الگوریتم کوانتومی جستجو

وحید کریمی پور_ دانشکده فیزیک _ دانشگاه صنعتی شریف

۱۰ خرداد ۱۴۰۲

۱ مقدمه

بسیاری از مسایل در حوزه های ریاضیات، علوم کامپیوتر و علوم طبیعی (فیزیک، شیمی، زیست شناسی،...) وجود دارند که برای آنها راهی بجز جستجو نداریم. صورت این مسائل بسیار ساده ولی حل آنها بسیار سخت است. اگر فضای هیئت های ممکن برای این مسایل را با S نشان دهیم که در آن تعداد هیئت ها را با $|S| = N$ نشان دهیم، یک یا چند هیئت خاص در این فضا وجود دارند که دارای یک خاصیت معین هستند و پاسخ مسئله ی ما هستند. چند نمونه از این مسایل اینها هستند:

- **یافتن حالت پایه یک هامیلتونی بس ذره ای:** به عنوان مثال پیدا کردن حالت پایه یک هامیلتونی بس ذره ای نمونه ای از این مسایل است. برای سادگی یک هامیلتونی کلاسیک آیزینگ با برهم کنش های تصادفی در نظر بگیرید:

$$H = \sum_{i,j} J_{i,j} S_i S_j, \qquad (۱)$$

که در آن $S_i = \pm 1$ مقادیر یک و منهای یک اختیار می کند. می توانیم از خود بپرسیم که کدام هیئت از اسپین هاست که مقدار انرژی را از یک مقدار معین E_0 پایین تر می آورد. با تکرار این عمل و کوچکتر کردن E_0 می توانیم حالت پایه این هامیلتونی را پیدا کنیم. در واقع این مسئله نمونه ای کلی از گروه وسیعی از مسایل فیزیک است که در آنها می خواهیم حالت پایه یک هامیلتونی را پیدا کنیم.

- **پیدا کردن حالت ثانوی یک پروتئین:** یک پروتئین ماکرومولکولی است شامل صدها و هزاران آمینو اسیدِ مختلف که در یک زنجیره قرار گرفته اند. انواع آمینو اسید ۲۱ تاست. بسته به نحوه قرار گرفتن این آمینواسید ها و انرژی بین آنها پروتئین نهایتا یک ساختار فضایی پیدا می کند که کارکرد آن را در سلول تعیین می کند. اغلب پروتئین ها مثل قفل ها و کلیدهای مختلف یا ماشین های سلولی عمل می کنند و کارکردشان دقیقا به شکل فضایی آنها وابسته است. یک مسئله مهم برای شناخت کارکرد پروتئین ها و احتمالا سنتز آنها این است که از روی ساختار اولیه (یعنی نحوه چینش آمینواسیدها) بتوانیم ساختار نهایی آنها را پیدا کنیم. بدیهی است که تعداد ساختارهای نهایی فوق العاده زیاد است. در غیاب راه های تحلیلی تنها راه برای یافتن ساختار نهایی جستجوست.

- **مسئله تصدیق عبارت های منطقی** این مسئله یک مسئله مهم در علوم کامپیوتر و طبیعتا در ریاضیات است. فرض کنید که $A = \{x_1, x_2, \cdots x_n\}$ متغیرهای منطقی هستند که می توانند مقادیر درست 1 یا نادرست 0 را اختیار کنند. یک عبارت k تایی[1]، عبارتی است مثل

$$x_{i_1} \vee x_{i_2} \vee x_{i_3} \vee \cdots \vee x_{i_K}, \qquad (۲)$$

که درآن هرکدام از x_i ها یا یکی از متغیرهای A ست یا یکی از متغیرهای $\overline{A} = \{\overline{x_1}, \overline{x_2}, \cdots \overline{x_n}\}$. به عنوان مثال یک $4 - Clause$ عبارتی است مثل $x_1 \vee \overline{x_3} \vee \overline{x_5} \vee x_6$. حال یک جمله شامل تعدادی عبارت هم اندازه در نظر می گیریم مثل

$$S = C_1 \wedge C_2 \wedge C_3 \wedge \cdots \wedge C_p. \qquad (۳)$$

سوال این است که آیا یک انتخاب از متغیرهای A وجود دارد که به ازای آنها عبارتِ S مقدارِ ۱ را اختیار کند یعنی عبارت S ارزش منطقی درست داشته باشد یا خیر؟ لازمه این کار آن است که عبارت های C_1 تا C_p همه مقادیر ۱ را اختیار کنند. بنابراین، این مسئله را که اصطلاحاً مسئله $K - Sat$ [2] می نامند، می توان به عنوان یک مسئله‌ی p معادله و n مجهولی از متغیرهای منطقی نامید، به این معنا که می خواهیم ببینیم دستگاه معادلات منطقی زیر جواب دارند یا نه:

$$\begin{aligned} C_1 &= 1 \\ C_2 &= 1 \\ &\cdots \\ C_p &= 1. \end{aligned} \qquad (۴)$$

[1] Clause
[2] K-Satisfiability

بعداز آنکه اثبات کامل بودن مسئله تصدیق در کلاس NP توسط کوک و لوین در سال ۱۹۷۰، تعداد بسیار زیادی از مسائل کامل در همین کلاس کشف شدند. تعداد این نوع مسائل آنقدر زیاد شده است (حدود ۲۰۰۰ مسئله) که امروزه دیگر اثبات کامل بودن یک مسئله در کلاس NP هیجان چندانی ایجاد نمی کند. نمونه‌ای از این مسایل در ادامه می آید.

