

مقدمه‌ای بر محاسبات کوانتومی و پیچیدگی آن

لیلا تقوی

۳۰ خرداد ۱۳۹۴

۱ مقدمه

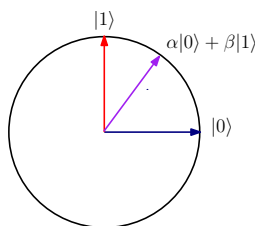
در این گزارش ابتدا معرفی کوتاهی از مکانیک کوانتومی ارائه کرده و سپس با بیان چند مثال ساده از الگوریتم‌های کوانتومی به بیان برتری نسبی دنیای کوانتوم نسبت به دنیای کلاسیک در برخی مسائل می‌پردازیم. در انتها پیچیدگی محاسباتی الگوریتم‌های کوانتومی و قدرت ماشینی که بر مبنای فیزیک کوانتومی کار کند را مطرح می‌کنیم.

۲ مروری بر فیزیک کوانتومی

واحد نمایش اطلاعات در دنیای کلاسیک بیت است که در حالت مشخص ۰ یا ۱ قرار دارد. در حالی که واحد اطلاعات کوانتومی کیوبیت^۱ نام دارد. یک کیوبیت می‌تواند به طور همزمان در حالت صفر و یک باشد، به این پدیده برهم‌نهی^۲ گویند. یک کیوبیت را با برداری به طول واحد مانند $\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha|0\rangle + \beta|1\rangle$ که در آن $|\alpha|^2 + |\beta|^2 = 1$ نمایش می‌دهیم. نماد $|\cdot\rangle$ که کت^۳ خوانده می‌شود، نشان دهنده یک بردار ستونی است.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

در دنیای واقعی برای محقق کردن یک کیوبیت از هر سیستمی با دو حالت می‌توان استفاده کرد. به عنوان یک مثال ملموس می‌توان از یک اتم هیدروژن با یک الکترون که می‌تواند در حالت پایه^۴ یعنی مدار اول یا حالت برانگیخته^۵ یعنی مدار دوم باشد، نام برد.



شکل ۱: حالت یک کیوبیت توسط یک بردار به طول واحد نمایش داده می‌شود.

$|0\rangle$ و $|1\rangle$ به عنوان پایه استاندارد برای نمایش بردار حالت یک کیوبیت به کار می‌رود. در حالت کلی می‌توان یک حالت کوانتومی با بیش از دو بعد داشت که در این صورت از پایه‌های $|1\rangle, |2\rangle, \dots, |k\rangle$ برای نمایش آن استفاده می‌شود. روش دیگری نیز برای داشتن حالت کوانتومی با بیش از دو بعد وجود دارد که کنار هم قرار دادن k کیوبیت بدست می‌آید. با این کار یک سیستم کوانتومی با بعد 2^k ساخته‌ایم.

همان طور که در شکل ۲ می‌بینید حالت سیستم در این صورت از ضرب تانسوری بردارهای حالت این k کیوبیت در یکدیگر به دست می‌آید. در حالت کلی یک سیستم n بعدی یک برهم‌نهی بردارهای پایه است، یعنی: $\alpha_1|1\rangle + \alpha_2|2\rangle + \dots + \alpha_n|n\rangle$ که در آن $|\alpha_1|^2 + |\alpha_2|^2 + \dots + |\alpha_n|^2 = 1$.

qubit^۱
superposition^۲
ket^۳
state roundg^۴
state xcitede^۵

$$\begin{array}{lll}
\textcolor{red}{q_1} & \textcolor{blue}{q_2} & \\
|0\rangle & |0\rangle & \longrightarrow |00\rangle \\
\frac{|0\rangle+|1\rangle}{\sqrt{2}} & |0\rangle & \longrightarrow \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \\
\frac{|0\rangle+|1\rangle}{\sqrt{2}} & \frac{|0\rangle+|1\rangle}{\sqrt{2}} & \longrightarrow \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)
\end{array}$$

