دیگری کیوبیت هدف است. عملیاتی که گیت $CNOT$ انجام می دهد را می توان به صورت $|c\rangle|t\rangle \rightarrow |c\rangle|t \oplus c\rangle$ نوشت که اگر کیوبیت کنترل $|1\rangle$ باشد کیوبیت هدف تغییر می کند و در غیر این صورت تغییری صورت نمی گیرد. $CNOT$ یک ماتریس 4×4 است:

$$CNOT = \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix}.$$

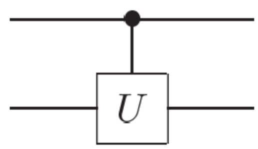
در مدارها این گیت به صورت زیر نمایش داده می‌شود که در آن کیوبیت بالایی، کیوبیت کنترل، و پایینی کیوبیت هدف است.



به طور کلی برای هر گیت U با اضافه کردن یک کیوبیت کنترلی c می‌توان گیت کنترلی $Controlled - U$ را تعریف کرد:

$$Controlled-U = \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}$$

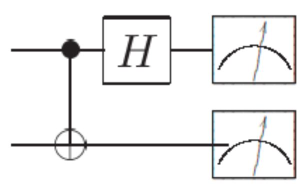
در واقع $CNOT = Controlled-X$. در شکل زیر نمایش مداری گیت $Controlled-U$ نشان داده شده است:



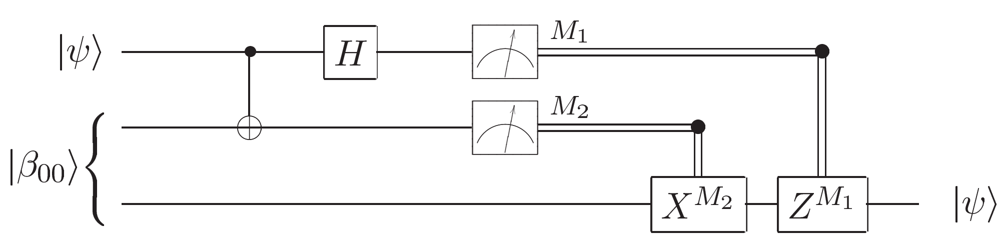
۴. **اندازه گیری:** برای مشخص شدن حاصل محاسبه در انتهای یک مدار کوانتمی باید یک اندازه‌گیری انجام شود. همان طور که فرض می‌کنیم گیت‌ها، تحول‌های زمانی ساده هستند، در مدارهای کوانتمی نیز فقط اندازه‌گیری‌های ساده را در نظر می‌گیریم. تنها اندازه‌گیری‌ای که در مدارهای کوانتمی در نظر گرفته می‌شود اندازه‌گیری یک کیوبیت در پایه استاندارد $\{|0\rangle, |1\rangle\}$ است. این اندازه گیری به صورت زیر نمایش داده می شود.

توجه: در مدارهای کوانتومی $FANOUT$ وجود ندارد، زیرا طبق قضیه‌ی *No-cloning* در مکانیک کوانتم اطلاعات را نمی‌توان کپی کرد. (به صفحه‌ی ۵۳۲ کتاب مراجعه کنید.)

مثال: در شکل زیر مدار اندازه‌گیری در پایه‌ی $Bell$ نشان داده شده است که به وسیله گیت‌های $Hadamard$ و $C-NOT$ و اندازه‌گیری در پایه‌ی استاندارد پیاده سازی شده است .



در نتیجه مدار کوانتومی مربوط به *teleportation* به صورت زیر است.



در این مدار $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$، و M_2, M_1 بیت‌هایی کلاسیکی هستند که حاصل اندازه‌گیری‌ها را نشان می‌دهند.

۴ پیچیدگی محاسبات کوانتومی

تعریف ۹ کلاس پیچیدگی BQP[6] شامل تمام مسأله‌هایی است که برای آنها یک خانواده از مدارهای کوانتومی وجود دارد که تعداد گیت‌های آنها چندجمله‌ای است و با احتمال حداقل $2/3$ نتیجه درست را محاسبه می کند.

همانند *BPP*، عدد $2/3$ در تعریف *BQP* قابل تغییر به هر عدد $p > 1/2$ است.