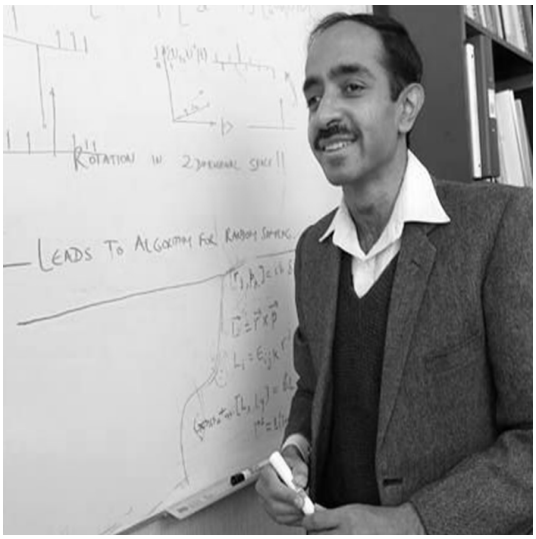
- **مسئله فروشنده دوره گرد** این مسئله نیز یک مسئله مهم در علوم کامپیوتر و ریاضیات است. دلایل این اهمیت را در درسهای بعدی خواهیم دید. یک گراف ِ وزن دار[۳] $G = (V, E)$، عبارت از گرافی است که به هرکدام از یال های آن یک عدد نامنفی نسبت داده شده است. می توان راس های این گراف را به عنوان شهرهای یک منطقه و وزن ها را مسافت بین این شهرها یا مثلاً بهای سفر بین این شهرها تلقی کرد. مسئله فروشنده دوره گرد عبارت است از پیدا کردن ارزان ترین مسیر بسته‌ای که از همه شهرهای این منطقه بگذرد. در این مسئله نیز سایز مسئله همان سایز گراف است.

به این ترتیب همه این مسایل را می توان تحت عنوان یک مسئله کلی جستجو طبقه بندی کرد و مسئله جستجو را به صورت مجرد و کلی زیر تعریف کرد. مجموعه $S := \{x_1, x_2, \cdots x_N\}$ شامل N شی است. تابعی مثل $f : S \longrightarrow \{0, 1\}$ روی این مجموعه تعریف شده است. می دانیم که‌مقدار تابع f تنهایکی از عناصر این مجموعه که آن را با w نشان می دهیم برابربا صفر است و روی دیگر عناصر مجموعه S مقدار این تابع برابر با صفر است. w یکی از x_i هاست ولی نمی دانیم که کدام یک از آنهاست. فعلا حالت ساده ای را در نظر می گیریم که تنها یک جواب وجود دارد. حالت کلی تر در تمرین ها آمده است. درغیاب هرنوع اطلاعات اضافه ای، تنها کاری که باید بکنیم آن است که x_i های مختلف را یک به یک به تابع بدهیم و خروجی تابع را نگاه کنیم . هرگاه خروجی تابع f برابر با یک شد می فهمیم که عنصر داده شده به تابع w بوده است. بطور متوسط می بایست تابع را $O(\frac{N}{2})$ بار بخوانیم تا بتوانیم به w دسترسی پیداکنیم. اما با استفاده هوشمندانه ای از اصل برهم نهی و توازی کوانتومی می توان این مقدار را به $O(\sqrt{N})$ تقلیل داد که برای N های بزرگ کاهش قابل ملاحظه ای است. مسلم است که کلاس این مسئله با این ابداع تغییری نکرده است و همچنان این مسئله درکلاس مسائل چند جمله ای است،اما بدلیل نقشی که یک آلگوریتم جستجو دراغلب آلگوریتم های دیگربازی می کند، این پیشرفت اهمیت زیادی دارد. دقت کنید که در همه این مسایل ما تابع f را بخوبی می شناسیم اما نمی دانیم که کدام متغیر w است که این تابع به ازای آن برابر با 1 است.

- تمرین: یک مجموعه داده نامنظم که دارای N داده است و یکی از آنها داده مطلوب ماست در نظر بگیرید. حال به یکی از این دو روش شروع به جستجوی این مجموعه داده می کنیم:

روش اول: مجموعه داده را یکی یکی به طور منظم جستجو می کنیم تا به داده مطلوب برسیم. طبیعی است که در این روش هر داده را فقط

[۳] Weighted graph



شکل ۱: لو گرور (۱۹۶۱ـ)

یک بار تست می کنیم.

روش دوم: مجموعه داده ها را به طور تصادفی جستجو می کنیم تا به داده مطلوب برسیم. در این روش یک داده ممکن است بیش از یک بار تست شود. تعداد متوسط دفعاتی را که باید داده ها را تست کنیم تا به نتیجه مطلوب برسیم در هرکدام از دو روش محاسبه کنید.