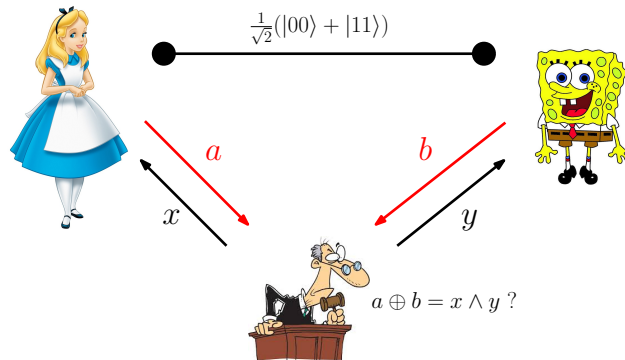
شکل ۲: یک سیستم چهار بعدی متشکل از دو کیوبیت که در آن حالت کلی سیستم از ضرب تانسوری حالت دو کیوبیت بدست می‌آید. کیوبیت اول با رنگ قرمز و کیوبیت دوم با رنگ آبی نمایش داده شده است.

۱.۲ درهم‌تنیدگی

گاهی اوقات حالت یک سیستم را نمی‌توان به صورت ضرب تانسوری حالت کیوبیت‌های آن نوشت. به چنین پدیده‌ای درهم‌تنیدگی^۶ گویند. برای مثال حالت‌های زیر که دارای بیشترین مقدار درهم‌تنیدگی هستند، حالت‌های بل^۷ نام دارند.

$$\begin{aligned}
\Phi_1 &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
\Phi_2 &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\
\Psi_1 &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\
\Psi_2 &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)
\end{aligned}$$

به کمک درهم‌تنیدگی برخی از قواعد دنیای کلاسیک را می‌توان نقض کرد. به عنوان مثال یک بازی^۸ دونفره بین آلیس و باب را در نظر بگیرید که در بیشان دو کیوبیت که در حالت بل هستند به اشتراک گذاشته شده است. بازی به این صورت است که آلیس و باب پس از دریافت دو بیت تصادفی $x, y \in \{0, 1\}$ بیت‌های $a, b \in \{0, 1\}$ را به عنوان پاسخ برمی‌گردانند. آنها در صورتی برنده می‌شوند که $a \oplus b = x \wedge y$ ثابت می‌شود که در حالت کلاسیک بیشترین احتمال برد $\frac{3}{4}$ است ولی پروتکلی وجود دارد که با استفاده از کیوبیت‌های بل به اشتراک گذاشته شده می‌توان این احتمال را به 0.85 افزایش داد.

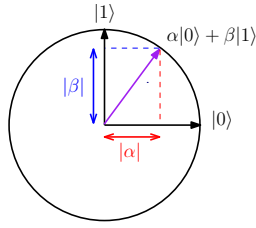


شکل ۳: بازی CHSH مثالی از استفاده درهم‌تنیدگی برای نقض قواعد دنیای کلاسیک.

۲.۲ اندازه‌گیری

حالت یک کیوبیت را می‌توان با یک بردار یکه نمایش داد لذا بینهایت داده را می‌توان در آن کد کرد. در نگاه اول این مسئله شگفت‌انگیز به نظر می‌رسد. ولی برای بازیابی اطلاعاتی که در یک کیوبیت کد شده است باید آن را اندازه گرفت. طبق اصول مکانیک کوانتومی حالت یک کیوبیت بعد از اندازه‌گیری درهم می‌شکند^۹. به این معنی که اگر حالت یک کیوبیت $\alpha|0\rangle + \beta|1\rangle$ باشد حالت آن بعد از اندازه‌گیری در پایه $\{|0\rangle, |1\rangle\}$ با احتمال $|\alpha|^2$ به حالت $|0\rangle$ و با احتمال $|\beta|^2$ به حالت $|1\rangle$ درهم می‌شکند. لذا بعد از اندازه‌گیری یک کیوبیت نمی‌توان بیش از دو بیت اطلاعات را از یک کیوبیت بازیابی کرد.

