محاسبات کوانتمی (۲۲۶۷۱) ترم بهار ۱۳۹۱-۱۳۹۰

مدرس: سلمان ابوالفتح بیگی نویسنده: هیربد کمالی نیا

جلسه ۹

۱ مدل جعبه-سیاه یا جستاری

مدل‌هایی که در جلسه‌ی پیش برای استفاده از توابع در الگوریتم‌های کوانتمی بیان شد، از ساختار و ماهیت تابع به ما اطلاعی نمی‌دهند، و صرفا با سوال پرسیدن از مدل، مقدار تابع را در ورودی مورد نظر به ما می‌دهند. گویی این مدل یک جعبه سیاه[۱] است که ورودی را می‌گیرد و خروجی را با توجه به آنچه تابع روی آن اثر می کند، به ما می‌دهد. به این نوع مدل کردن، مدل جعبه-سیاه یا مدل جستاری می گویند. قابل توجه است که پیچیدگی مسائل در این مدل بر حسب تعداد سوال کردن[۲] ها محاسبه می شود.

۲ الگوریتم جستجوی Grover

۱.۲ مسأله

ورودی: $f : \{0,1\}^n \to \{0,1\}$

شرط: دقیقاً یک $t \in \{0,1\}^n$ وجود دارد که $f(t) = 1$.

خروجی: t را بیابید.

تعداد ورودی‌ها برابر $N = 2^n$ می باشد. و به طور کلاسیک نمی‌توان این مساله را با «پیچیدگی» بهتر از $O(N)$ حل کرد. الگوریتم کوانتمی Grover توانایی حل این مساله را با $O(\sqrt{N})$ سوال دارد.

۲.۲ مقدمات

برای حل مساله‌ی فوق، سوال کوانتمی[۳] از تابع f را به صورت عملگر یکانی زیر مدل می‌کنیم:

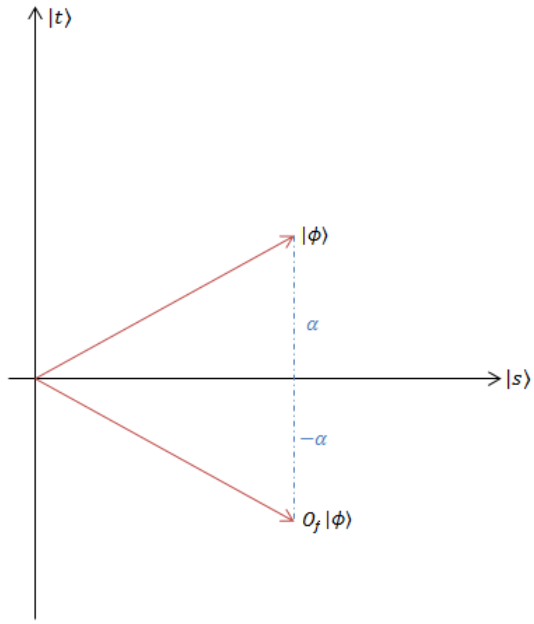
$$O_f|x\rangle = (-1)^{f(x)}|x\rangle.$$

پس اگر $|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x|x\rangle$ آنگاه $O_f|\psi\rangle = \sum_{x\in\{0,1\}^n}(-1)^{f(x)}\alpha_x|x\rangle$.

[۱] Black Box Model/Query Model

[۲] Query

[۳] Quantum query



شکل ۱: اعمال O_f در واقع عمل قرینه کردن نسبت به $|s\rangle$ است

تعریف کنید

$$|s\rangle := \frac{1}{\sqrt{N-1}} \sum_{y\in\{0,1\}^n, y\neq t} |y\rangle.$$

در نتیجه $\langle s|t\rangle = 0$ و

$$|\phi\rangle = \alpha|t\rangle + \beta|s\rangle \quad \Rightarrow \quad O_f|\phi\rangle = -\alpha|t\rangle + \beta|s\rangle.$$

در واقع با توجه به شکل ۱ اعمال O_f متناظر با قرینه کردن نسبت به بردار $|s\rangle$ است.