۲ آلگوریتم جستجوی گرورِ

لو گرور دانشمند ($Lov \quad Grover$) علوم کامپیوتر آمریکایی هندی تبار است که تحصیلات لیسانس خود را درموسسه فناوری هند و تحصیلات تکمیلی خود را در دانشگاه استانفورد تمام کرده است و سپس به آزمایشگاه بل و پس از آن به دانشگاه کرنل رفته. در آزمایشگاه بل و در سال ۱۹۹۶ آلگوریتم خود را برای جستجوی کوانتومی ارائه کرد، که دومین آلگوریتم کوانتومی مهم بعد از آلگوریتم شر [۲] دومین

آلگوریتم مهم کوانتومی است.

Shor Algorithm[۳]

نخست دقت می کنیم که تابع f دریک مدار کوانتومی بصورت عملگر کوانتومی یکانی زیر نشان داده می شود:

$$U_f|x_i, y\rangle = |x_i, f(x_i) \oplus y\rangle. \tag{۵}$$

هرگاه این عملگر را روی ورودی $|x_i\rangle \otimes |-\rangle$ اثر دهیم که درآن $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$، آنگاه براحتی دیده می شود که

$$\begin{aligned} U_f|w\rangle \otimes |-\rangle &= -|w\rangle \otimes |-\rangle \\ U_f|x_i\rangle \otimes |-\rangle &= |x_i\rangle \otimes |-\rangle \qquad x_i \neq w. \end{aligned} \tag{۶}$$

بنابراین روی زیرفضای اول اثر این عملگر به شکل یک انعکاس ظاهر می شود . یعنی این عملگر حالت $|w\rangle$ را به حالت $-|w\rangle$ برمی گرداند وبقیه حالات را دست نخورده باقی می گذارد. ازاین به بعد دربحث خود فضای دوم یعنی $|-\rangle$ را برای سادگی حذف می کنیم. درنتیجه می توان عملگر U_f را به شکل زیرنوشت :

$$U_f = I - 2|w\rangle\langle w|. \tag{۷}$$

دراین جا تذکر این نکته مهم است که علیرغم شکل ظاهری خود عملگر U_f بدون دانستن حالت $|w\rangle$ این انعکاس را انجام می دهد زیرا این عملگر چیزی نیست جزهمان عمل تابع f روی عناصر مجموعه S ویا حالات متناظر با آنها.

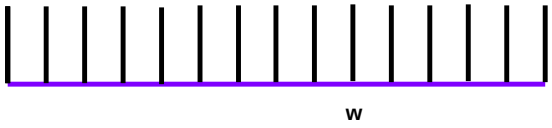
حال فرض کنید که عملگر U_f را روی حالت

$$|s\rangle := \frac{1}{\sqrt{N}}(|x_1\rangle + |x_2\rangle + \cdots |x_N\rangle) \tag{۸}$$

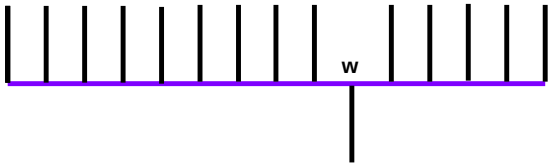
اثر دهیم. نخست آلگوریتم گرور را به طور کیفی توضیح می دهیم. هرگاه حالت فوق رابه شکل 2 نشان دهیم بعداز اثر عملگر U_f به شکل 3 درخواهد آمد. حال اگر این حالت را روی متوسط یا میانگین خودش (کەروی شکل به صورت خط چین نشان داده شده و بعدا به صورت دقیق تعریف خواهد شد) انعکاس دهیم، حالت نشان داده شده درشکل 4 بدست خواهد آمد. این کار را بازتاب نسبت به میانگین [۴] می خوانیم.

می توان نشان داد که این بازتاب نسبت به میانگین نیز یک عملگر یکانی است کەآن را با I_s نشان می دهیم. خواننده می تواند به راحتی تصدیق کند که بعدازچند بار خواندن تابع و بازتاب نسبت به میانگین، یعنی بعد از چند بار اعمال عملگر $G := I_s U_f$ شکل حالت به صورتی

Inversion around the average[۴]



شکل ۲ : بیان شماتیک بردار حالت ورودی که ترکیبی خطی از همه داده های ممکن با ضرایب مساوی است.

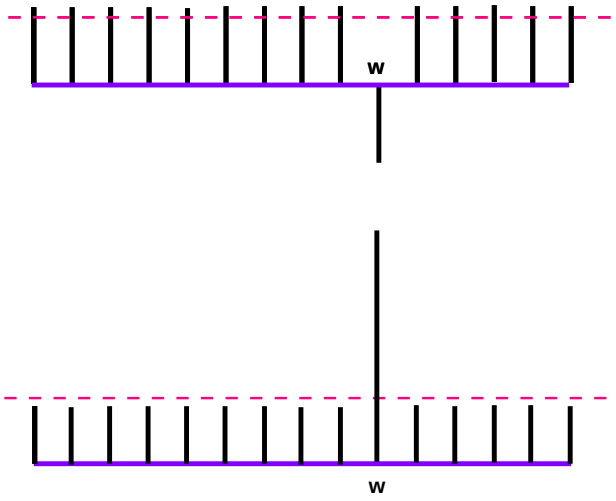


شکل ۳: بردارحالت ورودی پس از آنکه تابع یک بارآن را خوانده است .