^۶ entanglement
^۷ Bell states
^۸ CHSH game
^۹ collapse



شکل ۴: بردار یکه نشان دهنده حالت یک کیوبیت که پس از اندازه‌گیری در پایه $\{|0\rangle, |1\rangle\}$ با احتمال $|\alpha|^2$ به حالت $|0\rangle$ و با احتمال $|\beta|^2$ به حالت $|1\rangle$ درهم می‌شکند.

۳ مدارهای کوانتومی

در مکانیک کوانتومی می‌توان حالت یک کیوبیت را متحول کرد. این کار توسط یک تبدیل خطی حافظ اندازه که با یک ماتریس یکانی قابل بیان است، انجام می‌شود. ماتریس یکانی U ماتریسی که در شرط $U^\dagger U = U U^\dagger = I$ صدق کند. U^\dagger الحاقی ماتریس U است:

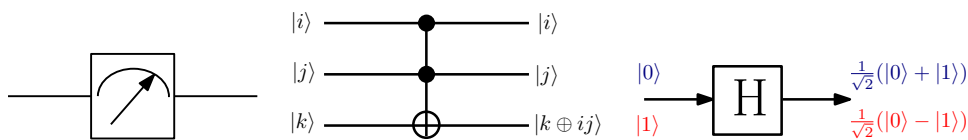
$$U = \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix} \Rightarrow U^\dagger = \begin{pmatrix} u_{00}^* & u_{10}^* \\ u_{01}^* & u_{11}^* \end{pmatrix}$$

مثال‌هایی از گیت‌های کوانتومی عبارتند از:

$$\begin{aligned} \text{Bit flip: } & \begin{cases} |0\rangle \rightarrow |1\rangle \\ |1\rangle \rightarrow |0\rangle \end{cases} \\ \text{Hadamard: } & \begin{cases} |0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{cases} \\ \text{CNOT: } & \begin{cases} |00\rangle \rightarrow |00\rangle \\ |01\rangle \rightarrow |01\rangle \\ |10\rangle \rightarrow |11\rangle \\ |11\rangle \rightarrow |10\rangle \end{cases} \equiv |i, j\rangle \rightarrow |i, i \oplus j\rangle \\ \text{Toffoli: } & |i, j, k\rangle \rightarrow |i, j, i \oplus j \oplus k\rangle \end{aligned}$$

از آنجا که گیت‌های کوانتومی تبدیلات خطی هستند، برای مشخص شدن عملکردشان روی کل فضا، کافی است عملکرد آن‌ها را روی بردارهای پایه فضا بدانیم. لذا هر گیت کوانتومی یک ماتریس یکانی است.

برای داشتن یک ماشین با قدرت محاسبه الگوریتم‌های کوانتومی نیاز به یک مجموعه جهانی متناهی از گیت‌های کوانتومی داریم. همان‌طور که در دنیای کلاسیک برای این منظور از مجموعه جهانی گیت‌های AND و OR و NOT استفاده می‌کنیم. مشکلی که در دید اول به نظر می‌رسد این است که گیت‌های کوانتومی یک مجموعه پیوسته از ماتریس‌های یکانی هستند که ساختن آن‌ها با یک مجموعه متناهی ممکن نیست. ولی ثابت شده است که هر گیت کوانتومی یکانی را با دقت دلخواه می‌توان به کمک گیت‌های هادامارد و توفولی تخمین زد.

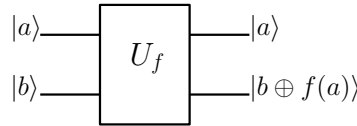


شکل ۵: از راست به چپ: گیت هادامارد، گیت توفولی، نماد اندازه‌گیری

گیت‌های یکانی معکوس پذیرند برای تبدیل یک تابع کلاسیک به یک تابع معکوس پذیر و ساختن آن به کمک گیت‌های کوانتومی، کافی است علاوه بر مقدار تابع ورودی‌های آن را نیز به خروجی بدهیم (شکل ۶ را ببینید).