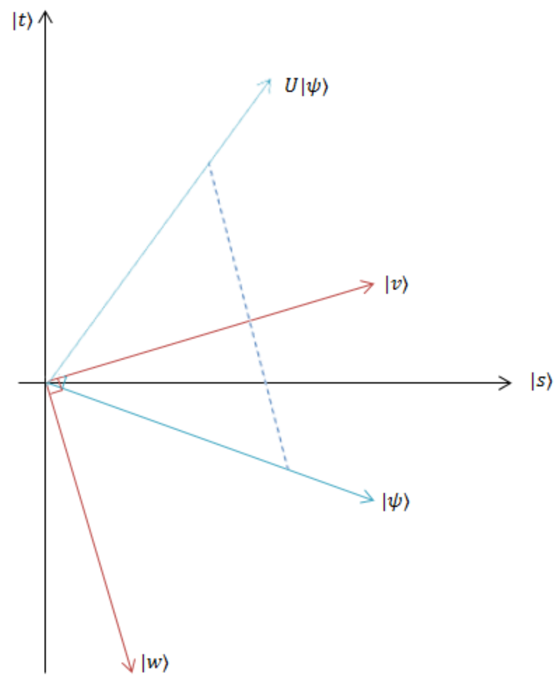
بردارهای $|v\rangle$ و $|w\rangle$ را به صورت زیر تعریف کنید

$$|v\rangle := \frac{1}{\sqrt{N}} \sum_{x\in\{0,1\}^n} |x\rangle \quad \Rightarrow \quad |v\rangle = \sqrt{\frac{N-1}{N}}|s\rangle + \frac{1}{\sqrt{N}}|t\rangle$$

$$|w\rangle := \frac{1}{\sqrt{N}}|s\rangle - \sqrt{\frac{N-1}{N}}|t\rangle \quad \Rightarrow \quad \langle v|w\rangle = 0$$

تبدیل یکانی U را در نظر بگیرید:

$$U := H^{\otimes n}(2|0\dots0\rangle\langle0\dots0| - I)H^{\otimes n} = 2H^{\otimes n}|0\dots0\rangle\langle0\dots0|H^{\otimes n} - I$$



شکل ۲: اعمال U در واقع عمل قرینه کردن نسبت به $|v\rangle$ است

که در آن H ماتریس هادامارد است. داریم:

$$\begin{aligned} H^{\otimes n}|0\dots 0\rangle &= (H|0\rangle) \otimes \dots \otimes (H|0\rangle) \\ &= (\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) \otimes \dots \otimes (\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) \\ &= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle = |v\rangle. \end{aligned}$$

در نتیجه

$$U = 2|v\rangle\langle v| - I$$

و برای $|\psi\rangle = \gamma|v\rangle + \lambda|w\rangle$ داریم

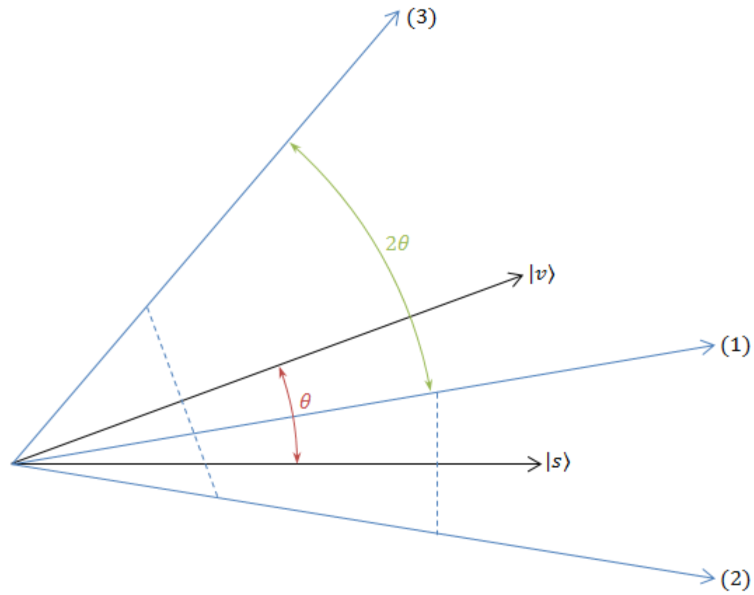
$$U|\psi\rangle = \gamma U|v\rangle + \lambda U|w\rangle = \gamma|v\rangle - \lambda|w\rangle.$$

O_f نسبت به $|s\rangle$ و U نسبت به $|v\rangle$ عمل تقارن را انجام می‌دهند. و همانطور که می‌دانیم، ترکیب دو عمل تقارن، یک عمل دوران بدست می‌دهد (شکل ۳)

$$UO_f = R_{2\theta}$$

که در آن

$$\cos\theta = \langle v|s\rangle = \sqrt{\frac{N-1}{N}} \quad \Rightarrow \quad \theta \approx \frac{1}{\sqrt{N}}$$