درخواهد آمد که درآن دامنه مربوط به $|w\rangle$ نسبت به بقیه دامنه ها افزایش قابل ملاحظه ای پیداکرده است و درنتیجه اندازه گیری چنین حالتی به احتمال زیاد، نتیجه اش $|w\rangle$ خواهد بود. البته پس از هرباراندازه گیری بااحتمال ضعیفی ممکن است که عنصری غیراز $|w\rangle$ یافت شود که دراین صورت با خوراندن آن به تابع f و بدست آمدن مقدار صفر آلگوریتم دوباره از اول طی می شود.

حال آنچه را که به طور کیفی گفتیم بطور دقیق بازگو می کنیم. نخست می بایست ببینیم آیا بازتاب نسبت به میانگین را واقعا می توان با یک عملگر یکانی نشان داد. حالتی مثل

$$|\psi\rangle = \sum_x \psi_x |x\rangle \qquad (۹)$$



شکل ۴: شکل بالا بردار حالت را قبل از انعکاس حول متوسط و شکل پایین بعد از انعکاس حول متوسط نشان می دهد. خط چین مقدار متوسط است.

را در نظر بگیرید. متوسط این حالت برابر است با:

$$\overline{\psi} = \frac{1}{N}\sum_x \psi_x. \qquad (۱۰)$$

و بازتاب نسبت به میانگین $|\psi\rangle$ به صورت زیر است:

$$I_s|\psi\rangle := \sum_x (\psi_x - 2(\psi_x - \overline{\psi}))|x\rangle = \sum_x (2\overline{\psi} - \psi_x)|x\rangle \qquad (۱۱)$$

و در نتیجه

$$I_s|\psi\rangle := \sum_x (2\overline{\psi} - \psi_x)|x\rangle = 2\overline{\psi}\sqrt{N}|s\rangle - |\psi\rangle. \qquad (۱۲)$$

اما می دانیم که

$$\overline{\psi} = \frac{1}{\sqrt{N}}\langle s|\psi\rangle. \qquad (۱۳)$$

بنابراین

$$I_s|\psi\rangle := 2|s\rangle\langle s|\psi\rangle - |\psi\rangle = (2|s\rangle\langle s| - I)|\psi\rangle. \qquad (۱۴)$$

بنابراین عملگر I_s را می توان به صورت زیر نوشت :

$$I_s = 2|s\rangle\langle s| - I, \qquad (۱۵)$$

عملگرترکیبی $G := I_s U_f$ را به ا فتخار کاشف این آلگوریتم عملگر گرور می خوانیم . دراین قسمت می خواهیم نشان دهیم که با اثر عملگر گرور به تعداد $O(\sqrt{N})$ بار روی حالت اولیه $|s\rangle$ می توانیم به حالتی برسیم که دامنه $|w\rangle$ درآن بسیارافزایش یافته است. برای این کار درفضای حالت ها، حالت زیر را تعریف می کنیم :

$$|r\rangle = \frac{1}{\sqrt{N-1}}(\sum_{x_i \neq w} |x_i\rangle). \qquad (۱۶)$$

حال دقت می کنیم که هردو عملگر I_s و U_f را می توان تنها برحسب بردارهای $|w\rangle$ و $|r\rangle$ نوشت. درواقع تمام دینامیک ازاول تا به آخر درزیرفضایی طی می شود که توسط این دوبردار جاروب می شوند. ازآنجا که این دوبرداربرهم عمودند می توانیم نمایش زیر را برای آنها انتخاب کنیم:

$$|w\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad , \qquad |r\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad (۱۷)$$

و

$$|s\rangle = \frac{1}{\sqrt{N}}|w\rangle + \sqrt{\frac{N-1}{N}}|r\rangle = \begin{pmatrix} \frac{1}{\sqrt{N}} \\ \sqrt{\frac{N-1}{N}} \end{pmatrix}. \qquad (۱۸)$$

درنتیجه خوا هیم داشت :

$$U_f = I - 2|w\rangle\langle w| = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad (۱۹)$$

و

$$I_s = 2|s\rangle\langle s| - I = \begin{pmatrix} \frac{2}{N} - 1 & \frac{2}{N}\sqrt{N-1} \\ \frac{2}{N}\sqrt{N-1} & 1 - \frac{2}{N} \end{pmatrix} \qquad (۲۰)$$

درنتیجه عملگر گرور به شکل زیر درخواهد آمد:

$$G = I_s U_f = \begin{pmatrix} 1-\frac{2}{N} & \frac{2}{N}\sqrt{N-1} \\ -\frac{2}{N}\sqrt{N-1} & 1-\frac{2}{N} \end{pmatrix}. \qquad (۲۱)$$

خواننده براحتی می تواند تحقیق کند که این عملگریک عملگر متعامد است یعنی $G^t G = I$ و درنتیجه چیزی جزیک دوران درصفحه جاروب شده توسط $|r\rangle$ و $|w\rangle$ نیست. برای ادامه تحلیل، پارامتر دوران θ را به شکل زیر تعریف می کنیم:

$$\cos\theta = 1 - \frac{2}{N}, \qquad \sin\theta = \frac{2}{N}\sqrt{N-1}, \qquad (۲۲)$$