۴ الگوریتم‌های کوانتومی

قبل از پرداختن به الگوریتم‌های کوانتومی در مورد گیت هادامارد و عملکرد آن توضیح مختصری می‌دهیم. می‌دانیم اگر گیت هادامارد روی حالت پایه $|0\rangle$ عمل کند یک برهم‌نهی از کل حالات یک کیوبیت با دامنه‌های برابر به ما می‌دهد، یعنی حالت: $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.



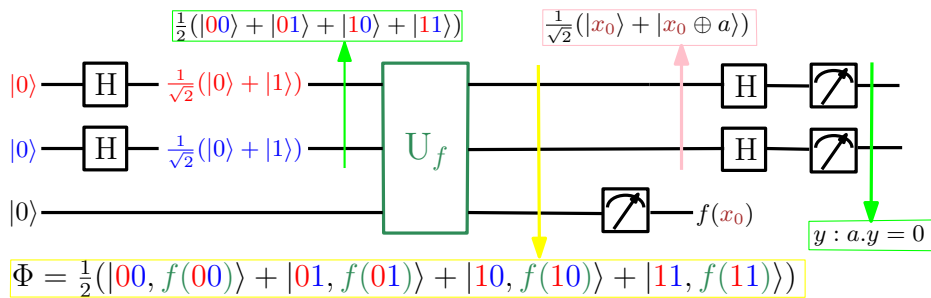
شکل ۶: تبدیل یک تابع کلاسیک به یک تابع معکوس پذیر

لذا برای ساختن یک برهم‌نهی از کل حالات $|0\rangle, |1\rangle, \dots, |2^k - 1\rangle$ کافی است روی k کیوبیت عملگر هادامارد اعمال کنیم. با داشتن چنین برهم‌نهی تنها با یکبار صدا زدن تابع f میتوان یک برهم‌نهی از مقدار تابع در تمام نقاط $0, 1, \dots, 2^k - 1$ به دست آورد.

به طور کلی عملگر هادامارد روی n کیوبیت به این شکل اثر می‌کند: $H^{\otimes n}|a\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{a \cdot x} |x\rangle$

۱.۴ الگوریتم یافتن دوره تناوب

در این الگوریتم که به الگوریتم سایمون^{۱*} معروف است، تابع $f: \{0, 1\}^* \rightarrow \{0, 1\}^*$ به ما داده شده است، هدف یافتن دوره تناوب این تابع با این شرط است که $\forall x \exists! a: f(x) = f(x \oplus a)$. مدار کوانتومی که برای این مسئله پیشنهاد شد در شکل ۷ نمایش داده شده است. در این شکل برای سادگی فرض شده تابع $f: \{0, 1\}^2 \rightarrow \{0, 1\}^2$ است. در این الگوریتم ابتدا یک برهم‌نهی از کل نقاط دامنه تابع ایجاد و سپس با یک بار صدا زدن تابع مقدار آن روی تمام نقاط دامنه به دست می‌آید که در شکل با بردار $|\Phi\rangle$ نشان داده شده است. در این مرحله با اندازه‌گیری n کیوبیت آخر که مقدار تابع را در خود دارند، حالت آن‌ها به یکی از مقادیر خروجی تابع f مثلاً $f(x_0) = f(x_0 \oplus a)$ درهم می‌شکند و در نتیجه حالت n کیوبیت اول به حالت $\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus a\rangle)$ درهم می‌شکند. به راحتی قابل اثبات است که از اندازه‌گیری این n کیوبیت بردار y حاصل می‌شود که در شرط $a \cdot y = 0$ صدق می‌کند. لذا با n بار اجرای این الگوریتم یک دستگاه n معادله و مجهول به دست می‌آید که حل آن بیت‌های a را به دست می‌دهد. زمان اجرای این الگوریتم $O(n^3)$ است که نسبت به بهترین الگوریتم کلاسیک که حداقل نیاز به $\Omega(2^{n/2})$ بار فراخوانی تابع دارد، افزایش سرعت نمایی دارد.