شکل ۳: $(2) = O_f(1), (3) = U(2)$

۳.۲ الگوریتم

با n کیوبیت که همگی در حالت $|0\rangle$ آماده‌سازی شده‌اند شروع می‌کنیم. ابتدا روی هر یک از n کیوبیت عملگر هادامارد را اعمال می‌کنیم و بعد $UO_f = R_{2\theta}$ را q بار و در آخر همه‌ی n کیوبیت را در پایه‌ی استاندارد اندازه می‌گیریم:

$$|0\dots0\rangle \xmapsto{H^{\otimes n}} |v\rangle \xmapsto{(UO_f)^q} |\tau\rangle \to \text{measurement}$$

$|\tau\rangle = (UO_f)^q|v\rangle$ یک بردار با زاویه $2q\theta + \theta$ از حالت $|s\rangle$ می‌باشد. اگر $q \approx \frac{\sqrt{N}}{4}\pi$ بگیریم، این زاویه تقریباً برابر $\frac{\pi}{2}$ خواهد بود. در این صورت $|\tau\rangle$ تقریباً برابر $|t\rangle$ می‌شود. حال با اندازه‌گیریی $|\tau\rangle$ در پایه‌ی استاندارد، حاصل اندازه‌گیری با احتمال

$$p(t) = \|\langle t|(UO_f)^q|v\rangle\|^2 = \|\langle t|\tau\rangle\|^2$$

برابر t خواهد شد، و از آنجا که $|\tau\rangle$ و $|t\rangle$ به هم نزدیک هستند، این عدد نزدیک به 1 است. در نتیجه این الگوریتم با $q = O(\sqrt{N})$ سوال کوانتمی، جواب را با احتمال بالا می‌یابد.

۳ الگوریتم تجزیه Shor

۱.۳ مسأله

مسأله 1:

ورودی: $N \in \mathbb{N}$

خروجی: تجزیه N به عوامل اول

مسأله‌ی تجزیه، به مسأله‌ی زیر کاهش می‌یابد. یعنی اگر مسأله‌ی زیر را حال کنیم، آنگاه الگوریتمی برای تجزیه خواهیم داشت.

مسأله 2:

ورودی: $N \in \mathbb{N}$

خروجی: k که $2 \leq k \leq N-1$ و $k|N$ ؛ یا اعلام اینکه N عدد اول است.

الگوریتم کوانتمی Shor، این مسأله را در زمان $O((\log N)^3)$ حل می‌کند.

۲.۳ بخش کلاسیک

در ابتدا به نکاتی از نظریه اعداد توجه می‌کنیم که در حل مسأله 2 به کار برده می‌شوند:

(الف) اگر N زوج باشد، $k=2$ و مسأله حل شده است.

(ب) اگر $N=m^t$ که $t \geq 2$ ، مسأله را می توان به طور کلاسیک در زمان لگاریتمی $O((\log N)^2)$ حل کرد. زیرا در این صورت $\log N = t \log m$ یعنی t حداکثر $\log N$ است. پس به ازای هر عدد طبیعی t در بازه‌ی $2 \leq t \leq \log N$ می‌توان چک کرد که آیا m در $\log m = \log N/t$ عددی صحیح است یا خیر. در این صورت قرار دهید $k=m$.

(ج) فرض کنید $2 \leq x \leq N-1$،

اگر $\gcd(x,N) \neq 1$ قرار دهید $k=\gcd(x,N)$

در غیر این صورت: وجود دارد r به طوری که $x^r \equiv 1 \pmod N$ و فرض می کنیم r کوچکترین عدد با این خاصیت باشد.

با فرض اینکه r را می دانیم و همچنین r زوج است:

$$y := x^{\frac{r}{2}} \quad \Rightarrow \quad N | y^2-1=(y-1)(y+1), \quad N \not| (y-1)$$

در نتیجه $\gcd(N,y+1) \neq 1$ و قرار می‌دهیم $k=\gcd(N,y+1)$

قضیه ۱ فرض کنید N زوج نباشد، و N به صورت m^t نباشد؛ در این صورت اگر x را به طور تصادفی بین 2 تا $N-1$ انتخاب کنیم به طوری که:

$$\gcd(x, N) = 1$$

آنگاه با احتمال حداقل $\frac{1}{2}$ ، r زوج است.