و به این ترتیب عملگرگرور به شکل زیر درخواهد آمد:

$$G = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}. \qquad (۲۳)$$

هرگاه روی حالت اولیه $|s\rangle$ عملگر گرور را m بار اثردهیم یعنی اینکه آن حالت را به اندازه زاویه $m\theta$ چرخانده ا یم. برای اینکه ببینم این حالت چه مقدار به حالت مطلوب یعنی $|w\rangle$ نزدیک شده است می بایست عنصر ماتریسی $\langle w|G^m|s\rangle$ را حساب کنیم که برابر خواهد شد با:

$$\langle w|G^m|s\rangle = \frac{1}{\sqrt{N}}\cos m\theta + \sqrt{\frac{N-1}{N}}\sin m\theta. \qquad (۲۴)$$

اگر قرار دهیم

$$\cos\alpha = \frac{1}{\sqrt{N}} \quad , \quad \sin\alpha = \sqrt{\frac{N-1}{N}} \qquad (۲۵)$$

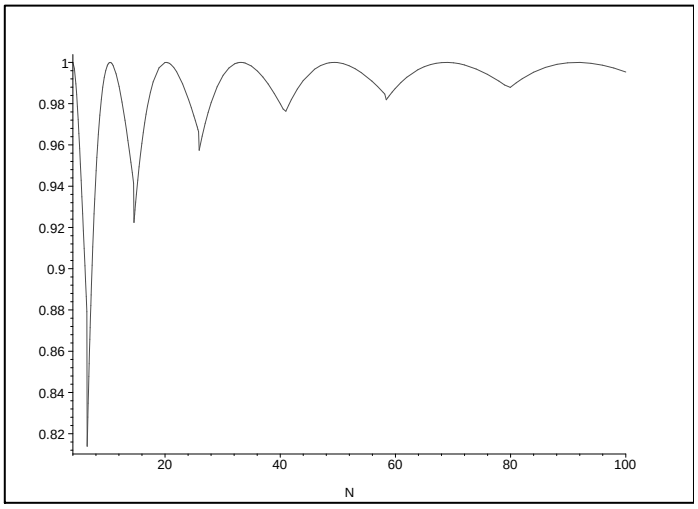
آنگاه خواهیم داشت :

$$\langle w|G^m|s\rangle = \cos(m\theta - \alpha). \qquad (۲۶)$$

برای این که این همپوشانی به حداکثر خود برسد تقاضا می کنیم که $m \approx \frac{\alpha}{\theta}$.

یک نتیجه خیلی جالب که زود می توان دریافت مربوط به حالتی است که $N = 4$ باشد. دراین حالت داریم $\cos\theta = \frac{1}{2}$ و $\cos\alpha = \frac{1}{2}$ و یا

$$\alpha = \frac{\pi}{3}, \qquad \theta = \frac{\pi}{3}, \longrightarrow m = 1 \qquad (۲۷)$$



شکل ۵: احتمال یافتن یک شی دربین N با استفاده از آلگوریتم گرور به عنوان تابعی از N برای $4 \leq N \leq 100$.

یعنی می توان دراین حالت تنها با یک بارخواندن تابع به w آنهم با احتمال یک دست یافت.

برای وقتی که N خیلی بزرگ است داریم

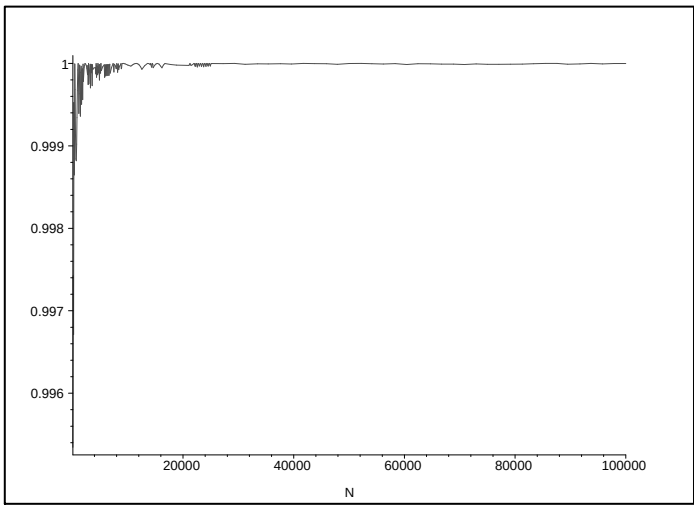
$$\alpha \approx \frac{\pi}{2}, \qquad \cos\theta \approx 1 - \frac{\theta^2}{2} = 1 - \frac{2}{N}, \longrightarrow \theta = \frac{2}{\sqrt{N}}, \tag{۲۸}$$

ودرنتیجه $m \approx \frac{\pi}{4}\sqrt{N}$. به این ترتیب پس از $O(\sqrt{N})$ مرتبه می توانیم با احتمال خیلی خوب شی مورد نظر را دردرون داده ها پیدا کنیم.

برای اینکه این احتمال را پیدا کنیم کافی است که مقدار صحیح m یعنی $[\frac{\pi}{4}\sqrt{N}]$ را درعبارت 26 قراردهیم. این احتمال برابراست با:

$$P(N) := \cos^2([\frac{\pi}{4}\sqrt{N}]\cos^{-1}(1 - \frac{2}{N}) - \cos^{-1}(\frac{1}{\sqrt{N}})). \tag{۲۹}$$

شکل های 5 و 6 این تابع را برحسب N ، نشان می دهد.