شکل ۷: مدار کوانتومی سایمون برای یافتن دوره تناوب تابع $\forall x \exists! a: f(x) = f(x \oplus a)$

۲.۴ الگوریتم تجزیه به عوامل اول

افزایش سرعت نمایی در الگوریتم یافتن دوره تناوب سایمون انگیزه‌ای برای حل مسئله دیگری به نام تجزیه اعداد شد. این مسئله از نظر امنیتی بسیار با اهمیت است، زیرا مبنای الگوریتم معروف رمزنگاری RSA سختی تجزیه اعداد بزرگ به عوامل اولشان است. در این الگوریتم که به الگوریتم تجزیه شور^{۱۱} معروف است یک N داده شده است و هدف تجزیه آن به عوامل اولش است. ایده اصلی حل این مسئله کاهش آن به مسئله یافتن دوره تناوب است. برای این کار از قانون زیر استفاده می‌شود:

اگر N حاصلضرب دو عدد اول باشد یعنی $N = p \times Q$ ، برای هر x که p و q را بشمارد، دنباله

$$x \bmod N, x^2 \bmod N, x^3 \bmod N, \dots$$

دوره تناوبی دارد که $(p-1)(q-1)$ را می‌شمارد.

پس کافی است چند x خوب انتخاب شود و بعد از پیدا کردن چند شمارنده $(p-1)(q-1)$ با احتمال خوبی خود p و q تخمین زده شود. نقش کوانتوم در این الگوریتم یافتن دوره تناوب است که با کمک تکنیکی مشابه الگوریتم سایمون کار می‌کند.


^{۱*}Simon
^{۱۱}Shor

۳.۴ الگوریتم جستجوی کوانتومی

افزایش سرعت نمایی در الگوریتم‌های ارائه شده این امید را به ما می‌دهد که با حل سریع مسئله جستجو، بتوانیم مسائل تمام-NP را در زمان چندجمله‌ای حل کنیم. در این بخش الگوریتم زمان $O(\sqrt{n})$ متناسب به گراور را ارائه می‌کنیم. در این الگوریتم فرض شده که یک گیت $U_f|x\rangle$ وجود دارد که:

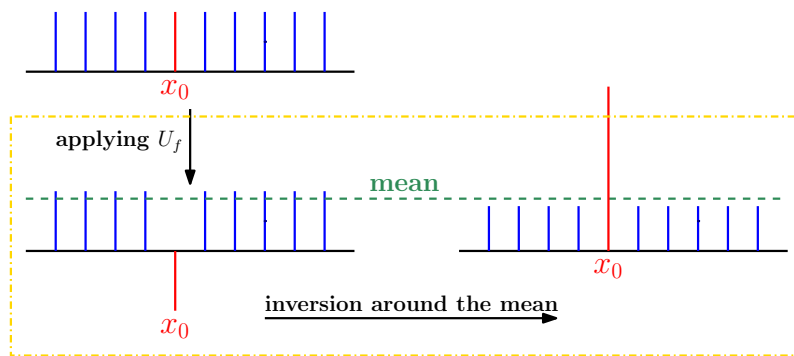
$$U_f(|x\rangle) = \begin{cases} -|x\rangle & \text{if } |x\rangle = |x_0\rangle \\ |x\rangle & \text{if } |x\rangle \neq |x_0\rangle \end{cases}$$