پس در آخر ، حل مسأله 1 به یافتن r با شرایط زیر کاهش می‌یابد:

$$f : \{1, \ldots, N\} \to \{1, \ldots N\}$$

$$f(s) = x^s (\mod N)$$

$$f(s + r) = f(s)$$

برای یافتن r الگوریتمی کوانتمی معرفی می‌کنیم.

۳.۳ تبدیل فوریه روی گروه $\mathbb{Z}_M$

V را یک فضای M بعدی با پایه‌ی متعامد یکه‌ی $\{|0\rangle, |1\rangle, \ldots |M-1\rangle\}$ در نظر بگیرید؛ تبدیل فوریه روی این گروه عبارتست از:

$$F|x\rangle = \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} \omega^{xy} |y\rangle$$

که $\omega = e^{\frac{2\pi i}{M}}$ ریشه‌ی M-ام واحد است. برای اثبات یکانی بودن F کافیست نشان دهیم:

$$\forall x, x' \in V : x \neq x' \Rightarrow (F|x\rangle, F|x'\rangle) = 0$$

که داریم:

$$(F|x\rangle, F|x'\rangle) = \frac{1}{M} \sum_{y=0}^{M-1} (\omega^*)^{xy} \omega^{x'y} = \frac{1}{M} \sum_{y} \omega^{y(x'-x)} = \delta_{xx'}$$

۴.۳ الگوریتم

ورودی: $f : \{0, \ldots, M-1\} \to \{0, \ldots, M-1\}$

شرط: $\exists r : f(x + r) = f(x)$

خروجی: r را بیابید.

سوال کوانتمی از f را با نگاشت یکانی زیر مدل می‌کنیم:

$$O_f |x\rangle|y\rangle = |x\rangle|f(x) + y(\mod M)\rangle.$$

الگوریتم ۲

$$
\begin{aligned}
|0\rangle|0\rangle &\xmapsto{F\otimes I} \frac{1}{\sqrt{M}}\sum_{x=0}^{M-1}|x\rangle|0\rangle \\
&\xmapsto{O_f} \frac{1}{\sqrt{M}}\sum_{x=0}^{M-1}|x\rangle|f(x)\rangle \\
&= \frac{1}{\sqrt{M}}\sum_{s=0}^{r-1}\left(\sum_{t=0}^{\frac{M}{r}-1}|rt+s\rangle\right)|f(s)\rangle \\
&\xmapsto{F^\dagger\otimes I} \frac{1}{M}\sum_{s=0}^{r-1}\sum_{t=0}^{\frac{M}{r}-1}\sum_{y=0}^{M-1}\omega^{-(rt+s)y}|y\rangle|f(s)\rangle \\
&= \frac{1}{M}\sum_{s=0}^{r-1}\sum_{y=0}^{M-1}\left(\sum_{t=0}^{\frac{M}{r}-1}\omega^{-t(ry)}\right)\omega^{-sy}|y\rangle|f(s)\rangle =: |\psi\rangle.
\end{aligned}
$$

گیریم $\alpha = \omega^{-ry}$، بدین ترتیب داریم:

$$
\sum_t \omega^{-t(ry)} = \sum_{t=0}^{\frac{M}{r}-1}\alpha^t = \begin{cases} 0 & \alpha \neq 1 \\ \frac{M}{r} & \alpha = 1 \end{cases}
$$

پس خواهیم داشت:

$$
\sum_t \omega^{-t(ry)} = \begin{cases} 0 & M \nmid ry \\ \frac{M}{r} & M|ry \end{cases}
$$

در نتیجه، حالت حاصل از الگوریتم به صورت زیر خواهد بود:

$$
|\psi\rangle = \frac{1}{r}\sum_s \sum_{y:M|ry}\omega^{-sy}|y\rangle|f(s)\rangle
$$

با اندازه گیری مؤلفه اول، یک y بدست می آید با این خاصیت که $M|ry$. پس اگر قرار دهیم $k = \gcd(M,y)$ آن گاه

$$
\frac{M}{k}|r
$$

یعنی می‌فهمیم که r مضربی از M/k است. لذا با چندبار تکرار، r را می توان بدست آورد.

برای اطلاعات بیشتر و مشاهده‌ی فهرست الگوریتم‌های کوانتومی به وب سایت زیر رجوع کنید:

`math.nist.gov/quantum/zoo/`