شکل ۶: احتمال یافتن یک شی دربین N با استفاده از آلگوریتم گرور به عنوان تابعی از N برای $100 \leq N \leq 100000$.

هرگاه تعداد عناصر مطلوب بیش از یکی مثلاً l تا باشد، اصلاح کوچکی در استدلال بالا نشان می دهد که می توان درزمانی از مرتبه $O(\frac{\pi}{4}\sqrt{\frac{N}{l}})$ به یکی از عناصر مطلوب دست یافت. اثبات دقیق این امر را به عنوان یک تمرین به عهده خواننده می گذاریم.

- تمرین: یک مجموعه داده نامنظم که دارای N داده است و k تا از داده های مطلوب ما هستند در نظر بگیرید. هدف ما این است که یکی از این داده های مطلوب را به روش کلاسیک پیدا کنیم. حال به یکی از این دو روش شروع به جستجوی این مجموعه داده می کنیم:

  روش اول: مجموعه داده را یکی یکی به طور منظم جستجو می کنیم تا به داده مطلوب برسیم. طبیعی است که در این روش هر داده را فقط یک بار تست می کنیم.

  روش دوم: مجموعه داده ها را به طور تصادفی جستجو می کنیم تا به داده مطلوب برسیم. در این روش یک داده ممکن است بیش از یک بار تست شود.

  تعداد متوسط دفعاتی را که باید داده ها را تست کنیم تا به نتیجه مطلوب برسیم در هرکدام از دو روش محاسبه کنید. در روش اول یک عبارت بسته و ساده برای وقتی که $k = 2$ است بدست بیاورید.

■ تمرین: یک مجموعه داده نامنظم که دارای N داده است و دارای k داده مطلوب است در نظر بگیرید. می خواهیم یکی از این داده ها را پیدا کنیم. نشان دهید که یک آلگوریتم کوانتومی می تواند این کار را در زمانی از مرتبه $\sqrt{\frac{N}{k}}$ پیدا کند.

---

۳ مدار کوانتومی آلگوریتم گرور

دراین قسمت نشان می دهیم که عملگرگرور را می توان با ترکیب تعدادی از عملگرهای یک بیتی و دوبیتی کوانتومی به نحو کارآیی ساخت.

می دانیم که $I_s = I - 2|s\rangle\langle s|$. ازطرفی می دانیم که

$$|s\rangle = H^{\otimes N}|0, 0, \cdots 0\rangle =: H^{\otimes N}|\overline{0}\rangle, \tag{۳۰}$$

که درآن H عملگر هادامارد است. بنابراین می توان نوشت :

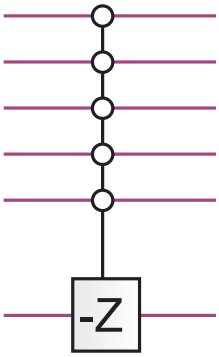
$$I_s = H^{\otimes N} I_0 H^{\otimes N} \tag{۳۱}$$

که درآن $I_0 = 2|\overline{0}\rangle\langle\overline{0}| - I$. بنابراین هرگاه که مدارِ I_0 را بسازیم می توانیم از روی آن مدار I_s را بسازیم. راه ساختن مدارِ I_0 آن است که به شکل ماتریسی آن توجه کنیم. به عنوان مثال برای سه تا کیوبیت I_0 به صورت زیر عمل می کند:

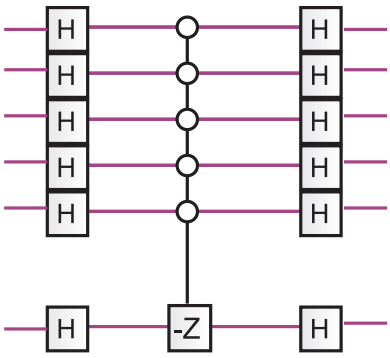
$$\begin{aligned} I_0|000\rangle &= |000\rangle \\ I_0|001\rangle &= -|001\rangle \\ I_0|010\rangle &= -|010\rangle \\ &\cdots \end{aligned} \tag{۳۲}$$

پس معلوم است که $-I_0$ یک عملگر کنترلی فاز [۵] است که فقط وقتی دو کیوبیت اول برابر با صفر باشند عملگر $-Z$ روی کیوبیت آخر عمل می کند. مدار این عملگر و در نتیجه مدار عملگرِ $-I_s$ در شکل های ۷ و ۸ رسم شده است. دایره سفید به این معناست که بیت کنترلی مربوطه با مقدارِ 0 فعال می شود.

[۵] Controlled Phase Gate



شکل ۷: مدار عملگرِ $-I_0$.



شکل ۸: مدار عملگرِ $-I_s$.

۴ بهینه بودن آلگوریتم گرور

. فرض کنید که آلگوریتم جستجو را به شکل زیر تغییردهیم. حالت اولیه رایک حالت دلخواه مثل $\psi(0)$ می گیریم که دیگر یک حالت یکنواخت نیست.