و ما به دنبال پیدا کردن این x_0 هستیم. ابتدا با اعمال یک گیت هادامارد همانطور که در الگوریتم‌های قبلی گفته شد، یک برهم‌نهی با دامنه برابر از تمام نقاط دامنه تابع درست می‌کنیم:



$$\frac{1}{\sqrt{N}} \sum_{i=1}^N |i\rangle$$

این الگوریتم از دو مرحله تشکیل شده است. در مرحله اول گیت U_f اعمال می‌شود که در آن همانطور که در سمت چپ شکل ۸ می‌بینید دامنه نقطه x_0 را منفی می‌کند. مرحله دوم تقارن حول میانگین است که در سمت راست شکل دیده می‌شود. با اعمال این تابع که می‌توان نشان داد یک عملگر یکانی است، دامنه همه نقاط کم می‌شود و دامنه نقطه x_0 بیش از دو برابر بزرگتر می‌شود. اثبات می‌شود با تکرار این دو مرحله به تعداد \sqrt{n} بار دامنه x_0 به بیشترین مقدار خود رسیده لذا با اندازه‌گیری کیوبیت‌ها در این مرحله با بیشترین احتمال حالت کیوبیت‌ها به $|x_0\rangle$ درهم می‌شکند.



شکل ۸: یک مرحله اجرای الگوریتم جستجوی گراور- سمت چپ: حالت کیوبیت‌ها بعد از اعمال عملگر U_f . سمت راست: حالت کیوبیت‌ها بعد از اعمال تقارن حول میانگین.

نشان داده شده که این الگوریتم از نظر تعداد فراخوانی‌های تابع f بهترین زمان اجرا را دارد که افزایش سرعت چندجمله‌ای نسبت به حالت کلاسیک دارد. لذا حل مسئله $P=NP$ با این روش ممکن نیست.

۵ پیچیدگی کوانتومی

بعد از ارائه الگوریتم‌های کوانتومی، سوال مطرح این است که در صورت درست بودن فیزیک کوانتوم، ماشینی که بر اساس فیزیک کوانتومی کار کند چقدر قدرت دارد. این سوال برای اولین بار در سال ۱۹۹۰ مطرح شد و محققین زیادی در این زمینه مشغول به تحقیق شدند. برای جواب دادن به این سوال رده پیچیدگی BQP^{12} را تعریف می‌کنیم.

رده پیچیدگی BQP: زبان $L \in BQP$ است اگر یک خانواده چندجمله‌ای یکنواخت از مدارهای کوانتومی $\{Q_n : n \in \mathbb{N}\}$ داشته باشد به طوری که:

۱. برای هر $n \in \mathbb{N}$ مدار Q_n تعداد n کیوبیت ورودی و یک بیت خروجی دارد.

۲. برای هر $x \in \{0, 1\}^n$ ، $\Pr(Q_n(x) = L(x)) \geq 2/3$.

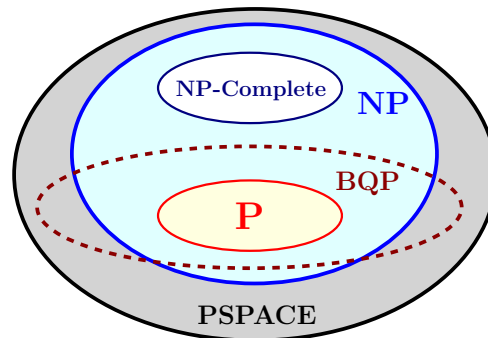
این رده پیچیدگی معادل کوانتومی کلاس پیچیدگی BPP است. از آنجا که ماهیت مدارهای کوانتومی احتمالاتی است، برای تعمیم رده‌های پیچیدگی کلاسیک به کوانتومی، به سراغ BPP رفتیم و نه NP.

¹²Bounded error Quantum Polynomial time

اکثر محققین احتمال می دهند که $NP \not\subseteq BQP$ باشد. از طرفی مسئله‌ای وجود دارد که بر این باوریم عضو PH نیست ولی در BQP است.