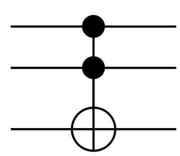
۱.۴ BPP ⊆ BQP

برای ثابت کردن $BPP \subseteq BQP$ باید نشان دهیم که هر مدار کلاسیک را می‌توان به یک مدار کوانتمی «معادل» تبدیل کرد به طوری که تعداد گیت‌های متناظر تقریباً برابر تعداد گیت‌های مدار کلاسیک باشد. از آنجا که هر مدار کلاسیک را می‌توان با $NAND$ و $FANOUT$ ساخت، کافی است نشان دهیم که این دو گیت کلاسیک را می‌توان به صورت کوانتمی پیاده سازی کرد.

برای این کار می‌توان از گیت *Toffoli* استفاده کرد. گیت *Toffoli* روی سه کیوبیت عمل می‌کند که حاصل آن روی بردارهای پایه‌ی استاندارد به صورت زیر است

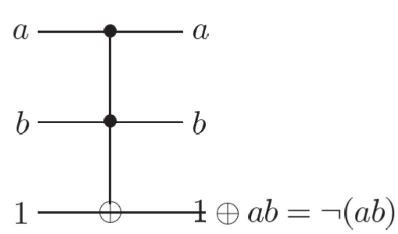
$$|a\rangle|b\rangle|c\rangle \mapsto |a\rangle|b\rangle|c \oplus ab\rangle$$

و در مدارها به صورت زیر نمایش داده می‌شود

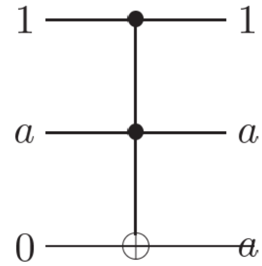


توجه کنید که گیت *Toffoli* دارای دو کیوبیت کنترلی و یک کیوبیت هدف است و آن را می‌توان به صورت *Controlled-Controlled-X* در نظر گرفت.

در شکل‌های زیر گیت $NAND$ و $FANOUT$ با کمک *Toffoli* و کیوبیت‌های کمکی پیاده‌سازی شده‌اند.



[6] Bounded-error Quantum Polynomial time



۲.۴ BQP $\subseteq$ PSPACE

در این جا نشان می‌دهیم که هر محاسبه‌ی کوانتمی را می‌توان به صورت کلاسیک شبیه‌سازی کرد. به این معنا که هر مسأله‌ای که با استفاده از یک مدار کوانتمی قابل حل باشد، به طور کلاسیک نیز قابل حل است. توجه کنید که این شبیه‌سازی ممکن است بهینه نباشد.

یک مدار کوانتمی در نظر بگیرید که مجموع کیوبیت‌های ورودی و کمکی آن $q(n)$ و تعداد گیت‌های آن $p(n)$ باشد. در نتیجه حالت سیستم در ابتدای مدار با یک بردار در فضای $2^{q(n)}$ بعدی مشخص می‌شود. یعنی $2^{q(n)}$ عدد مختلط کافی است برای بیان حالت سیستم. همچنین هر یک از گیت‌های یکانی نیز متناظر با یک ماتریس یکانی $2^{q(n)} \times 2^{q(n)}$ است. لذا با ضرب ماتریسی می‌توان بردار حاصل پس از اعمال هر یک از گیت‌های کوانتمی را به صورت کلاسیک حساب کرد. در انتهای مدار که اندازه‌گیری انجام می‌شود، توزیع احتمال متناظر را می‌توان از روی مؤلفه‌های بردار $2^{q(n)}$ بعدی حساب کرد. در نتیجه کل مدار کوانتمی را می‌توان به صورت کلاسیک شبیه‌سازی کرد.

اگر الگوریتم کوانتمی متناظر چندجمله‌ای باشد، $p(n), q(n)$ چندجمله‌ای خواهند بود. عملیات متناظر با اعمال یک گیت کوانتمی، برابر ضرب کردن یک ماتریس $2^{q(n)} \times 2^{q(n)}$ در یک بردار است، و لذا به ازای هر گیت کوانتمی حدوداً $2^{2q(n)}$ عمل کلاسیک وجود دارد. بنابراین تعداد عملیات کلاسیک در شبیه‌سازی تقریباً برابر $p(n)2^{2q(n)}$ است. نتیجه می‌گیریم که $BQP \subseteq EXP$.

تحلیل دقیق‌تر شبیه‌سازی فوق نشان می‌دهد که $BQP \subseteq PSPACE$. پس داریم

$$P \subseteq BPP \subseteq BQP \subseteq PSPACE \subseteq EXP.$$