- در این بخش برای سادگی نمادگذاری از علامت کت برای نوشتن بردارهای استفاده نمی کنیم. بنابراین به جای $|\psi\rangle$ به سادگی می نویسیم ψ. البته ضرب داخلی دو بردار را هم چنان با استفاده از علامت کت و برا می نویسیم.

در جاهایی که ابهامی ممکن است وجود داشته باشد، خواننده می تواند به قرینه ابهام را رفع کند. عملگرگرور را نیز درمرحله t ام با $G_t := K_t U_f$ نشان می دهیم. طبیعی است که از خواندن تابع درهرمرحله گریزی نیست و بنابراین U_f همچنان بخش اول عملگر گرور را تشکیل می دهد اما بخش دوم آن بجای بازتاب نسبت به میانگین با یک عملگر مناسب دیگر مثل K_t که درهرمرحله نیز می تواند متفاوت بامرحله قبل باشد تشکیل شده است. می خواهیم نشان دهیم که با عوض کردن حالت یکنواخت اولیه و هم چنین عملگر گرور با یک عملگر دیگر نمی توان جستجو را به صورت بهتری انجام داد. هرگاه عملگرهای گرور را T بار روی حالت اولیه اثر دهیم خواهیم داشت :

$$\begin{aligned} \psi_w(T) &= G_T G_{T-1} G_3 G_2 G_1 \psi(0) \\ &= K_T U_f K_{T-1} U_f \cdots K_3 U_f K_2 U_f K_1 U_f \psi(0) \end{aligned} \qquad (۳۳)$$

دلیل این که حالت سمت چپ را با $\psi_w(T)$ نشان داده ایم این است که این حالت قرار است به حالت w نزدیک شود. برای ادامه کار احتیاج به چند لم و قضیه احتیاج داریم.

■ **قضیه:** قرار می دهیم

$$\psi(T) := K_T K_{T-1} \cdots K_2 K_1 \psi(0). \qquad (۳۴)$$

این حالت حالتی است که بعد از T با ر عمل اپراتورهای K_i بدست می آید بدون این که در هیچ مرحله ای تابع U_f فراخوانی شده باشد. می خواهیم ثابت کنیم که

$$\| \psi_w(T) - \psi(T) \|^2 \leq 4 \left(\sum_{t=0}^{T-1} |\langle w|\psi(t)\rangle| \right)^2 . \qquad (۳۵)$$

به عبارت دیگر داریم:

$$\begin{aligned} \| \psi_w(1) - \psi(1) \| &\leq 2|\langle w|\psi(0)\rangle| \\ \| \psi_w(2) - \psi(2) \| &\leq 2\Big(|\langle w|\psi(0)\rangle| + |\langle w|\psi(1)\rangle|\Big) \\ \| \psi_w(3) - \psi(3) \| &\leq 2\Big(|\langle w|\psi(0)\rangle| + |\langle w|\psi(1)\rangle| + |\langle w|\psi(2)\rangle|\Big) \\ \cdots &\quad \cdots \end{aligned} \qquad (۳۶)$$

■ **اثبات:** برای فهم این قضیه کافی است که چند حالت ساده را بررسی کنیم تا به یک نظم کلی دست پیداکنیم.

به ازای $T = 1$ داریم :

$$\| \psi_w(1) - \psi(1) \| = \| K_1 U_f \psi(0) - K_1 \psi(0) \| = \| (U_f - I)\psi(0) \| = \| 2|w\rangle\langle w|\psi(0)\rangle \| = 2|\langle w|\psi(0)\rangle|, \quad (۳۷)$$

که درآن از یکانی بودن عملگر K_1 وهم چنین تساوی $U_f = I - 2|w\rangle\langle w|$ استفاده کرده ایم .

به ازای $T = 2$ بدست می آوریم:

$$\| \psi_w(2) - \psi(2) \| = \| K_2 U_f K_1 U_f \psi(0) - K_2 K_1 \psi(0) \| = \| U_f K_1 U_f \psi(0) - K_1 \psi(0) \|, \quad (۳۸)$$

که در آن از یکانی بودن K_2 استفاده کرده ایم.

حال یک جمله مناسب به جمله داخل $\| \ \|$ اضافه و کم می کنیم و از نامساوی $\| a + b \| \leq \| a \| + \| b \|$ استفاده کرده و بدست می آوریم:

$$\| \psi_w(2) - \psi(2) \| \leq \| U_f K_1 U_f \psi(0) - U_f K_1 \psi(0) \| + \| U_f K_1 \psi(0) - K_1 \psi(0) \| . \quad (۳۹)$$

حال در طرف راست این نامساوی از یکانی بودن U_f و $U_f K_1$ و اینکه یک عملگر یکانی نرم بردارها را تغییر نمی دهد استفاده می کنیم و بدست می آوریم

$$\begin{aligned} \| \psi_w(2) - \psi(2) \| &\leq \| U_f \psi(0) - \psi(0) \| + \| U_f K_1 \psi(0) - K_1 \psi(0) \| \\ &= \| (U_f - I)\psi(0) \| + \| (U_f - I) K_1 \psi(0) \| . \end{aligned} \quad (۴۰)$$

حال از این که $U_f - I = -2|w\rangle\langle w|$ استفاده کرده و نامساوی بالا را به شکل زیر می نویسیم:

$$\begin{aligned} \| \psi_w(2) - \psi(2) \| &\leq 2 \| |w\rangle\langle w|\psi(0)\rangle \| + 2 \| |w\rangle\langle w|K_1|\psi(0)\rangle \| \\ &= 2|\langle w|\psi(0)\rangle| + 2|\langle w|\psi(1)\rangle| \end{aligned} \quad (۴۱)$$

باتکراراین استدلال برای T دلخواه رابطه (۳۵) ثابت می شود.