می دانیم $BQP \subseteq PSPACE$ زیرا اگر یک مدار کوانتومی داشته باشیم که با مجموعه جهانی گیت‌های کوانتومی ساخته شده است، از آنجا که ورودی‌های هر گیت حداکثر سه کیوبیت است می توان به صورت بازگشتی ورودی‌های گیت‌ها را مرحله به مرحله در حافظه چندجمله‌ای حساب کرد.

با توجه به موارد مطرح شده در بالا رابطه بین کلاس‌های پیچیدگی در شکل ۹ نشان داده شده است.



شکل ۹: رابطه احتمالی کلاس پیچیدگی BQP با کلاس‌های پیچیدگی کلاسیک

دیدیم که رابطه دقیق بین NP و BQP نداریم. لذا کلاس پیچیدگی QMA^{۱۳} را تعریف می کنیم که تعمیم کوانتومی کلاس پیچیدگی QMA^{۱۴} است. برای این کار دو گزینه داریم:

- ماشین محاسباتی آرتور را کوانتومی کنیم. با این کار به کلاس محاسباتی QCMA می رسیم.
- ماشین محاسباتی آرتور و هم پیغام مرلین به آرتور را کوانتومی کنیم. با این کار به کلاس پیچیدگی QMA می رسیم.

به وضوح روابط زیر را داریم:

$$P \subseteq NP \subseteq MA \subseteq QCMA \subseteq QMA$$

$$P \subseteq BPP \subseteq BQP \subseteq QCMA$$

آیا مسئله QMA - تمام وجود دارد؟ بله. مسئله همیلتونی کوانتومی k موضعی^{۱۵} تعمیمی از مسئله k -SAT است که QMA - تمام است. مسئله همیلتونی کوانتومی k موضعی: عملگرهای کوانتومی H_1, H_2, \dots, H_m داده شده است که هر کدام روی k کیوبیت از مجموع n کیوبیت اثر می کنند. H را به شکل $H = \sum_{i=1}^m H_i$ تعریف می کنیم. می دانیم در یکی از حالات زیر هستیم:

- همه مقادیر ویژه H بزرگتر از b هستند.
- H یک مقدار ویژه کوچکتر از a دارد.

هدف تعیین این است که در کدام یک از این حالات هستیم.

می دانیم مسئله SAT-3 - NP تمام است در صورتی که مسئله SAT-2 ساده است و راه حل چندجمله‌ای دارد. در حالی که مسئله همیلتونی کوانتومی k موضعی حتی برای $k=2$ هم QMA - تمام است.

در پایان به یکی از مسائل حل نشده در پیچیدگی محاسبات کوانتومی اشاره می کنیم. این مسئله که حدس PCP کوانتومی نام دارد، صورت تعمیم یافته قضیه PCP است. در مورد صورت صحیح این حدس هم تردید وجود دارد. یک روش برای بیان آن به شرح زیر است:

حدس PCP کوانتومی: برای هر $L \in QMA$ یک اثبات $|\xi\rangle$ و یک تصدیق گر زمان چندجمله‌ای وجود دارد که روی ورودی x و $|\xi\rangle$ عمل می کند و تنها با خواندن $O(1)$ کیوبیت از اثبات، با یک خطای ثابت در مورد عضویت x در زبان تصمیم می گیرد.

^{۱۳}Quantum Merlin Arthur

^{۱۴}کلاس پیچیدگی MA یک سیستم اثبات تعاملی است که در آن تصادفی بودن عمومی داریم. در این سیستم اثبات، اثبات گر را مرلین و تصدیق گر را آرتور می نامیم.

^{۱۵}k-local Hamiltonian problem

1. Sanjeev Arora, Boaz Barak “Computational Complexity: A Modern Approach”
2. Michael A. Nielsen, Isaac L. Chuang, “Quantum Computation and Quantum Information”
3. <http://www.scottaaronson.com/blog>
4. Dorit Aharonov, Itai Arad, Thomas Vidick, “The Quantum PCP Conjecture” [arXiv:1309.7495]