■ تمرین: نامساوی (۳۵) را برای $T = 3$ ثابت کنید.

حال به لم زیر توجه می کنیم:

■ **لم ۱:** هرگاه a_1 تا a_N اعداد حقیقی باشند آنگاه

$$(a_1 + a_2 + \cdots a_N)^2 \leq N(a_1^2 + a_2^2 + \cdots a_N^2). \qquad (۴۲)$$

اثبات: این نامساوی چیزی نیست جز نامساوی کوشی شوارتز برای دو بردار $u = (a_1, a_2, \cdots a_N)$ و $v = (1, 1, \cdots 1)$.

با استفاده از این لم می توانیم نامساوی (۳۵) را به صورت زیر بنویسیم:

$$\| \psi_w(T) - \psi(T) \|^2 \leq 4T \left(\sum_{t=0}^{T-1} |\langle w|\psi_w(t)\rangle|^2 \right). \qquad (۴۳)$$

دقت کنید که نامساوی (۴۴) قرار است برای هر کدام از w ها به طور جداگانه برقرار باشد به این معنی که ممکن است داده مورد نظر که در جستجوی آن هستیم هر کدام از حالت های $|1\rangle$ تا $|N\rangle$ باشد . این حالت ها همه برهم عمود بوده و یک پایه کامل تشکیل می دهند بنابراین می توانیم طرفین رابطه (۴۴) را روی w ها جمع بزنیم و بدست آوریم:

$$\begin{aligned} \sum_w \| \psi_w(T) - \psi(T) \|^2 &\leq 4T \sum_w \sum_{t=0}^{T-1} |\langle w|\psi(t)\rangle|^2 \\ &= 4T \sum_{t=0}^{T} \sum_w |\langle w|\psi(t)\rangle|^2 = 4T \sum_{t=0}^{T} \langle\psi(t)|\psi(t)\rangle = \sum_{t=0}^{T-1} 1 = 4T^2 \end{aligned} \qquad (۴۴)$$

بنابراین تا کنون بدست آورده ایم که

$$\sum_w \| \psi_w(T) - \psi(T) \|^2 \leq 4T^2. \qquad (۴۵)$$

بقیه استدلال این است که نشان دهیم طرف چپ نامساوی بالا از $2N - 2\sqrt{N}$ بزرگ تر است که به معنای آن است که تعداد دفعات خواندن تابع یعنی T حتما در نامساوی زیر صدق می کند

$$2N - 2\sqrt{N} \leq 4T^2. \qquad (۴۶)$$

این همان چیزی است که می خواستیم به آن برسیم . در واقع در حد N های بزرگ که $\sqrt{N}$ در مقابل N کوچک است بدست می آوریم که

$$\sqrt{\frac{N}{2}} \leq T.$$

به این ترتیب باقی می ماند که نامسای قول داده شده را ثابت کنیم. این نامساوی چیزی نیست جز یک تمرین ساده در جبر خطی که در پایان به آن می پردازیم.

■ **لم ۲:** هرگاه یک مجموعه بردار های متعامد یکه مثل $\{|u_1\rangle, |u_2\rangle, \cdots |u_N\rangle\}$ داشته باشیم آنگاه به ازای هربرداریکه دیگر مثل $|Y\rangle$ نامساوی زیر برقراراست :

$$\sum_{i=1}^{N} \langle u_i|Y\rangle + \langle Y|u_i\rangle \leq 2\sqrt{N}. \qquad (۴۷)$$

■ **اثبات:** کافی است که برداریکه زیر را تعریف کنیم:

$$|s\rangle := \frac{1}{\sqrt{N}}(|u_1\rangle + |u_2\rangle + \cdots |u_N\rangle), \qquad (۴۸)$$

ونامساوی کوشی شوارتز را برای این بردار و بردار $|Y\rangle$ بنویسیم. بدست می آوریم

$$|\langle Y|u_1\rangle + \langle Y|u_2\rangle + \cdots \langle Y|u_N\rangle| \leq \sqrt{N}. \qquad (۴۹)$$

امامی دانیم که برای هر عدد مختلط a

$$a + a^* = 2\ Re(a) \leq 2|a|, \qquad (۵۰)$$

بنابراین با ترکیب این نامساوی با نامساوی قبلی یعنی (۴۹) به رابطه‌ی ۴۷ می رسیم.

■ تمرین: از ترکیب این دو نامساوی واقعا نشان دهید که رابطه (۴۷) بدست می آید. سپس نشان دهید که این نامساوی را به شکل زیر نیز می توان نوشت:

$$\sum_{i=1}^{N} ||u_i - Y||^2 \geq 2N - 2\sqrt{N}. \qquad (۵۱)$$